A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records

Oversight and Review Division
Office of the Inspector General
January 2010

UNCLASSIFIED

TABLE OF CONTENTS

TABLE OF CONTENTS i

LIST OF ACRONYMS viii

TABLE OF CHARTS, TABLES, AND DIAGRAMS xi

CHAPTER ONE INTRODUCTION xii

I. Findings in the OIG's Previous Reports 2

II. Methodology of the OIG Investigation 4

III. Organization of this Report 6

CHAPTER TWO THE FBI'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 9

I. The Electronic Communications Privacy Act (ECPA) 9

II. Background on the FBI's Use of Exigent Letters 11

A. Origins of Exigent Letters in the FBI's New York Field Division 11

1. The FBI's New York Field Division Contract with Company A 12
2. The New York Field Division's First Use of Exigent Letters 12

B. The Work of the Communications Analysis Unit (CAU) and the FBI's Contracts with the Three Communications Service Providers 14

1. The CAU's Mission and Organizational Structure 16
2. Terminology Used in this Report for Non-Content Telephone Transactional Records 19
3. FBI Contracts with the Three Communications Service Providers 20
4. Location of the Three Communications Service Providers 24
5. Relationship between CAU Personnel and the Providers' Employees 25

III. Exigent Letters Issued by CAU Personnel 25

A. Text of the CAU Exigent Letters 27

B. Counterterrorism Division's and CAU's Recognition of the Use of Exigent Letters 28
C. CAU's Exigent Letters Practice 29
1. Signers of Exigent Letters in the CAU 34
2. CTD Supervisors 38
D. The FBI's Senior Leadership 40
E. Employees of On-site Communications Service Providers 41
F. Types of Cases in which Exigent Letters were Used 43
IV. Other Informal Methods for Requesting Records without Prior Service of Legal Process 45
A. E-mail, Face-to-Face or Telephone Requests, and Informal Notes 45
B. "Sneak Peeks" or "Quick Peeks" 47
V. Records Obtained in Response to Exigent Letters and Other Informal Requests 50
A. Types of Records Collected by the Providers 50
B. How Records were Uploaded and Analyzed by the FBI 52
C. Community of Interest/Calling Circle [redacted] 54
1. Community of Interest [redacted] 54
2. Community of Interest [redacted] for the FBI 56
3. Company A's Use of Community of Interest [redacted] 61
4. FBI Guidance on Community of Interest [redacted] Requests 62
VI. OIG Analysis 64
A. Requests for Telephone Records through Exigent Letters and Other Informal Requests 64
B. "Sneak Peeks" 72
C. Calling Circle/Community of Interest [redacted] 75
CHAPTER THREE: ADDITIONAL USES OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 79
I. Obtaining Calling Activity Information on "Hot Numbers" 79

A. Legal Authority for Obtaining Calling Activity Information 80
B. Hot Number [redacted] 81
1. Company C 82
2. Company A 83
C. FBI OGC and CAU's Unit Chiefs' Knowledge of Hot Number [redacted] 85
D. OIG Analysis 87
II. Seeking Reporters' Telephone Records Without Required Approvals 89
A. Federal Regulations and Department Policies 89
B. First Matter 91
1. Background 91
2. The Investigation of the Leak of Information to the Media 91
3. FBI Notifies the Reporters That Their Records Were Obtained 101
4. OIG Analysis 102
C. Second Matter 104
1. Background 104
2. The Leak Investigation 105
3. OIG Investigation 111
4. OIG Analysis 113
D. Third Matter 114
1. Background 114
2. The Leak Investigation 115
3. OIG Analysis 120
III. Inaccurate Statements to the Foreign Intelligence Surveillance Court 122
A. FISA Case No. 1 124
B. FISA Case No. 2 124
C. FISA Case No. 3 125
D. FISA Case No. 4 126
E. OIG Analysis 127
IV. Improper Administrative Subpoenas Issued to the On-site Providers 129

A. The FBI's Administrative Subpoena Authority 130
B. Administrative Subpoenas Served on the On-Site Providers 131
C. Improper Administrative Subpoenas Issued in Two FBI Investigations 131
1. Issuing FBI Administrative Subpoenas in the Absence of an Active Narcotics Investigation 131
2. Administrative Subpoenas were Signed by Unauthorized Personnel 132
3. Two Additional After-the-Fact Administrative Subpoenas 133
4. Knowledge of the Use of The Title 21 Administrative Subpoenas 134
D. OIG Analysis 134

CHAPTER FOUR: THE FBI'S ATTEMPTS AT CORRECTIVE ACTIONS REGARDING EXIGENT LETTERS 137

I. The FBI's Attempts at Corrective Actions From 2003 through October 2006 137
A. A Backlog First Develops During Rogers's Tenure as CAU Unit Chief 139
B. NSLB Knowledge of Exigent Letters and Involvement in Issuing After-the-Fact NSLs 142
C. NSLB Attorney Meets with CAU Personnel Regarding Exigent Letters 146
D. CAU Begins Implementing then Abandons a Tracking System for Legal Process 150
E. CAU Unit Chief Youssef Learns that the CAU has Obtained Records in Advance of Legal Process 151
F. NSLB Attorney Provides Incorrect Advice to the CAU About the Use of Exigent Letters 154
G. NSLB Fails to Recognize Applicability of the ECPA's Authority for Emergency Voluntary Disclosures to Requests Sent to the CAU 155
H. The September 26, 2005, Meeting 157
I. The CAU Efforts to Reduce the Backlog 159
J. OIG Analysis of FBI Attempts at Corrective Actions From 2003 through October 2006 162

K. FBI Issues 11 Improper Blanket NSLs in May to October 2006 165

1. Youssef Proposes Policy and Procedures for Service of NSLs 165
2. NSLB Revises Model for Exigent Letters but Approves Their Continued Use 166
3. Three Blanket NSLs (May, July, and September 2006) 167
4. Eight Additional Blanket NSLs in 2006 178
5. OIG Analysis of 11 Improper Blanket NSLs 184

II. The FBI's Corrective Action Since November 2006 185

A. FBI OGC Learns of Blanket NSLs 186

B. The CAU's Draft Memorandum to the FBI OGC Reporting Possible Intelligence Oversight Board Violation 187

C. FBI Legal Guidance Clarifying Legal Authorities 190

D. Relocation of Communications Service Providers' Employees From the FBI 191

E. FBI Analysis of Whether it Will Retain or Purge Records 192

1. FBI Analysis 192
2. FBI Analysis of Records Obtained From Exigent Letters and 11 Improper Blanket NSLs 196
3. Steps Taken to Purge Records 208
4. Records Improperly Acquired Relating to Criminal Investigations 208
5. Other NSLs Referred by the OIG to the FBI 209
6. OIG Analysis of FBI Retention Decisions 210

III. OIG Conclusions Regarding FBI Attempts at Corrective Action for Exigent Letters 211

CHAPTER FIVE OIG FINDINGS ON FBI MANAGEMENT FAILURES AND INDIVIDUAL ACCOUNTABILITY 213

I. Management Failures 213

A. Failure to Plan for Proper Use of the On-Site Communications Service Providers 214

B. Failure to Provide Training and Guidance to CAU Personnel 216

C. Failure to Oversee the CAU Activities 219

II. Individual Performance 221
A. CAU Unit Chief Glenn Rogers 221
B. CAU Unit Chief Bassem Youssef 224
C. NSLB Deputy General Counsel Julie Thomas 230
D. NSLB Assistant General Counsel 235
E. General Counsel Valerie Caproni 237
F. Signers of the 11 Blanket NSLs: Joseph Billy, Jr., Arthur Cummings III, Michael Heimbach, and Jennifer Smith Love 239
1. Joseph Billy, Jr. 239
2. Arthur A. Cummings III 240
3. Michael Heimbach 241
4. Jennifer Smith Love 242
5. OIG Conclusion on CTD officials who signed improper blanket NSLs 243
G. CAU Personnel Who Signed Exigent Letters 244
H. FBI Personnel Involved in Media Leak Investigations 249
1. First Matter 249
2. Second Matter 252
3. Third Matter 254
III. Conclusion 256
CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS 257
I. Conclusions 257
A. Exigent Letters and Other Informal Requests 257
B. Other Informal Requests for Telephone Records 268
C. FBI Attempts at Corrective Actions 272
1. The FBI's Initial Attempts at Corrective Action 273
2. Corrective Actions after the OIG's First NSL Report 275
D. Improper Requests for Reporters' Telephone Records or Other Calling Activity in Three Media Leak Investigations 276
E. OIG Findings on Management Failures and Individual Accountability for Exigent Letters and other Improper Requests for Telephone Records 279

II. Recommendations 285

III. OIG Conclusion on Exigent Letters and Other Improper Requests for Telephone Records 288

[PAGE LEFT INTENTIONALLY BLANK]

LIST OF ACRONYMS

AUSA	Assistant United States Attorney
CAU	Communications Analysis Unit
CD	Compact Disk
CDC	Chief Division Counsel
CTD	Counterterrorism Division
CXS	Communications Exploitation Section
DAD	Deputy Assistant Director
DT-6	Domestic Terrorism [Squad] 6
EC	Electronic Communication
ECPA	Electronic Communications Privacy Act
EOPS	Electronic Surveillance Operations & Sharing Unit
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act of 1978
FISA Court	Foreign Intelligence Surveillance Court
FISDU	Field Investigative Software Development Unit
IOB	Intelligence Oversight Board
ITOS-I	International Terrorism Operations Section
NSD	National Security Division
NSI Guidelines	The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection
NSL	National Security Letter
NSLB	National Security Law Branch
OGC	Office of the General Counsel
OIG	Department of Justice Office of the Inspector General
OLC	Office of Legal Counsel
PIOB	Possible Intelligence Oversight Board
SAC	Special Agent in Charge
SSA	Supervisory Special Agent

[PAGE LEFT INTENTIONALLY BLANK]

TABLE OF CHARTS, TABLES, AND DIAGRAMS

CHART 2.1	Organizational Chart of Communications Exploitation Section	15
CHART 2.2	FBI OGC, Senior Leadership, and Counterterrorism Division Officials Management (2003 through 2007)	18
CHART 2.3	Exigent Letters Issued by CAU Personnel to the Three On-Site Communications Service Providers (2003 through 2006)	30
CHART 4.1	Analysis of FBI's Basis for Retaining Records from Exigent Letters and 11 Blanket NSLs	200
CHART 4.2	Analysis of FBI's Basis for Retaining Records from Exigent Letters and 11 Blanket NSLs	201
CHART 4.3	Records for 10 Telephone Numbers Uploaded into FBI Databases with the Longest Periods of Overcollections	207
TABLE 2.1	Exigent Letters Issued by CAU Personnel by Calendar Year (2003 through 2006)	26
TABLE 2.2	Exigent Letters Issued by CAU Personnel to the Three On-Site Communications Service Providers (2003 through 2006)	26
TABLE 4.1	Three Blanket NSLs Issued by the CTD in 2006	169
TABLE 4.2	Eight Blanket NSLs Issued by the CTD in Connection with FBI Operations Y and Z	178
TABLE 4.3	FBI's Analysis of Basis for Retaining Records Listed in Exigent Letters and 11 Blanket NSLs	198
DIAGRAM 2.1	Calling Circle or "Community of Interest" [redacted]	55
DIAGRAM 2.2	Comparison of NSL Approval Process with Exigent Letters	69
DIAGRAM 4.1	Timeline of Requests Made [redacted] by the Three On-Site Communications Service Providers Addressed by Three Blanket NSLs, and Subsequent Corrective Actions	177
DIAGRAM 4.2	FBI Summary Chart of Plan to Rectify the Exigent Letters Situation	194

[PAGE LEFT INTENTIONALLY BLANK]

CHAPTER ONE[1]
INTRODUCTION

On March 9, 2007, the Department of Justice (Department or DOJ) Office of the Inspector General (OIG) issued its first report on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL). Issued in response to the requirements in the *USA PATRIOT Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act), the first report described the use and effectiveness of NSLs, including "any illegal and improper use," in calendar years 2003 through 2005.[2]

On March 13, 2008, the OIG issued its second report on NSLs, which assessed the corrective actions the FBI and the Department had taken in response to the OIG's first NSL report. The second report also described NSL usage in calendar year 2006.[3]

In this third report, we describe the results of our investigation of the FBI's use of exigent letters and other informal requests, instead of NSLs or other legal process, to obtain the production of non-content telephone records from employees of three communications service providers (Companies A, B, and C).[4] The OIG conducted this investigation to examine in greater detail the extent of the FBI's use of exigent letters and other informal requests for such information, as well as to assess the accountability of FBI employees and supervisors who were responsible for these practices. We examined the conduct of the FBI personnel who signed

---

[1] The Office of the Inspector General (OIG) has redacted (blacked out) from the public version of this report information that the FBI and the Intelligence Community considered to be classified. We have provided full versions of our classified reports – a Secret version and a Top Secret/Secure Compartmented Information (SCI) version – to the Department of Justice, the Intelligence Community, and Congressional committees.

[2] U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 9, 2007) (NSL I), available at www.usdoj.gov/oig. We refer to this report as the first NSL report, or NSL I. All references to this report are to the unclassified version that was publicly released. We provided a separate classified version of the report to the Department and Congress.

[3] U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (March 13, 2008) (NSL II), available at www.usdoj.gov/oig. We refer to this report as the second NSL report, or NSL II.

[4] In this report, we do not identify the specific companies because the identities of the specific providers who were under contract with the FBI for specified services are classified.

these letters or made these informal requests, their supervisors, and the FBI's senior leadership.

I. Findings in the OIG's Previous Reports

In our first NSL report, we described how the FBI issued at least 739 so-called "exigent letters" between March 11, 2003, and December 16, 2005. These letters were signed by personnel in the FBI Counterterrorism Division's (CTD) Communications Exploitation Section (CXS) who were not authorized to sign NSLs, including two Assistant Section Chiefs, Unit Chiefs assigned to the CXS's Communications Analysis Unit (CAU), Supervisory Special Agents (SSA), Intelligence Analysts, and an Intelligence Operations Specialist. We determined that the 739 exigent letters requested information relating to approximately 3,000 telephone numbers. The overwhelming majority of the letters requested production of telephone records, allegedly "due to exigent circumstances," and also stated that subpoenas requesting the information had been submitted to a U.S. Attorney's Office for processing and would be served formally as expeditiously as possible.

We concluded that by using exigent letters to acquire information from three communications service providers prior to serving NSLs or other legal process, the FBI circumvented the requirements of the *Electronic Communications Privacy Act* (ECPA) NSL statute and violated the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), and internal FBI policy. We also found that there were factual misstatements in the letters. While almost all exigent letters stated that subpoenas requesting the information had been submitted to a U.S. Attorney's Office and would be served on the providers, in fact subpoenas were not issued in many instances and in other instances had not been requested. Moreover, we developed information that exigent letters sometimes were used in non-exigent circumstances. We also found that the FBI was unable to later establish that some of the exigent letter requests were made in connection with the required open preliminary or full investigations conducted pursuant to the Attorney General's NSI Guidelines or that the records requested were relevant to those investigations.

In our first NSL report we also described the circumstances in which attorneys in the FBI Office of General Counsel's (FBI OGC) National Security Law Branch (NSLB) became aware of the exigent letters practice in late 2004 and the efforts NSLB attorneys made to limit the practice, and the fact that the FBI did not direct that the practice stop for over two years, until after the OIG provided its first NSL report to the FBI in February 2007.

While we recognized the significant challenges the FBI faced during the period covered by our first review, we concluded that these circumstances did not excuse the FBI's circumvention of the requirements of the ECPA NSL statute, the inaccurate statements in the exigent letters, and the violations of the Attorney General's NSI Guidelines and internal FBI policy governing the use of NSLs.

In our second NSL report, we assessed the FBI's response to the findings on the misuse of NSLs in our first NSL report. In particular, we examined the status of the FBI's implementation of our recommendations from our first NSL report and additional corrective actions by the FBI and other Department components. We concluded that the FBI and the Department had made significant progress in implementing our recommendations and had taken other significant corrective actions in response to the serious problems we identified in the use of NSLs. However, we concluded that it was too early to definitively state whether the new systems and controls developed by the FBI and the Department would eliminate fully the problems identified with the FBI's use of NSLs.

As required by the Patriot Reauthorization Act, our second NSL report also described the FBI's use of NSLs in 2006. We found similar misuses of NSLs to those we identified in our first NSL report and a continuation of the upward trend in NSL usage.

Finally, in our second NSL report we made 17 additional recommendations designed to help the FBI further improve its oversight and use of NSLs.

Our first and second NSL reviews were limited to the FBI's use of NSLs and exigent letters and did not investigate other ways in which the FBI initiated requests for records or other calling activity information from the three communications service providers, such as by e-mail, face-to-face, or telephone requests. Our reviews also did not investigate other ways in which the providers' employees gave information to the FBI without legal process, such as by providing calling activity information through what CAU personnel and the three providers called "sneak peeks" or "quick peeks," or by [redacted] FBI personnel to calling activity information by [redacted] "hot numbers."[5] Similarly, our first and second NSL reviews did not investigate ways in which the resources available from the on-site communications

[5] As discussed in more detail in Chapter Three of this report, a hot number is a telephone number identified by the FBI to either Company A or Company C for purposes of having the providers [redacted] to identify calling activity by that number.

service providers were used in connection with other FBI or Department activities, such as FBI administrative subpoenas, applications for electronic surveillance orders filed with the Foreign Intelligence Surveillance Court (FISA Court), or grand jury subpoenas in media leak investigations.

Moreover, in our previous NSL reviews we did not assess the individual accountability of the signers of the exigent letters, their supervisors, or attorneys in the FBI OGC. In addition, we did not address the training, guidance, supervision, or legal oversight provided to the CAU employees who signed the exigent letters, or the role of FBI supervisors and senior FBI management in the use of exigent letters.

In this investigation, as described in this report, we cover these and related subjects.

II. Methodology of the OIG Investigation

The OIG team that conducted this investigation was composed of attorneys, special agents, program analysts, auditors, and paralegals from the OIG's Oversight & Review, Investigations, and Audit Divisions. The OIG team led this investigation and wrote this report. Personnel from the FBI's Inspection Division participated with the OIG team on parts of this investigation.[6]

In this investigation, we interviewed over 100 FBI employees and former employees, as well as employees of Company A, Company B, and Company C, each of which co-located employees in FBI offices beginning in 2003 and continuing through late 2007. We interviewed 31 of the 32 current or former FBI employees who signed the exigent letters. We also

---

[6] After we issued our first NSL report, we initially referred our findings regarding exigent letters to the FBI for it to conduct an investigation to determine whether disciplinary action should be taken against any FBI employees involved in the exigent letters practice. However, after further consideration and discussion with the FBI, we determined that the OIG should lead the investigation. As a result, the OIG determined the scope of the investigation, the witnesses to interview, and the content of this report. Initially, FBI Inspection Division personnel assisted us in interviews of FBI employees and employees of the communications service providers. However, we determined that they should not participate in all aspects of the investigation. For example, the Inspection Division did not participate in the review of CAU Unit Chief Bassem Youssef or his conduct. In addition, after our first interview made clear the scope of the issue, the FBI was not involved in further interviews relating to the leak investigations in which the FBI sought or obtained toll billing records or other calling activity information of members of the news media. Finally, no FBI personnel participated in the writing of this report, and this report reflects the conclusions of the OIG only.

interviewed all 4 of the officials in the FBI Counterterrorism Division (CTD) who signed a total of 11 after-the-fact "blanket" NSLs in 2006 that were issued in an attempt to "cover" or "validate" records previously obtained in response to exigent letters or other improper requests.

We also interviewed FBI supervisory personnel who oversaw the CTD's CXS and one of its units, the CAU, from 2003 to the present; current and former Deputy Assistant Directors (DAD) and Assistant Directors in the CTD; the former Executive Assistant Director of the FBI's National Security Branch; the FBI's Deputy General Counsel for the FBI OGC NSLB; an Assistant General Counsel assigned to the NSLB and other NSLB attorneys; several retired or former FBI officials; and the FBI General Counsel, Deputy Director, and Director.

In addition, we examined thousands of FBI documents and electronic records from FBI Headquarters and field divisions, as well as additional documents obtained through OIG administrative subpoenas served on the three communications service providers.

Our investigation also sought to determine whether any FBI personnel who signed or had supervisory responsibility for those who signed the exigent letters and made other informal requests violated any criminal laws or engaged in administrative misconduct or improper performance of official duties. To this end, we consulted with the Public Integrity Section of the Department's Criminal Division for a decision on whether the evidence warranted criminal prosecution. We provided to the prosecutor the evidence we gathered in our investigation, including transcripts of interviews, relevant documents, and e-mails. The Public Integrity Section declined prosecution of any individuals relating to the exigent letters matter.

With the assistance of the Department's National Security Division we also examined applications for pen register/trap and trace orders or electronic surveillance orders filed with the Foreign Intelligence Surveillance Court (FISA Court) that referred to telephone numbers listed in exigent letters or some of the blanket NSLs signed by CTD officials in 2006.[7] We examined these applications to determine if the supporting documents accurately characterized the means by which the FBI had obtained the subscriber or calling activity information it relied upon in seeking the orders.

---

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

We also served OIG administrative subpoenas on the three communications service providers to obtain copies of exigent letters, NSLs, administrative subpoenas, and other documents relevant to our investigation.

III. Organization of this Report

This report is divided into six chapters. Chapter Two describes in detail the circumstances in which the FBI used exigent letters and other informal requests to obtain telephone records from the three on-site communications service providers. This chapter also contains our analysis of each of these methods for obtaining telephone records and other calling activity information.

Chapter Three contains additional findings and analysis concerning how the use of exigent letters and other informal requests led to additional improper practices, including the acquisition of calling activity information regarding "hot numbers" without legal process; improper [redacted] and the acquisition of reporters' and news organizations' telephone toll billing records and other calling activity information; inaccurate statements to the FISA Court about the source of subscriber and calling activity information supporting applications for FISA Court pen register/trap and trace and electronic surveillance orders; and the improper use of FBI administrative subpoenas to cover records acquired from exigent letters or other informal requests.

Chapter Four contains our findings and analysis regarding the various corrective actions attempted by the FBI to address the use of exigent letters, including the issuance of 11 improper blanket NSLs. This chapter also describes steps taken by the FBI after the OIG's first NSL report was issued in March 2007 to address the use of exigent letters and other informal requests for telephone records. This chapter also contains our findings on the FBI's analysis of whether it will retain telephone records it acquired after issuing exigent letters or that were listed in the 11 blanket NSLs.

Chapter Five examines the FBI's management failures that led to these improper practices. It also evaluates the actions of individual FBI employees, including the CAU personnel who signed exigent letters; the CAU Unit Chiefs who supervised the unit; the senior CTD officials who signed 11 improper blanket NSLs; and attorneys in the FBI's Office of the General Counsel who provided legal advice relating to the exigent letters. In addition, this chapter examines the conduct of FBI and Department personnel who sought or acquired reporters' telephone toll billing records or other calling activity information without proper authority or approvals.

Chapter Six contains our conclusions and recommendations.

The appendix to the report provides examples of exigent letters signed by CAU personnel.

[PAGE LEFT INTENTIONALLY BLANK]

CHAPTER TWO
THE FBI'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS

This chapter details the FBI's use of exigent letters and other types of informal requests for telephone records. First, it provides background on the FBI's initial use of exigent letters in 2002 in connection with its criminal investigations of the September 11 hijackers, the migration of the practice to FBI Headquarters in 2003, and the FBI's contracts with Company A, Company B, and Company C to provide on-site support to FBI investigations. It describes the FBI's establishment of the Communications Analysis Unit (CAU), and the FBI's process for issuing exigent letters; the CAU personnel who signed them; and how the requests were initiated, drafted, approved, and documented.

This chapter also describes other practices by which CAU personnel requested and received telephone records from the on-site communications service providers without prior issuance of legal process or even exigent letters. These other informal methods included e-mail requests or oral requests. These informal requests also included what CAU personnel called "sneak peeks," which were requests without legal process to obtain information about whether calling activity existed for particular telephone numbers or subscribers, to obtain details about the calling activities, or to view records on the on-site providers' computer screens without obtaining the records themselves.

In addition, this chapter describes how the telephone records were analyzed by the FBI and uploaded into FBI databases. The chapter also describes FBI requests for a "community of interest" or "calling circle"

[redacted]

I. The Electronic Communications Privacy Act (ECPA)

To protect the confidentiality of telephone and e-mail subscriber information and telephone toll billing records information, the *Electronic Communications Privacy Act* (ECPA) states that communications service providers "shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service . . . to any

government entity."[8] The ECPA contains an exception to maintaining the confidentiality of such records by imposing a "duty to provide" responsive records if the Director of the FBI or his designee certifies in writing that the records sought are

> relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.[9]

During the period covered by our review, the ECPA and Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) authorized the use of national security letters (NSL) only during investigations of international terrorism or espionage upon the written request of a Special Agent in Charge or other specially delegated senior FBI official.[10] In order to open such investigations, the FBI must satisfy certain evidentiary thresholds, which are documented in FBI case files and approved by supervisors. If case agents want to issue NSLs, FBI policies require a 4-step approval process. Case agents must secure the approval of the case agent's supervisor, an Assistant Special Agent in Charge, the field office's Chief Division Counsel, and the Special Agent in Charge (or equivalent supervisors and attorneys at FBI Headquarters) who signs the NSL. FBI personnel authorized to sign NSLs are all members of the Senior Executive Service.

We concluded in our first NSL report that the CAU's use of exigent letters circumvented the ECPA NSL statute.[11] We found that neither the ECPA, the Attorney General's NSI Guidelines, nor FBI policy authorize the

---

[8] 18 U.S.C. § 2702(a)(3) (2000). In this report we refer to entities that provide electronic communication services to the public as "communications service providers" or the "providers."

[9] 18 U.S.C. §§ 2709(a) and 2709(b)(2) (2000 & Supp. IV 2005).

[10] The Attorney General's NSI Guidelines were consolidated with other Attorney General Guidelines into a new set of Attorney General Guidelines, referred to as the Attorney General's Consolidated Guidelines, which became effective on December 1, 2008. The new guidelines now govern the FBI's criminal investigations, national security investigations, and foreign intelligence investigations. However, these new guidelines did not alter the requirements for NSLs issued in national security investigations, which include investigations of international terrorism and espionage.

[11] OIG, NSL I, 95-98.

FBI to obtain ECPA-protected records by serving this type of informal letter prior to getting the records, with "legal process to follow."

In our first report, we noted that in limited circumstances, a separate provision of the ECPA authorizes the FBI to obtain non-content telephone records from communications service providers. From April 2003 through March 2006 – the period when most of the exigent letters were issued – the ECPA provision authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably believe[d] that an emergency involving immediate danger of death or serious physical injury to any person justifie[d] disclosure of the information."[12] However, for several reasons we did not agree with the FBI's after-the-fact argument that the exigent letters could be justified under this provision. In fact, senior CAU officials and FBI attorneys told us they did not rely at the time on the emergency voluntary disclosure provision to authorize the exigent letters, and we also found that the letters were sometimes used in non-emergency circumstances.[13]

II. Background on the FBI's Use of Exigent Letters

A. Origins of Exigent Letters in the FBI's New York Field Division

As described in our first NSL report, the FBI initiated a criminal investigation, referred to as PENTTBOM, immediately after the September 11, 2001, terrorist attacks. As a part of that investigation, the FBI arranged to have a Company A fraud detection analyst located on-site at the FBI's New York Field Division to assist in providing and analyzing telephone records associated with the September 11 hijackers and their associates.

---

[12] 18 U.S.C. § 2702(c)(4) (Supp. 2002). In March 2006, the provision was amended by the *USA PATRIOT Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act) to allow voluntary disclosure "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006).

[13] OIG, NSL I, 96-97.

1. The FBI's New York Field Division Contract with Company A

The analysis of telephone records associated with the September 11 hijackers and their associates became the primary responsibility of a newly created squad in the FBI's New York Field Division known as Domestic Terrorism 6, or DT-6. DT-6 developed close working relationships with several communications service providers due to the heavy volume of FBI requests for telephone records.

In early 2002, the New York Field Division, with the approval of FBI Headquarters, entered into a contract with Company A that provided for a Company A fraud detection analyst to be co-located with DT-6 to respond to the FBI's increased need for telephone records. To provide this support, the Company A analyst accessed Company A's telephone records databases from a computer work station installed for his use at the New York Field Division. The Company A analyst was able to respond immediately to FBI telephone records requests and also was available to respond to requests after normal business hours. According to an FBI Supervisory Special Agent (SSA) who worked in the New York Field Division, this arrangement proved to be highly beneficial to the FBI's ability to investigate terrorist threats and was soon used to support a wide variety of FBI counterterrorism investigations.

2. The New York Field Division's First Use of Exigent Letters

At first, the FBI obtained records from the on-site Company A analyst solely through grand jury subpoenas issued in the PENTTBOM investigation.[14] An SSA assigned to the DT-6 squad said this process was also facilitated by the co-location of several Assistant United States Attorneys (AUSA) at the FBI's New York Field Division's offices. As a result, FBI agents were able to quickly obtain grand jury subpoenas from the co-located AUSAs to serve on the Company A analyst prior to obtaining responsive records.

Eventually, the AUSAs left the New York Field Division's office space, and over time Company A [redacted]

[14] Since the PENTTBOM investigation was a criminal investigation, grand jury subpoenas were appropriate legal process by which to obtain non-content records from a communications service provider.

[redacted] The on-site Company A analyst told us that he therefore began to provide records in response to a letter from the FBI – called an "exigent letter" – which stated that exigent circumstances had prompted the request and that

> subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to Company A as expeditiously as possible.

According to the SSA who signed the first of these exigent letters in November 2002, the exigent letters were issued as "placeholders" to enable the FBI to secure the records promptly. However, the letters still committed the FBI to serve grand jury subpoenas on Company A after the records were provided, which the FBI did.

We identified a total of 37 exigent letters issued by the New York Field Division between November 2002 and April 2003.[15] The SSA who signed the first exigent letter and 11 other exigent letters issued on New York Field Division letterhead said that he signed these letters because he understood that the concept had been approved by Company A attorneys and he never thought about the legal authority for the letters. A Company A analyst told us that the exigent letter was drafted by someone in the FBI, and that Company A thereafter accepted the letters. However, we were not able to determine who initially drafted or approved the New York Field Division's use of these first exigent letters.

In 2002, the FBI reassigned several SSAs who had been working in the New York Field Division to temporary duty assignments at FBI Headquarters to help set up the CAU as a new unit in the FBI Headquarters' Counterterrorism Division (CTD). In 2003, one of the Company A analysts who had worked at the FBI's New York Field Division's offices was also reassigned to work in the CAU. The overlap in Company A personnel who worked in the New York Field Division and later at FBI Headquarters contributed to the migration of the exigent letter practice to FBI Headquarters in 2003.

---

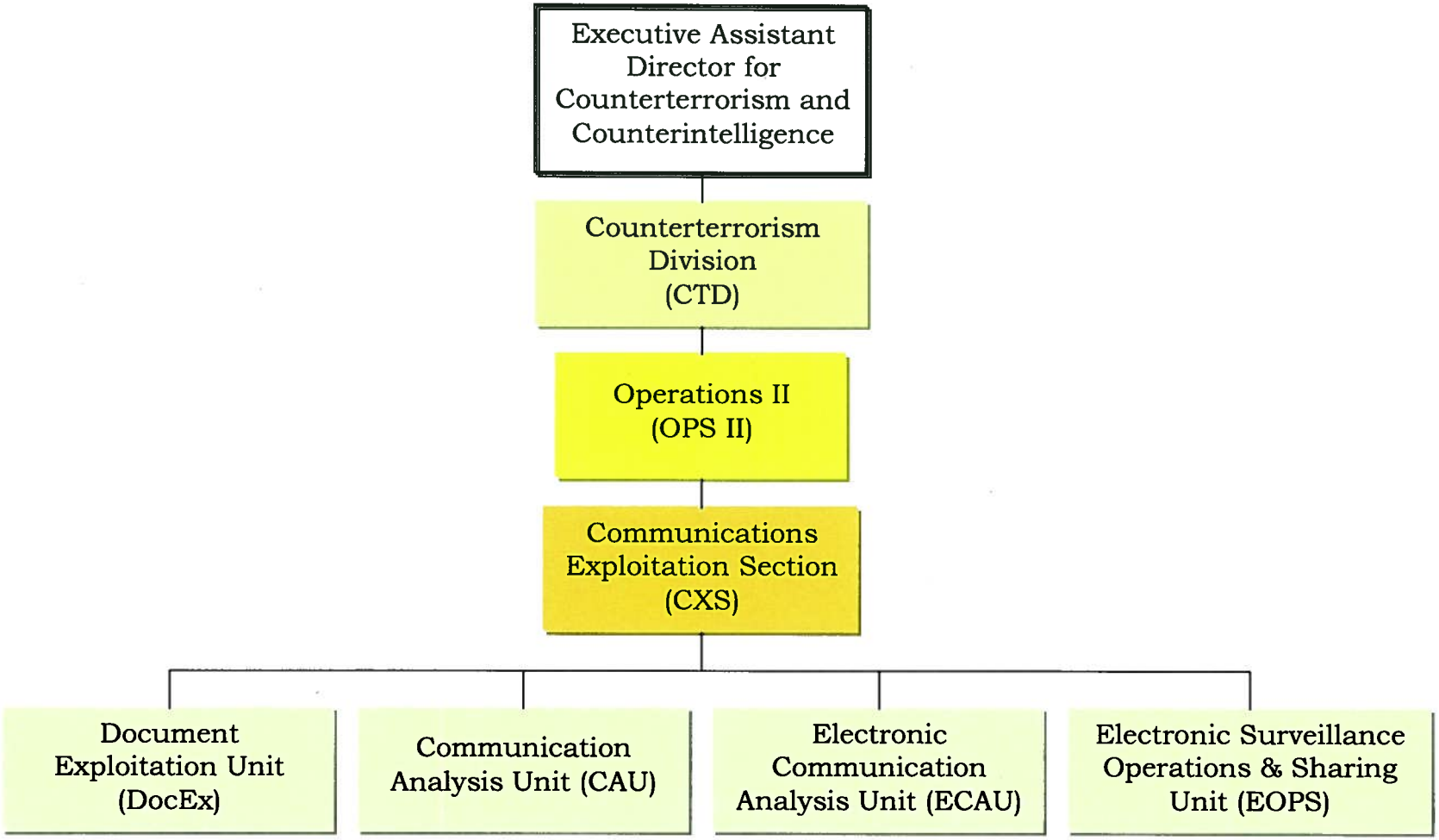
[15] New York Field Division personnel issued at least 20 additional exigent letters from October 2004 to September 2006. Although an SSA assigned to work in the New York Field Division estimated that he signed at least 50 to 60 exigent letters, the OIG identified only 19 exigent letters signed by this SSA. Based on this statement and other information developed in our investigation, we believe more exigent letters than the 798 we identified in our investigation were issued by the FBI. However, because of the FBI's inadequate record keeping practices, we could not determine how many more were issued.

B. The Work of the Communications Analysis Unit (CAU) and the FBI's Contracts with the Three Communications Service Providers

As part of a reorganization of the CTD following the September 11 attacks, the FBI created the Communications Exploitation Section (CXS) in 2002. The mission of the CXS was to support the FBI's investigative and intelligence missions by analyzing terrorist communications. As noted in Chart 2.1, one of the four units created within the CXS was the CAU.

CHART 2.1

Organizational Chart of Communications Exploitation Section



*The Document Exploitation Unit became the Digital Media Exploitation Unit (DMX) on March 26, 2006.

In 2003, the FBI entered into a contract with Company A pursuant to which a Company A analyst was located in the CAU's office space. The FBI also entered into separate contracts in 2003 with Company C and in 2004 with Company B to locate one of their analysts in the CAU's office space.

We determined that a CAU SSA issued the CAU's first exigent letter to the Company A analyst, then still located at the New York Field Division, on March 14, 2003. When the three communications service providers' employees were located in the CAU, CAU personnel issued similar exigent letters to these individuals. These exigent letters issued by CAU personnel were for the most part identical to the exigent letters issued by the New York Field Division in its criminal investigations after the September 11 attacks. As described below, we determined that from March 14, 2003, through November 13, 2006, CAU personnel issued a total of 722 exigent letters to the 3 on-site communications service providers.

1. The CAU's Mission and Organizational Structure

The CAU's mission is to analyze telephone communications and provide actionable intelligence to the appropriate operational units in the FBI.[16] The CAU was established as an "operational support unit" rather than an operational unit. Under FBI internal policy, as operational support components, neither the CXS nor CAU personnel could initiate national security investigations or sign NSLs.

From 2003 through 2006, the CAU was organized into teams, each of which was led by an SSA and included other SSAs, Supervisory Intelligence Analysts, Intelligence Analysts, and Technical Information Specialists. Each team supported specific FBI field and Headquarters operational divisions, legal attachés, and classified special projects.

Following its establishment in late 2002, the CAU initially was supervised by Acting Unit Chiefs. Two SSAs served as the Acting Unit Chiefs from September 2002 to March 2003. In March 2003, Glenn Rogers was appointed as the first permanent CAU Unit Chief.

---

[16] The CAU's mission was described in a January 6, 2003, FBI Electronic Communication (EC). This EC, which was drafted by the CAU's Acting Unit Chief and sent to all FBI divisions, described the CAU's mission:

> CAU facilitates the prevention and prosecution of international and domestic terrorism activities through the relevant collation, incisive analysis, and timely dissemination of high-quality intelligence identified through telephone calling activity.

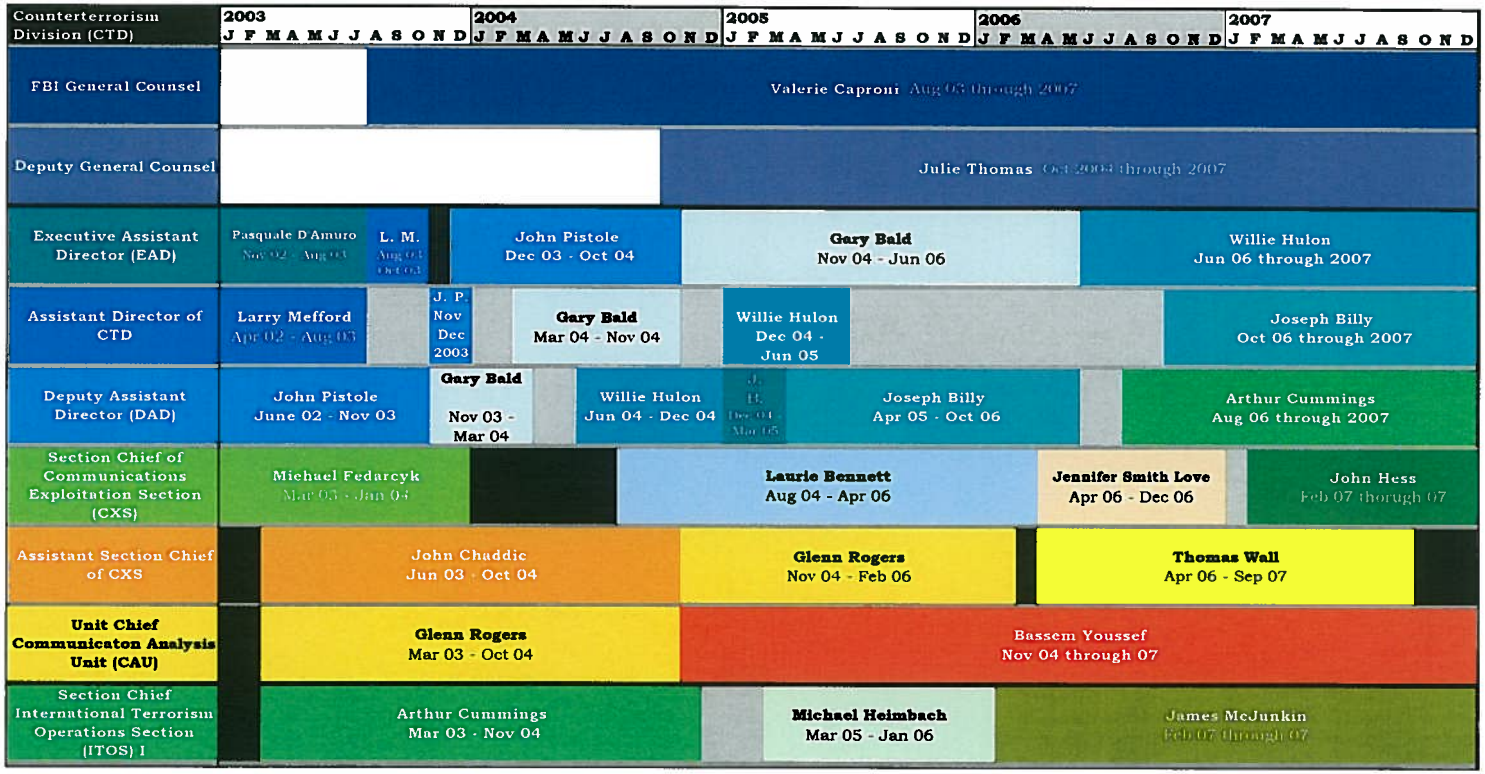
In November 2004, Rogers was promoted to Assistant Section Chief for the CXS.[17] Bassem Youssef succeeded Rogers as the CAU Unit Chief and remained the CAU's Unit Chief throughout the period covered by our review.

Chart 2.2 shows the personnel who held key positions in the FBI's senior leadership, the FBI Office of the General Counsel (FBI OGC), and the Counterterrorism Division during the period covered by our review.

[17] Rogers retired from the FBI in November 2006.

CHART 2.2

FBI OGC, Senior Leadership, and Counterterrorism Division Officials Management (2003 through 2007)



Acting Data NOT Provided **L.M.** = Larry Mefford **J.P.** = John Pistole **J.B.** = James Bernazzani

We interviewed 15 SSAs and 10 Intelligence Analysts who were assigned to the CAU beginning in March 2003. They stated that their duties consisted chiefly of responding to requests from field divisions, legal attachés, and operational Headquarters units. These requests included asking the CAU to obtain and analyze telephone numbers related to ongoing FBI investigations and to report back to the requester with telephone records and analysis.

CAU personnel analyzed the telephone numbers by obtaining information from numerous databases and other resources, including information from the three on-site communications service providers. One SSA from a CTD operational unit who frequently requested CAU support characterized the CAU's role as having "a phone database on steroids; to identify 'good' versus 'bad' numbers; to provide [redacted] charts and analysis; and to get numbers in a usable format for the field."

Nearly all of the 15 SSAs we interviewed who worked in the CAU told us that when they arrived at the CAU they had little or no experience in national security investigations.[18] In addition, all but 2 of the 29 FBI employees we interviewed who were assigned to work in the CAU said they had limited or no prior experience working with NSLs. None of the SSAs we interviewed said that the FBI provided them training on the legal and internal FBI requirements for issuing NSLs until after the OIG's first NSL report was issued in March 2007.[19]

2. Terminology Used in this Report for Non-Content Telephone Transactional Records

As described above, the ECPA generally prohibits communications service providers from divulging "a record or other information pertaining to a subscriber to or a customer of" their services.[20] However, in authorized

---

[18] Virtually all of these SSAs had extensive experience in conducting or supporting criminal investigations, which were governed by a different set of Attorney General Guidelines than the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), which applied to the conduct of national security investigations.

[19] In response to the OIG's recommendations in our first NSL report, the FBI is now providing mandatory NSL training to FBI employees involved in the use of NSLs. This training, as well as the NSL guidance and other corrective actions implemented by the FBI and the Department in response to our first NSL report, is described in Chapter Four of our second NSL report.

[20] 18 U.S.C. § 2702(a)(3).

international terrorism and espionage investigations, the ECPA created an exception to this general prohibition, which allows the FBI to request "the name, address, length of service, and local and long distance toll billing records of a person or entity" upon written certification by the FBI Director or his designee that the records sought are relevant to an authorized international terrorism investigation, provided that any investigation of a United States person "is not conducted solely on the basis of activities protected by the first amendment."[21]

In this report we generally use the term "toll records" to refer to the non-content records of telephone calls that the three communications service providers provided to the FBI in response to exigent letters and other informal requests.[22]

Toll records in this context are the date, time, duration, and the originating and terminating numbers to a telephone call. These records are also sometimes referred to as "transactional" records, as distinguished from the content of telephone calls. The FBI is not authorized to collect the content of any telephone calls through NSLs.

3. FBI Contracts with the Three Communications Service Providers

In 2003 and 2004 the FBI entered into contracts with three communications service providers requiring the communications service providers to place their employees in the CAU's office space and to give these employees access to their companies' databases so they could immediately service FBI requests for telephone records.[23] These employees were also on call to the FBI after business hours. The contracts required

---

[21] 18 U.S.C. § 2709(b)(1).

[22] FBI personnel and employees of the on-site communications service providers sometimes referred to these records by using other industry terms such as "call records," "call detail records," "calling activity information," or "tolls." In addition, the terminology used in the contract documents to describe records provided to the FBI by the communications service providers varied, and there were some differences among the three providers as to the types of records available to the FBI. Accordingly, while we generally use the term "toll records," we use other terminology when quoting from contract documents or witness interviews.

[23] During the period covered by our review, Company B and Company C each assigned one full-time employee to service their respective contracts with the FBI. Company A rotated four analysts through two full-time positions.

the providers to deliver the toll records to the FBI in a specific electronic format that was compatible with the FBI's databases.[24]

CTD officials told us that the ability to have requests for toll records serviced immediately by the communications service providers and to receive the records in an electronic format that could be immediately uploaded into FBI databases improved the CAU's ability to support FBI counterterrorism investigations in a timely fashion. A CTD memorandum requesting approval to obligate funds for the contract with Company A described the contract as providing for "near real-time servicing" of legal process by Company A analysts.

In 2003, the FBI entered into a contract with Company A. Pursuant to its contract, Company [redacted][25]

Company A documents also stated that [redacted]

In addition to providing toll records, the Company A analysts could [redacted] the telephone toll data for the FBI.[26] According to the Company A

[24] A May 28, 2003, EC from the CAU described problematic delays with toll records received through conventional channels that were "often via hard copy reports that had to be retyped into FBI databases."

[25] [redacted]

[26] Company B and Company C did not perform [redacted] of the records they provided to the CAU.

employees, the types of [redacted] that Company A analysts performed for the FBI were: (S)

- [redacted] community of interest [redacted] (described later in this chapter), when requested;
- alerting CAU requesters if the Company A analysts noticed that the data reflected indicators that might make it a priority (such as calls to or from a [redacted]);
- evaluating telephone data to eliminate unnecessary follow-up on telephone numbers that were of no investigative value; and
- preparing visual presentations such as [redacted] charts showing communication [redacted] between telephone numbers of interest.

The FBI's contract with Company A significantly exceeded the scope of the services that were provided to the FBI by Company B and Company C. From 2003 to March 2007, the FBI paid Company A more than [redacted] under this contract.

In 2003, the FBI entered into a contract with Company C under which an on-site Company C employee assigned exclusively to service the CAU's requests provided toll records to the FBI on an expedited basis. From April 2004 to September 2008, the FBI has paid Company C over [redacted] under this contract. Similar to the Company A contract, the Company C [redacted] In addition, the on-site Company C employee told us that he could provide to the FBI subscriber data, which consisted of names and addresses of Company C customers. Company C's contract proposal stated that it would maintain [redacted] of telephone data storage.[27]

In 2004, the FBI entered into a contract with Company B, under which Company B agreed to provide the CAU with the same types of records it would provide to the FBI in response to an NSL. These records included: (1) subscriber and billing information, which included telephone numbers

---

[27] The on-site Company C employee told us in 2007 that in some instances Company C could provide records [redacted]

and subscriber names and addresses for both listed and non-published numbers; and (2) calling records for numbers dialed long distance, collect, or third party and, if available, local calls and calling card information. The Company B contract provided for making records available [redacted] As of March 2007, the FBI had paid Company B more than [redacted] under this contract.

In most instances, the toll records delivered by the three communications service providers to the FBI consisted of the originating and terminating telephone numbers and the date, time, and duration of the telephone calls. In addition, Company A and Company C could provide the [redacted]

Company A did not provide subscriber data as part of its services under its contract with the CAU.[28] Companies B and C were able to, and sometimes did, provide the CAU with subscriber data for their customers. However, the FBI typically did not obtain subscriber data from Companies B and C.

Glenn Rogers, the CAU's Unit Chief from March 2003 to November 2004, told us that a significant reason for the three contracts was the speed with which the on-site employees of the three communications service providers could respond to the CAU's requests.

Documents associated with the Company A and Company C contracts described additional resources and capabilities of the on-site providers, some of which were relevant to our review. For example, Company A's description of its capabilities in a March 2004 contract proposal stated that its database could "be customized specifically for the FBI based upon input data such as hot target list, significant numbers, secure data, etc." This contract proposal also referred [redacted] "Community of Interest." Company C's cost assessment proposal, dated May 23, 2003, stated that Company C [redacted] The FBI's Electronic Communication (EC) seeking approval to obligate funds for the Company C

[28] The on-site Company A employees told us that they referred FBI personnel seeking subscriber information to a Company A subpoena management centers.

contract in 2003 noted that the statement of work for the contract would allow for [redacted][29]

As described in Chapters Three, Four, and Five of this report, we found that the only FBI attorneys who reviewed the three contracts prior to late 2006 were FBI OGC attorneys who specialized in procurement law. Marion Bowman, who served as Deputy General Counsel for the FBI OGC National Security Law Branch (NSLB) when the contracts were executed, told us that he was unaware of and never reviewed the contracts. Julie Thomas, who was the NSLB Deputy General Counsel from October 2004 until December 2008, told us that she first reviewed the contracts in late 2006 after she reviewed a draft of the OIG's first NSL report.

4. Location of the Three Communications Service Providers

From April 2003 through January 2008, employees of one or more of the three communications service providers were located in the CAU's office space. The CAU's office space was arranged in an open manner, with no walls or partitions to set these employees apart from CAU personnel. The work stations for the providers' employees consisted of a desk, at which the employee had access to an FBI computer, an FBI telephone, and a separately networked computer that provided access to the records of the communications service provider. These work stations were located nearest the entry door to the CAU and were immediately adjacent to the CAU Unit Chief's office. The work stations of CAU's SSAs and Intelligence Analysts were located further inside the CAU's suite. All of the work stations in the CAU's suite, including the work stations for the three communications service providers, were integrated in one common area.

The FBI issued FBI e-mail accounts to employees of the three communications service providers for their use at the FBI. The providers' employees also had access to the CAU computer share drive.[30] The FBI e-mail accounts enabled them to communicate with FBI employees inside

---

[29] As described later in this chapter, we believe that the FBI's community of interest [redacted] practices were inappropriate under the ECPA and FBI policy. Further, as described in Chapter Three of this report, we found that, pursuant to the FBI's contracts with Company A and Company C, the FBI improperly obtained ECPA-protected calling activity information through the use of hot number [redacted]

[30] Employees from Company A and Company B told us that they accessed the CAU's share drive to review the exigent letter template because they were often asked about the template by FBI personnel who wanted to request records.

and outside the CAU. The providers' employees also communicated [redacted] As described below, many requests for telephone records were conveyed to the communications service providers through e-mails sent on the FBI e-mail accounts.

5. Relationship between CAU Personnel and the Providers' Employees

We found that the on-site providers' employees regularly attended CAU unit meetings and were treated by CAU personnel as "team" members. This team identification also was evidenced by the on-site employees' e-mail communications. When the FBI established FBI e-mail accounts for the providers' employees, one of the Company A analysts created a folder entitled "TEAM USA," and many of his outgoing e-mails began with a greeting to "Team," or "Team CAU."[31] CAU personnel and the on-site providers also socialized outside the office such as at "happy hour" celebrations for CAU SSAs who were transferring out of the unit.

To some degree, the collegial relationship between the providers' employees and CAU personnel fostered a productive working relationship. If the FBI had properly trained its personnel on the lawful methods for obtaining telephone records from the on-site providers and if the interactions between CAU personnel and the providers' employees were properly supervised, our observations about the team identity and informal social interactions would not be remarkable. However, we found that the proximity of the on-site providers' employees to CAU personnel, combined with the lack of guidance, supervision, and oversight of their interactions with FBI employees (which we discuss in Chapters Three and Four of this report), contributed to some of the serious abuses identified in this review.

III. Exigent Letters Issued by CAU Personnel

We determined that CAU personnel issued at least 722 exigent letters to the 3 on-site communications service providers from March 14, 2003,

---

[31] One on-site Company A analyst signed his e-mails with the following signature block: [Name], CTD/FBIHQ, Communications Analysis Unit.

through November 13, 2006, the date of the last exigent letter that we found.[32]

Table 2.1 shows the number of exigent letters we identified as issued by the CAU from 2003 through 2006.

TABLE 2.1

Exigent Letters Issued by CAU Personnel by Calendar Year (2003 through 2006)

CALENDAR YEAR	NUMBER OF EXIGENT LETTERS
2003	70
2004	323
2005	294
2006	35
TOTAL	**722**

Source: Company A, Company B, and Company C

Most of these letters were identical to the exigent letters that were first issued by the New York Field Division beginning in November 2002, discussed above.

Table 2.2 shows the number of exigent letters CAU personnel issued to each of the three communications service providers during the 4-year period.

TABLE 2.2

Exigent Letters Issued by CAU Personnel to the Three On-Site Communications Service Providers (2003 through 2006)

COMMUNICATIONS PROVIDER	NUMBER OF EXIGENT LETTERS
Company A	514
Company B	146
Company C	62
TOTAL	**722**

Source: Company A, Company B, and Company C

[32] As described below, the use of exigent letters that promised future legal process was formally barred (in a directive issued by the FBI's Deputy Director) in March 2007, when the OIG issued our first NSL report.

In addition to the CAU personnel who signed these 722 exigent letters, from 2002 to 2006, 76 other exigent letters were signed by FBI personnel not assigned to the CAU. Fifty-eight of these exigent letters were signed by FBI personnel assigned to the FBI's New York Field Division. The remaining 18 exigent letters were signed by FBI personnel in FBI Headquarters and field divisions who told us they learned about CAU's resources either through briefings, previous assignment in the CAU, or their own initiative. Because exigent letters were primarily issued by the CAU, however, our review focused on the CAU's use of the 722 exigent letters and other informal methods of obtaining non-content telephone records from the on-site providers, rather than the use of exigent letters by other FBI offices.

A. Text of the CAU Exigent Letters

The 722 CAU exigent letters were all drafted on official FBI letterhead. All but 17 of the 722 exigent letters signed by CAU personnel contained the following two sentences:

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

Of the 17 exigent letters that did not contain this language, 11 promised a follow-up NSL rather than a subpoena, 2 promised to follow up with either a subpoena or an NSL, and 4 did not mention any follow-up legal process. The appendix to this report includes examples of two exigent letters issued by CAU personnel during the period covered by our review.

Of the 722 exigent letters, 75 specified in either the body of the letter or in an attachment to the letter the types of records sought – either toll billing or subscriber records, or both. Most of the other exigent letter requests included only the generic request for "records" quoted above.

Some of the 722 exigent letters also instructed the recipient to conduct a "community of interest" or "calling circle" [redacted] A community of interest [redacted]

[redacted][33]

Some of the 722 exigent letters also had an attachment listing various categories of records requested, such as subscriber information, [redacted] data, and community of interest reports. However, we found that, as with the case with NSLs that had similar attachments, the FBI did not consistently obtain all records listed on the attachments to the exigent letters.

Of the 722 exigent letters issued by the CAU, only 77 letters included the date range for the request, which ranged [redacted] Several CAU SSAs and intelligence analysts told us that they sometimes requested whatever records the communications service provider had on a particular telephone number, regardless of the time period.

In addition, employees of the on-site communications service providers told us that CAU requesters would often come to their work stations and tell them the specific records they needed and the date parameters for their requests. When they did so, CAU personnel sometimes provided exigent letters to cover the request at that time or at a later time if responsive records were located. For example, we reviewed entries in the on-site Company C employee's log in which he noted references to [redacted] requested. However, the log also noted that the Company C employee only needed an exigent letter for those instances in which he located responsive records, not for all [redacted] he [redacted]

B. Counterterrorism Division's and CAU's Recognition of the Use of Exigent Letters

The first document we identified relating to the FBI's ability to obtain telephone records from the three on-site communications service providers without first serving legal process was a January 6, 2003, EC from the Acting Unit Chief of the CAU that was distributed to all FBI divisions.[34] It described the CAU's mission and processes, and stated that the CAU could obtain telephone records in "exigent circumstances" and that "[a]ppropriate legal authority (Grand Jury subpoena or NSL) must follow these requests."

---

[33] We describe community of interest requests in more detail below.

[34] This EC predated the contracts between the FBI and the three communications service providers.

This EC was approved by the CXS's Section Chief, the CTD's Deputy Assistant Director, and the CTD's Assistant Director. The EC made no explicit reference to exigent letters.

The first EC we identified that mentioned exigent letters was an EC to CAU personnel dated November 18, 2003, approved by CAU Unit Chief Glenn Rogers. The EC described how CAU personnel processed records received from the on-site Company A analyst in response to exigent letters. The EC stated:

Neither the CTD nor the CAU EC provided guidance regarding the circumstances in which these exigent letters were appropriate.

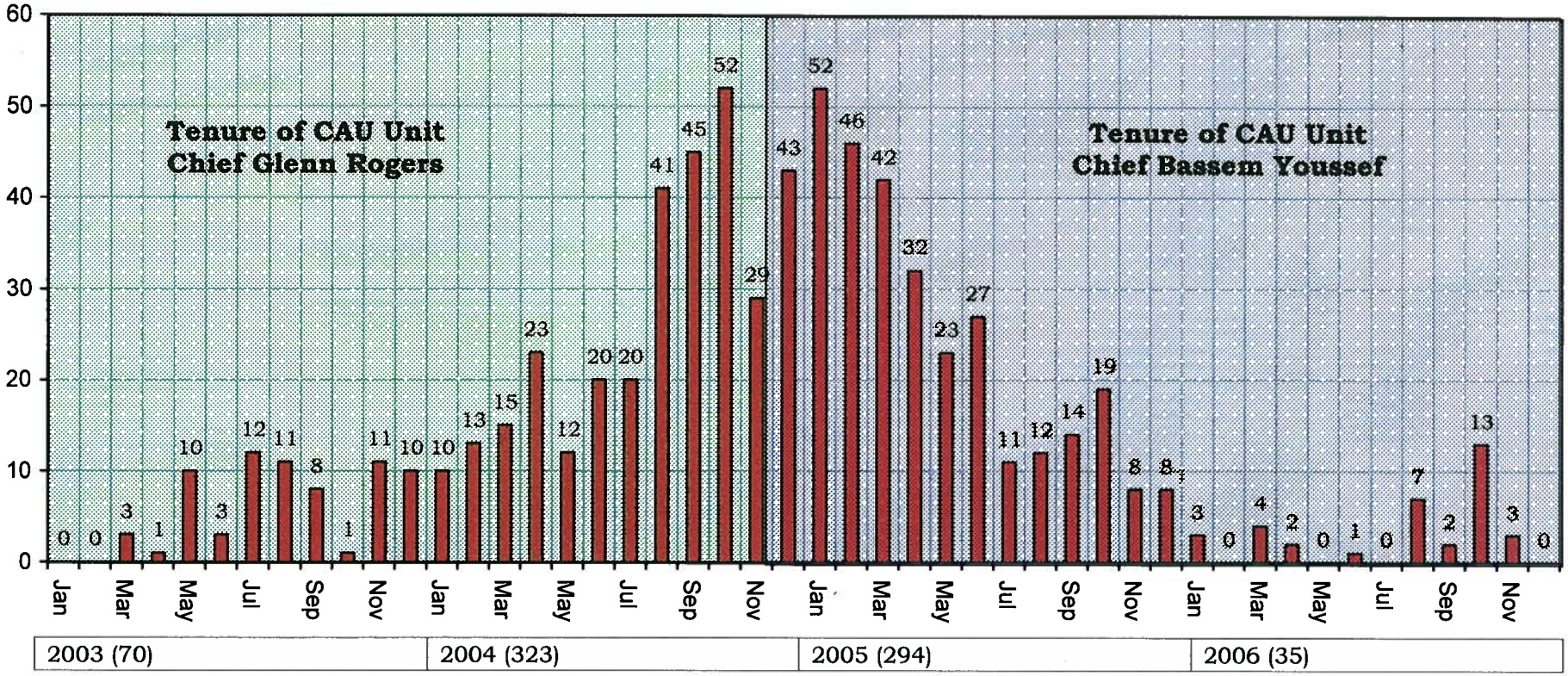
C. CAU's Exigent Letters Practice

This section provides further details on the exigent letters used by CAU personnel and their explanations for issuing these letters.

Of the 722 exigent letters issued by CAU personnel from March 14, 2003, through November 13, 2006, 1 was signed by an Assistant Section Chief, 12 were signed by 2 CAU Unit Chiefs, 706 were signed by 15 SSAs, and 3 were signed by 3 Intelligence Analysts.

CHART 2.3

Exigent Letters Issued by CAU Personnel to the Three On-Site Communications Service Providers (2003 through 2006)



Rogers, the CAU's first permanent Unit Chief, acknowledged to us that he was aware of and approved the use of exigent letters. He said that before he became the CAU Unit Chief in March 2003 he did not know about exigent letters. He said he first learned about exigent letters from an on-site Company A analyst on May 27, 2003, while the CAU was working on an investigation of a bomb threat.[35] Rogers said that the Company A analyst told him that exigent letters had been previously approved by Company A and government attorneys for use in the New York Field Division for emergency situations. Rogers said he was not sure whether the attorneys referred to by the Company A analyst were from the FBI's New York Field Division or possibly from the U.S. Attorney's Office. Rogers said he did not seek any further details about the identity of any FBI attorneys who may have approved the use of exigent letters.

Rogers said that based on what the Company A analyst told him about the prior use of exigent letters by the New York Field Division, he signed the exigent letter that requested records for four telephone numbers in the bomb threat matter. We determined that Rogers personally signed 10 more exigent letters while serving as the CAU's Unit Chief and 1 exigent letter after he was promoted to Assistant Section Chief for the CXS in November 2004. In addition, we identified a total of 355 other exigent letters that were issued by CAU personnel, listing 1,375 telephone numbers, while Rogers was the CAU Unit Chief.[36]

Rogers acknowledged that he was responsible for the use of exigent letters at the CAU. He said that he never established any unit policy for the use of exigent letters, and he provided only very general verbal guidance to CAU employees. Rogers stated that he told CAU personnel that if requesters "state that it's exigent," or "have circumstances they describe as 'exigent' and they promise the grand jury subpoena or NSL," then the exigent letter was authorized. Rogers said that incoming CAU employees usually learned about exigent letters when they received on-the-job training from more senior CAU employees.

---

[35] We determined that after Rogers became the Unit Chief in March 2003, CAU personnel issued eight exigent letters, dated between May 14 and May 27, 2003, that had Rogers's name typed in the signature block. The first exigent letter Rogers signed was dated May 27, 2003.

[36] The 1,375 total includes some duplicate telephone numbers. We identified 15 telephone numbers that were listed on exigent letters sent to more than one of the on-site providers.

Rogers distinguished exigent letters from the FBI's so-called "Patriot Act" letters requesting voluntary disclosure pursuant to the ECPA emergency voluntary disclosure provision.[37] Rogers told the OIG that he had used "Patriot Act letters" to obtain voluntary disclosures in other circumstances, and that the exigent letters used by the CAU were not Patriot Act letters. He said that exigent letters were used for "something that was not routine and needed immediate attention. When asked whether he was referring to instances in which there was an emergency that involved a threat of immediate death or serious injury, he responded, "No, no it just meant . . . that these were rapidly moving events . . . that required immediate attention."

Rogers told us that he was aware from the time he first learned about exigent letters from the on-site Company A analyst that follow-up legal process would be required whenever exigent letters were used. Rogers told us that he regularly reminded CAU personnel who issued exigent letters to stay current on securing the after-the-fact legal process owed to the providers. He also said he sometimes spoke with personnel assigned to CTD operational units and at least one field division about the importance of issuing after-the-fact legal process. Rogers asserted that he regularly checked with CAU personnel and with the on-site providers' employees to ensure that the after-the-fact legal process was being provided.

In November 2004, Rogers was promoted to be Assistant Section Chief of the CTD's Communications Exploitation Section (CXS), and Bassem Youssef was appointed as the CAU Unit Chief replacing Rogers. Youssef signed 1 exigent letter, and, while he was the CAU Unit Chief, 367 exigent letters listing 2,046 telephone numbers were issued under his name.[38]

---

[37] "Patriot Act letters" was the name FBI personnel used to refer to letters requesting emergency disclosure pursuant to the ECPA. As noted previously, from April 20, 2003, to March 8, 2006, 18 U.S.C. § 2702(c)(4) authorized a provider to voluntarily release customers' records to a governmental entity if the provider "reasonably believe[d] that an emergency involving immediate danger of death or serious physical injury to any person justifie[d] disclosure of the information." As discussed in Chapter Four, the FBI issued detailed guidance in August 2005 concerning the FBI's authority to request emergency voluntary disclosures.

[38] Company A records show that the CAU issued 11 exigent letters to Company A in 2006 and a total of 239 exigent letters to Company A during Youssef's tenure as CAU Unit Chief. We identified 367 exigent letters issued under Youssef's name as CAU Unit Chief and 1 signed by him.

The total of 2,046 telephone numbers in the 367 exigent letters includes some duplicate telephone numbers. We identified 97 telephone numbers that were listed on exigent letters sent to more than one of the on-site providers. We also identified 224 (Cont'd.)

Youssef told us that when he became the CAU Unit Chief he inherited the exigent letter practice from Rogers and that since Rogers was still his immediate supervisor as the Assistant Section Chief of CXS, Youssef felt he was not in a position to change the exigent letters practices then in place.

We asked Youssef about the one exigent letter he personally signed in November 2005. He stated that when he signed the letter he was unaware that the exigent letter he signed referred to an after-the-fact grand jury subpoena instead of an NSL, and he told us that it was not until April 2006 that he closely reviewed any exigent letter and learned of the reference to subpoenas.

CAU SSAs told us that most of the exigent letters signed by CAU personnel related to international terrorism investigations.[39] As discussed in Chapter Four of this report, the FBI has determined that a majority of these record requests were covered by NSLs, not by grand jury subpoenas.

The on-site providers' employees told us they were concerned only that the requests were followed up by some legal process – subpoenas or NSLs – and did not care about what type of process the letter promised.

The on-site providers' employees also told us that they sometimes generated the exigent letters themselves and gave them to CAU personnel to sign and provide back to them. One of the Company A on-site analysts told us that to facilitate his preparation of exigent letters for the FBI to use, he established a short-cut in the form of an icon on his FBI-issued computer desktop that enabled him to quickly generate exigent letters, which he gave to the CAU employees to sign.[40]

---

additional telephone numbers that were submitted to the same provider on multiple exigent letters.

[39] These statements by CAU SSAs were confirmed by the FBI's review team that researched, under the direction of the FBI OGC, all of the telephone numbers in exigent letters and 11 blanket NSLs in order to determine whether the FBI will retain records. As described in detail in Chapter Four of this report, the review team determined that nearly all of the 4,379 telephone numbers were relevant to national security investigations, while 266 were relevant to criminal or domestic terrorism investigations.

[40] None of the employees of the three on-site communications service providers or any FBI employees we interviewed said they could estimate the total number of exigent letters prepared by the three providers.

For much of the period when exigent letters were used, we found that there was no written guidance for CAU personnel regarding the circumstances under which exigent letters could be used. We found that there was only a general understanding among CAU employees that there had to be "exigent" or emergency circumstances for them to use an exigent letter. We also found that there was no process whereby a supervisor reviewed and approved the issuance of the exigent letters. Further, there was no requirement to document the circumstances under which the exigent letters were issued or the investigation to which the requested telephone number was related. In fact, CAU personnel were not even required to retain copies of the exigent letters and, as described below and in Chapter Four, for the most part were not required to track or otherwise account for the exigent letters issued to the on-site communications service providers.

1. Signers of Exigent Letters in the CAU

We determined that three SSAs assigned to the CAU from 2003 to 2005 signed nearly 50 percent of the 722 exigent letters issued by CAU personnel. One of these 3, an SSA who signed 139 exigent letters, told us that the communications service providers' employees often gave him exigent letters to sign after he had already been given the requested records – and he simply signed the letters. This SSA also said that while he realized the exigent letters inaccurately stated that grand jury subpoenas had been submitted, he signed the letters because he "thought it was all part of the program coming from the phone companies themselves," and he assumed the letters were approved by the communications service providers' attorneys. This SSA said that each time he issued an exigent letter, it was in response to a request from a field division or headquarters unit for records, and he believed that exigent circumstances were present.

Another SSA, who signed 115 exigent letters, said he learned about the letters from the same Company A analyst who initially had told Rogers about the letters. This SSA said the Company A analyst told him that the letter had been approved for use by both Company A and FBI OGC attorneys. The SSA said he went to Rogers and asked about the exigent letters, and Rogers told him that they were "standard operating procedure." This SSA also said that he knew that subpoenas had not been requested but signed the exigent letters anyway, based on the assurances of the Company A analyst and Rogers as well as his awareness that the letters were a standard practice in the CAU when he began his assignment there in September 2003. The SSA said that while most of the exigent letters he signed related to counterterrorism investigations, some were related to criminal and counterintelligence investigations. He also told us that in some instances, due to the exigent nature of the request, he did not believe there were open investigations when he issued an exigent letter.

A third SSA, who signed 98 exigent letters, said he learned of exigent letters from the Company A analyst shortly after he arrived at the CAU in September 2003. The SSA said he read the exigent letter but was not concerned with the reference to a subpoena being requested from the U.S. Attorney's Office. He said he assumed that the letter was a legitimate document because he saw other CAU personnel using exigent letters. The SSA also said that at one point either Rogers or a Company A analyst told him not to change the language in the exigent letter because attorneys for both Company A and the FBI had already agreed to the wording. This SSA told us that exigent letters were typically prepared by employees of the on-site communications service providers, who would forward the exigent letters to him by e-mail for his signature at the same time they furnished him the requested telephone data.[41] He said that on other occasions one of the intelligence analysts on his team would prepare the exigent letters. The SSA told us that he was not concerned with whether an incoming request was made pursuant to an open FBI investigation, because a case would eventually be opened even if it lagged behind the exigent letter process.

This SSA also told us that he used exigent letters only under exigent circumstances and that he would not sign his name to letters containing false statements. When we asked him about the inaccurate statements in the exigent letters that subpoenas had been submitted to the U.S. Attorney's Office, he said the language "did not make sense" since that language did not reflect how the process to obtain records and to issue after-the-fact legal process actually worked in the CAU. Yet, although he said he thought at the time that the language in the exigent letters did not make sense, he said he nevertheless signed the letters because he thought the letter was accepted by the providers and was an established practice in the CAU. He said his overriding concern was the fear that "something would blow up in the U.S." if he did not aggressively respond to requests for telephone data in support of FBI terrorism investigations.

While most SSAs told us they believed exigent circumstances were present when they signed the letters, we found contrary evidence regarding some of these letters. For example, an SSA who signed 34 exigent letters told us that he was "pretty sure" that some of the exigent letters he signed when he first joined the CAU "could be questionable" in terms of whether there were exigent circumstances. Another SSA who signed 61 exigent letters said that Intelligence Analysts on this team would sometimes describe the situations prompting the requests, but if he was busy, "they'll

---

[41] Other CAU personnel, documents, and e-mails confirmed that telephone records were often provided to the FBI before exigent letters were issued.

just hand me the letter, and . . . I'll sign it." We also identified an e-mail dated April 26, 2005, in which an FBI OGC National Security Law Branch (NSLB) Assistant General Counsel (the Assistant General Counsel) who was the NSLB point of contact for NSL-related policies and issues, expressed to Youssef that "on occasion, CAU is presuming that someone who comes to them [seeking records from the on-site providers] has an emergency."

The CAU SSAs who signed exigent letters gave us various descriptions about the matters for which exigent letters were used. Some said an exigent circumstance involved a life-threatening matter. Others described it as an important, pressing, or high-priority matter. Others said it was a matter related to an important case or one in which a high-level FBI official demanded the information.

Most of the CAU SSAs and Intelligence Analysts who signed exigent letters also said they were unconcerned about the letters' reference to subpoenas. Some SSAs asserted that they broadly read the reference of subpoenas in the exigent letters to include grand jury subpoenas, administrative subpoenas, or NSLs. One SSA stated that "for me everything was a subpoena." Other SSAs stated that they were unaware of the type of legal process that would follow because it was the responsibility of the FBI requester, not CAU personnel, to follow up with appropriate process. A few signers, including Youssef, told us that they did not closely read the exigent letters when they signed them.

Almost all of the SSAs who signed exigent letters told us that they did not give much thought to the underlying legal authority for the exigent letters. Rather, they said that they assumed the exigent letter was a legal instrument that had been reviewed by the appropriate authorities, including CTD management and attorneys from both the FBI and from the communications service providers. They stated that they used the exigent letters because they assumed that the letter was an authorized tool for requesting records from the on-site communications service providers. For example, one SSA stated that exigent letters were the "business process" in place when he came to the CAU.

CAU Unit Chief Glenn Rogers (who later served as Assistant Section Chief of the Communications Exploitation Section (CXS), which supervised the CAU) told us that he signed exigent letters even though he recognized at the time that subpoenas requesting the records had not been submitted to the U.S. Attorney's Office, as the letters stated. When we asked Rogers to explain this statement in the exigent letters, Rogers said that the exigent letter was "poorly worded" and should have been revised earlier to state that NSLs would be the after-the-fact legal process to be served on the providers. Rogers also stated that nothing was done "to hide the fact that we were

getting stuff in advance of NSLs" and that "nobody ever told me to cease" using exigent letters.

We found that the practice of obtaining records and providing after-the-fact legal process was so common in the FBI that it was mentioned in a CTD training video created in 2004. In the video, a CAU SSA speaks with a field agent by telephone and makes arrangements to provide telephone records that the SSA had already received from a communications service provider. The SSA says to the field agent, "I'll just need you to send me an NSL to cover the books."

As discussed in Chapter Three of this report, we found other irregular practices concerning the CAU's interaction with the on-site providers. One of our findings in that chapter has a bearing on the issue whether signers of exigent letters knew that exigent circumstances were present. In one of three instances involving subpoenas or other requests for the toll billing records of news reporters, a CAU SSA signed an exigent letter seeking toll billing records for reporters for the Washington Post and The New York Times. Yet, the case agent told us he did not inform either the CAU SSA who signed the exigent letter or anyone in his management chain that exigent circumstances existed. Similarly, the CAU SSA said he did not recall anyone informing him that exigent circumstances were present.

None of the CAU SSAs or Intelligence Analysts who signed the exigent letters received training on NSLs upon entering the CAU. In addition, these SSAs did not have prior national security investigation experience. Many told us that in their prior experience in criminal investigations field-based SSAs were authorized to sign administrative subpoenas for telephone toll billing records, and they therefore did not believe the exigent letter practice to be extraordinary.

Three of the SSAs who together signed 114 of the 722 exigent letters issued by the CAU told us that they were concerned with the use of exigent letters and separately brought their concerns to Rogers when he was the CAU Unit Chief.[42] Two of these SSAs said that Rogers assured them that the exigent letters were proper and had been approved by "lawyers." The three SSAs told us they were directed by Rogers to continue using the exigent letters. One SSA said he had also expressed concern to Rogers about the reference in the exigent letters to follow-up subpoenas when he became aware that after-the-fact process was more often NSLs than

---

[42] These SSAs are not the same SSAs described above who together had signed nearly 50 percent of the exigent letters signed by CAU personnel.

subpoenas. This SSA said Rogers told him not to change "a single word" in the letter because it had previously been reviewed and approved.[43]

Rogers told us that he did not recall any of the SSAs in the CAU coming to him with concerns about the wording of the exigent letter. Rogers also said that he never spoke to any attorneys from either the FBI or the communications service providers about the use of exigent letters. Rogers said that he accepted the validity of the exigent letter based on the briefing he received from the Company A analyst who told him in May 2003 that the letter had previously been approved for use in the New York Field Division in 2002. Rogers, who signed 12 exigent letters, told us that he took "full responsibility for that letter – that it wasn't worded properly, [and] that it took so long to change the wording" to refer to NSLs rather than subpoenas.

2. CTD Supervisors

In addition to our interviews of CAU personnel and supervisors, we also interviewed supervisors in the CTD who served during the 2003 through 2006 time period about the use of exigent letters. These officials included FBI Assistant Section Chiefs, Section Chiefs, Deputy Assistant Directors, and Assistant Directors who had responsibility either for oversight of the CAU or the other CTD units whose frequent requests for telephone records resulted in the CAU's issuance of the exigent letters. All but one of them told us they were unaware before the OIG's first NSL investigation that the CAU was using exigent letters to obtain telephone records from the three on-site communications service providers.

The one FBI official who told us that he knew about exigent letters at the time they were used was John Chaddic, the Assistant Section Chief of CXS from June 2003 to October 2004.[44] Chaddic told us that in approximately June 2003 Rogers briefed him about exigent letters and described them as a "placeholder so that we could get the toll records and analyze them while we waited on the NSL." Chaddic said he never saw an exigent letter but "wasn't surprised" when he learned about the exigent letter process because the FBI could not afford to wait for the appropriate legal process in emergency situations when lives might be at risk. Chaddic also told us that he had assumed the use of exigent letters was addressed in the FBI's contracts with the communications service providers. He also said

---

[43] None of the other SSAs we interviewed who signed exigent letters said they brought concerns about the use of exigent letters to either Rogers or Youssef.

[44] Chaddic is currently a Unit Chief in the FBI's Counterintelligence Division.

that the concept seemed consistent with at least one classified FBI program ongoing at the time. Chaddic added that since Rogers and most of the SSAs assigned to the CAU had previous experience with FBI drug investigations for which SSAs were authorized to obtain telephone records by signing administrative subpoenas, the exigent letter tool would not be a departure from their prior FBI experience in securing telephone records.

Other CTD officials told us they were not aware of the use of exigent letters until the OIG's investigation. For example, Laurie Bennett and Jennifer Smith Love, two of the FBI officials who served as the Section Chief of the CXS from 2004 through 2006, told us that they did not know about the letters until the details of the practice emerged during the OIG's first NSL investigation in 2006.[45] Bennett, who was the CXS Section Chief from August 2004 to April 2006, told us that she expected that information from the communications service providers was obtained legally and that the CAU would have informed her if they could not obtain the information legally. Love, who was the CXS Section Chief from April 2006 to December 2006, told us that she did not know about exigent letters, although she was aware that the CAU had obtained records from the providers prior to issuing legal process, and that the CAU had ongoing problems obtaining NSLs to cover telephone records that the FBI had previously received from the on-site providers.

Similarly, former CTD Deputy Assistant Directors John Lewis, Thomas Harrington, and Arthur Cummings III told us that they did not know about the exigent letters practice.[46] However, Lewis said he was "not surprised that [the FBI] [was] dealing with the phone companies in as aggressive a manner as possible." Cummings told us that he believed the use of the letters must have been approved by the FBI.

Former Assistant Directors in charge of the CTD also told us they were unaware of the exigent letter practice. Larry Mefford served as Assistant Director of the CTD from July 2002 until July 2003 and as Executive Assistant Director of the FBI National Security Branch from July 2003 until his retirement in October 2003. Mefford said that he was

---

[45] The official who served as the first Section Chief of CXS from 2002 until April 2004 has retired from the FBI and declined our request for an interview.

[46] Lewis served as a Deputy Assistant Director in the CTD from April 2004 to June 2006, and retired from the FBI in February 2009. Harrington served as a Deputy Assistant Director in the CTD from December 2002 until March 2008. Harrington currently serves as the Executive Assistant Director of the FBI's Cyber Division. Cummings, who served as a Deputy Assistant Director in the CTD from August 2006 to November 2007, is currently the FBI's Executive Assistant Director for the National Security Branch.

unaware of exigent letters until he read press accounts in 2007 about the OIG's first NSL report. Similarly, Willie Hulon, who served as Assistant Director of the CTD from December 2004 to June 2006, and as Executive Assistant Director for the FBI's National Security Branch from June 2006 to January 2008, told us that he did not know about exigent letters. Hulon said he "assumed that we were using the NSL legal process." Joseph Billy, Jr., who served as one of the CTD's Deputy Assistant Directors from April 2005 to October 2006, as its acting Assistant Director from June 2005 to October 2006, and as its Assistant Director from October 2006 until his retirement from the FBI in March 2008, also told us that he did not know about the CAU's use of exigent letters until the OIG's first NSL investigation discovered the practice in 2006.

D. The FBI's Senior Leadership

The FBI's senior leadership also told us they were unaware of the CAU's use of exigent letters until the OIG's first NSL investigation.

We determined that in July 2006, shortly after OIG investigators conducted the first interviews in our first NSL review, FBI General Counsel Valerie Caproni was informed by the Assistant General Counsel that in emergency circumstances the CAU was using letters that promised future legal process to obtain records from the on-site providers. The Assistant General Counsel also advised Caproni that there had been problems with identifying preliminary investigations to which after-the-fact NSLs could be tied, but that NSLs were being issued within 2 or 3 days. However, Caproni told us that she did not actually see an exigent letter until December 2006 when the OIG showed her some sample exigent letters during an interview in connection with our first NSL report.

FBI Deputy Director John Pistole served as Deputy Assistant Director and then Assistant Director of the CTD from May 2002 to October 2004, and as Executive Assistant Director of the National Security Branch from December 2003 to October 2004. Pistole told us that he did not know specifically about the use of exigent letters. He said he understood that if something was "hot, you could get the information right away and then follow up with paper," which was the "normal course of business" in counterterrorism investigations.

FBI Director Mueller told us that he was unaware of the CAU's use of exigent letters until at or about the time the FBI received the draft of the OIG's first NSL report, which was in late 2006. Mueller stated that, until then, he was unaware that the CAU was receiving telephone records without the appropriate legal process.

E. Employees of On-site Communications Service Providers

We also interviewed employees of the communications service providers who were assigned to the FBI about the use of exigent letters.

The first Company A analyst who arrived at the CAU in April 2003 told us that he was acquainted with the use of exigent letters from his previous experience as an on-site analyst at the FBI's New York Field Division, where, as noted above, exigent letters had been in use since 2002. Rogers and other CAU personnel who signed exigent letters said that this Company A analyst told them that exigent letters were a method for requesting telephone records from Company A. This analyst defined exigent circumstances as "needing of the records immediately." The Company A analyst confirmed that he often informally briefed CAU and other FBI personnel on the use of exigent letters, and said he told them that they could use an exigent letter when "they needed the records quicker."

The on-site Company C employee, who arrived at the CAU in April 2004, told us that neither his company supervisors nor FBI officials described exigent letters to him before he began working at the CAU. He said that he was first presented with an exigent letter soon after his arrival at the CAU and that he accepted the legitimacy of the letter based on the "credibility" of both the SSA who signed the exigent letter and "the whole unit."[47] The Company C employee, who did not have prior experience in subpoena or NSL compliance, told us that he accepted exigent letters at "face value" as indicating that the FBI needed the data as soon as possible and would subsequently provide legal process. The Company C employee stated that he honored exigent letters without consulting his Company C supervisors.

The on-site Company B employee arrived at the CAU in early September 2004. This employee had extensive prior experience with subpoena compliance. He said he had not been told prior to his arrival about the CAU's use of exigent letters, and that on the second day of his assignment, September 8, 2004, a CAU intelligence analyst presented him with an exigent letter. The Company B employee said he initially declined to honor the exigent letter, telling the CAU analyst that she would need to provide an NSL before Company B would process the request. The Company B employee stated that the analyst was "stunned" by his refusal

---

[47] The first exigent letter we found that was issued to the on-site Company C employee was dated April 14, 2004.

and took the matter to a CAU SSA. The Company B employee said the CAU SSA then explained to him the concept of exigent letters and told him the NSL was "not written or not going to be written right now or today." The Company B employee told us that he conferred with his Company B supervisor, who told him to honor the requests but to be sure to get the after-the-fact legal process. Thereafter, the Company B employee regularly accepted exigent letters and provided responsive records to the CAU. The Company B employee told us that "the majority of the time" he "did not know what the [exigent] circumstance was." He said he "pretty much assumed . . . that it was an exigent circumstance" because he was supporting counterterrorism investigations in the CAU.

We determined that the providers' on-site employees often received exigent letters from CAU personnel – and responded to them – without receiving any information about the FBI investigations for which the records were needed. The providers' employees told us that they accepted exigent letters without question and assumed that the circumstances were exigent. For example, the Company C employee told us, "most of the time I know nothing about the case personally" and that he sometimes relied on CAU personnel saying the matter was "hot." The Company B employee said that he only received case details related to exigent letter requests less than 25 percent of the time, but he reasoned each time that, "it is an emergency situation and they need my assistance. I am taking their word." A Company A analyst told us that the CAU requesters "did not always tell me the circumstances of why they needed the records" and said he accepted the FBI's representation in the exigent letters, observing, "personally, it wasn't my place to police the police."

The Company B employee told us that although he "assumed" CAU's requests were emergencies, he had concerns about whether the exigent letter requests were truly emergencies, and these concerns led in part to Company B's decision to change its procedures. Beginning on October 10, 2006, the on-site Company B employee placed a stamp on the exigent letters for which he provided responsive records. The stamped text stated, "An emergency involving danger of death or serious physical injury to a person requires disclosure without delay of information relating to the emergency."[48] The Company B employee told us that he added the stamped text to the exigent letters at the direction of Company B's legal counsel and he also required FBI requesters to certify by initialing and dating the stamped declaration that the circumstances of the request comported with

---

[48] The stamp appeared on the final 13 exigent letters served on the on-site Company B employee between October 10, 2006, and November 6, 2006.

the legal standard for an emergency voluntary disclosure pursuant to 18 U.S.C. § 2702(c)(4).[49] The Company B employee stated that he did not provide responsive records unless requesters signed or initialed this certification.

The Company B employee told us that he also followed his supervisor's instruction to be sure to get after-the-fact legal process, and he: (1) created a spreadsheet to track the outstanding legal process; (2) reminded CAU personnel and sometimes requesters in the field via either face-to-face conversations, telephone calls, or e-mails that he was still awaiting process; (3) brought the issue of exigent letters to the attention of CAU Unit Chief Glenn Rogers and later Unit Chief Bassem Youssef; and (4) provided a list of telephone numbers still awaiting process to a CAU SSA so that the numbers could be incorporated into the Company B May 12, 2006, "blanket NSL" described in Chapter Four.

F. Types of Cases in which Exigent Letters were Used

CAU agents, analysts, and Unit Chiefs told us that they used exigent letters and other informal requests to the on-site communications service providers to quickly obtain telephone records and analyze them in connection with many urgent, high priority counterterrorism investigations. They said that many of the requests that came to the CAU involved telephone numbers from [redacted]

---

[49] 18 U.S.C. § 2702(c)(4) provides:

Voluntary disclosure of customer communications or records.

* * *

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

* * *

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; . . . .

An earlier version of this provision that was in effect between 2003 and March 8, 2006 – the period when most of the exigent letters were issued – authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."

[redacted] Large groups of telephone numbers were [redacted] and the FBI moved quickly to exploit the numbers, [redacted] and that might reveal links to possible terrorist activities [redacted]

According to FBI officials, on some occasions the CAU sought telephone records in connection with international terrorism investigations involving terrorist plots that were believed to pose an imminent threat to the United States or its citizens abroad. For example, in a [redacted] case that received widespread media attention, the FBI investigated a terrorist plot [redacted] to detonate explosives [redacted] CAU personnel sought calling records for thousands of telephone numbers in support of this investigation, which we refer to as Operation Y in this report. CAU personnel also said they used exigent letters to obtain calling information to help the FBI address numerous bomb threats. FBI officials said that in these and other cases the CAU enabled the FBI to quickly address serious threats through its ready access to the on-site communications service providers.

The CAU also used the on-site communications service providers to obtain telephone records in support of criminal investigations, such as organized crime and kidnapping cases. For example, the CAU issued exigent letters in the kidnapping investigations regarding [redacted] who disappeared in 2005 [redacted] and [redacted], a U.S. citizen from [redacted] who was kidnapped in Iraq [redacted]

However, as described in Chapters Four and Six, FBI officials told us that the investigations for which exigent letters were used, although urgent and important, did not necessarily involve imminent threats or life-threatening circumstances. For example, we discuss in Chapter Four a high-profile FBI operation we call "Operation Z" for which CAU personnel used exigent letters and other informal requests to request records for hundreds of telephone numbers associated with a dead terrorist. According to the FBI supervisors responsible for the operation, the circumstances in which the records were obtained for exploitation were not exigent. In addition, we found that exigent letters were issued in cases such as media leak investigations, fugitive investigations, and other investigations that did not include exigent or life-threatening circumstances.

IV. Other Informal Methods for Requesting Records without Prior Service of Legal Process

In addition to the use of exigent letters, we determined that CAU personnel regularly requested and received from the three on-site communications service providers toll records and other information related to [redacted] telephone numbers without issuing any legal process or even providing exigent letters. We could not determine the full scope of this practice since the CAU had no systematic tracking system to document the requests, and the telephone providers did not consistently document these requests. However, based on our interviews of CAU personnel and the providers' employees, as well as our review of documents, we concluded that CAU personnel requested [redacted] for records of more than 3,500 telephone numbers without prior service of legal process or even exigent letters.

A. E-mail, Face-to-Face or Telephone Requests, and Informal Notes

In most of the instances described in this section, CAU personnel conveyed their record requests to the on-site providers by FBI e-mail. However, employees of the providers also told us that CAU personnel sometimes conveyed their [redacted] requests by giving target telephone numbers to the providers' employees verbally during telephone calls or visits to the providers' CAU work stations, or on pieces of paper, such as post-it notes. CAU personnel also sometimes sent requests to the providers' [redacted]

A CAU Intelligence Analyst told us that one of the Company A analysts routinely provided toll records to him without first receiving legal process or an exigent letter. The CAU Intelligence Analyst stated that this was the process he used "close to 100 percent of the time." The Intelligence Analyst said he would usually fax an exigent letter to the Company A analyst several days after he received responsive records pursuant to his informal requests. We also found several FBI documents indicating that on-site Company A employees [redacted] and in many cases provided telephone toll billing records to the FBI without any prior legal process or even exigent letters.

Exigent letters were never provided to Company A for many of these requests, either before or after the fact. Indeed, as we describe in Chapter

Four of this report, the FBI was able to locate exigent letters for only 235 of the 700 telephone numbers listed on one of the so-called "blanket" NSLs issued by the FBI to cover or validate records previously obtained by the FBI.[50]

We did not have similar data for Company B and Company C, but employees of both carriers told us they also [redacted] and provided telephone records to the FBI in response to e-mails and verbal requests and without legal process or exigent letters. The Company B and Company C employees stated that they believed such [redacted] usually related to major FBI counterterrorism investigations.

We also determined that in connection with at least three major FBI counterterrorism investigations in 2005 and 2006, CAU personnel requested telephone records for hundreds of telephone numbers from the three on-site communications service providers. While we identified some exigent letters associated with these operations, the majority of the requests in these operations were initiated without legal process or exigent letters. In a majority of these instances, even when records were turned over to the FBI, exigent letters were not subsequently provided to cover the requests and records provided for these major operations. Moreover, in most instances the FBI issued legal process to cover these requests well after the records had been provided to the FBI, from 20 days later to 6 months later.

The on-site Company C employee also told us that apart from major FBI operations, he occasionally provided records to CAU personnel prior to receiving legal process or an exigent letter. We also reviewed an e-mail message the Company C employee sent in January 2006 to Unit Chief Youssef and a CAU Intelligence Analyst in which the Company C employee stated that he would give priority to requests which did not have accompanying legal process or an exigent letter if the CAU provided him a reason to do so. In response to this e-mail, the CAU Intelligence Analyst stated that "[w]e are working with hundreds of numbers and it's not practical to give the [exigent letter] for every number that comes in."

We also reviewed the on-site Company C employee's log and identified numerous instances apart from major FBI operations where telephone records were provided to the CAU without legal process or exigent letters.[51]

---

[50] This was the Company A September 21, 2006, blanket NSL, described in Chapter Four.

[51] The Company C on-site employee kept a contemporaneous log of requests made by CAU personnel. He said he used the log to record requests for [redacted], including requests pursuant to legal process, exigent letters, sneak peek requests, and, in some (Cont'd.)

In some instances the FBI issued exigent letters after receiving the records. In other instances, exigent letters were never provided or the FBI did not issue any after-the-fact legal process for up to 20 months.

The on-site Company B employee told us that he gave telephone records to the FBI without legal process or exigent letters more often in connection with major FBI operations than in other matters. However, we reviewed e-mails from September 2005 to November 2005 indicating that on at least three occasions the Company B employee provided records to CAU personnel prior to receiving legal process or exigent letters, and none of these three instances related to major operations.

B. "Sneak Peeks" or "Quick Peeks"

Many CAU SSAs and Intelligence Analysts we interviewed, and employees of the three on-site communications service providers, also told us about a practice that became known in the CAU as "sneak peeks" or "quick peeks." At the request of CAU personnel, the providers' employees routinely [redacted] of their databases to determine whether they had any responsive records, without receiving legal process or exigent letters. The providers' employees would then describe for the CAU personnel the information contained in the databases without providing the records to CAU personnel. We reviewed documents showing that employees of all of the on-site providers communicated this type of information to CAU personnel either verbally, by e-mail, or telephonically. At times, the providers' employees even invited CAU personnel to view records on their computer screens. If the providers' databases contained requested records, CAU personnel would then decide whether to issue exigent letters or obtain legal process from the field division or Headquarters' operating unit in order to obtain the actual records.

Glenn Rogers, the CAU's first permanent Unit Chief, acknowledged to us that he knew about this practice of sneak peeks. He stated that he believed the practice was first used in the FBI's New York Field Division before it was used by CAU personnel. He said he did not see any legal problem with the practice and stated it was his understanding that there was no expectation of privacy in telephone records because the "numbers belong to the phone companies." He said he therefore did not think there was anything wrong with requesting sneak peeks, and he did not believe

---

instances, post-it notes or a "sticky." Neither Company A nor Company B maintained similar logs. However, both Company A and Company B are able to retrieve records of the [redacted] by their on-site employees.

that NSLs or other legal processes were required prior to such sneak peeks. Bassem Youssef, who succeeded Rogers as the CAU Unit Chief, told us that he had no "first-hand knowledge" of the sneak peek practice in the CAU during his tenure. However, Youssef stated that the concept, as he came to learn in 2007, was to indicate only whether the on-site providers had responsive records on a telephone number.[52]

We also reviewed the Company C employee's log and identified many entries of database [redacted] for which the employee noted that there was "no paper." The log identified CAU requests such as "any calls between these numbers in past month," "any [redacted] calls during Dec 22-25, 2005 [for three domestic telephone numbers]," and "any [telephone calling] activity [for three domestic telephone numbers]." The Company C employee told us that "sometimes there was nothing said" by FBI personnel about the reasons for sneak peek requests. The requesters sometimes just said, "here is a sticky with numbers" and they would specify a date range.

E-mail records we examined from employees of the three on-site communications service providers also showed that in response to sneak peek requests, they confirmed whether the provider had records on an identified telephone number. These e-mails also showed that the providers' employees sometimes responded to these requests with additional information about the calling activity by the identified telephone numbers. For example, e-mail messages from the providers to CAU personnel often included whether the telephone number belonged to a particular subscriber or a synopsis of the call records, such as the number of calls to and from a specific telephone number within certain date parameters, the area codes [redacted] called, and call duration.[53]

The on-site Company C employee told us that he responded to requests for sneak peeks "fairly frequently," estimating that he responded to such requests approximately 300 times (which represented nearly one-half of all the requests he received from CAU personnel from April 2004 until June 2007). The on-site Company B employee stated that sneak peeks

---

[52] We asked Youssef about an August 8, 2006, entry in the Company C employee's log which listed Youssef as the CAU requester for a sneak peek involving four telephone numbers. Youssef told us that he had no recollection of making such a request to the Company C employee.

[53] As described in Chapter Three of this report, sneak peeks were used by the FBI in connection with a media leak matter in which the three on-site providers [redacted] their databases for calling activity of a reporter.

"could have been 1, 2, or 3 times a week." An on-site Company A analyst told us that sneak peeks occurred daily.

We also reviewed e-mails from CAU personnel to employees of the three on-site providers with requests to [redacted] their databases for specific calling activity. For example, in September 2005 an on-site Company A analyst received an e-mail request from a CAU Intelligence Analyst that listed four domestic telephone numbers and asked:

> Could you take a look at these numbers, below, and let me know if you have any calls to [redacted] or Oregon in the past six months? If so, [FBI case agent] has indicated he will be able to provide us with a subpoena.

Similarly, in a March 2006 e-mail exchange between a CAU Intelligence Analyst and the on-site Company B employee with the subject line "quick peek," the Intelligence Analyst requested a "quick peek to see if [Company B has] any data" for a specific [redacted] cellular phone number. The Company B employee responded to the request, "I ran the number for the past [redacted] days and picked up some calls. Stop by my desk if you'd like to see the calls."

We also reviewed a series of e-mails between CAU personnel and a Company A analyst related to a major counterterrorism investigation that was underway in [redacted] 2006. In one of the e-mails, Unit Chief Youssef provided a list of four telephone numbers that were determined by a prior Company A [redacted] to be in contact with a particular telephone number that had been a target number in an NSL. In response, the Company A analyst wrote to Youssef, a CAU Intelligence Analyst, and a CAU SSA that, based on Youssef's request, Company A took a "quick peek" at the calling activity of the four telephone numbers identified in the earlier e-mail. The Company A analyst wrote, "very interesting calling patterns and we strongly suggest that these numbers are added to the NSL for exploitation."

The evidence indicates that the FBI OGC first learned about sneak peeks in February 2007 when a CAU SSA, at Youssef's direction, sent an e-mail to FBI General Counsel Valerie Caproni, NSLB Deputy General Counsel Julie Thomas, and the Assistant General Counsel in which the SSA addressed various statistics related to the CAU's use of exigent letters such as the total number of exigent letters issued by the CAU, the total number of telephone numbers included in the exigent letters, the number of telephone numbers for which records had been obtained from the providers without legal process or an exigent letter, and the number of telephone numbers for which legal process was required. In this e-mail, the CAU SSA, for no apparent reason, referred to the sneak peek practice. He described the practice as "a process wherein the telecom provider would glance at the

network to check if it was meritorious to draft a subpoena and/or NSL to officially request the records." The e-mail stated that if there were no records, an NSL would not be drafted.

Caproni told us that she did not recall the SSA's e-mail. When we asked her if she was aware that the FBI at times received more information than just whether the provider had records on a particular number, she said she was not.

As discussed in the analysis section at the end of this chapter, we concluded that the FBI's use of these sneak peeks in many cases violated the ECPA.

V. Records Obtained in Response to Exigent Letters and Other Informal Requests

In this section, we describe the types of records obtained by the FBI from the on-site communications service providers in response to exigent letters and other informal requests. We also discuss how these records were analyzed and uploaded into FBI databases. In addition, we describe "community of interest" or "calling circle" [redacted] (often called a [redacted] community of interest"), through which Company A [redacted]

A. Types of Records Collected by the Providers

Each of the three on-site communications service providers had different capabilities to respond to the CAU's requests for telephone records.

[redacted]

The amount of information available to the FBI under its contract with Company A was substantial. PowerPoint slides prepared by Company A explaining its resources, which were incorporated into a CAU presentation

for other FBI divisions and units, stated that Company A [redacted] The slides stated that Company A [redacted]

- domestic [redacted]
- local and long distance calls;
- [redacted]
- [redacted]
- cellular calls, [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Of the three providers, Company A had the greatest volume of records available to the FBI. The key features of Company A's on-site support were the availability of [redacted] of telephone records, [redacted] These features were not available to FBI field agents or Headquarters personnel who served NSLs on Company A through its more formal procedures.

The on-site Company C employee also had access to calling records of telephone [redacted]

[redacted], the Company B on-site employee could only provide calling records [redacted] These were the same types of telephone records that FBI agents outside of the CAU obtained from Company B's

subpoena compliance office. The records available to Company B's on-site employee dated back [redacted][54] Nevertheless, like the advantage offered by the Company A and Company C on-site employees, the advantage offered by the on-site Company B employee was the speed with which requests to Company B were processed and records provided to the CAU.

Employees of the three on-site communications service providers told us that they believed that they could release any information in their databases to the FBI without regard to whether the request was documented in exigent letters, NSLs, or grand jury subpoenas.

B. How Records were Uploaded and Analyzed by the FBI

CAU personnel told us that the three on-site communications service providers delivered telephone records to the CAU in an electronic format that was compatible with FBI databases and a [redacted] database used by the FBI primarily for analysis of telephone toll billing records. The records provided in electronic format could be directly uploaded without being re-formatted. The on-site communications service providers' employees told us that during normal business hours they usually hand-delivered to CAU employees the requested electronic records on a compact disk (CD). In many instances the on-site providers' employees would also contemporaneously forward an electronic copy of the records to the CAU requesters as e-mail attachments.

We found that in [redacted] the on-site providers sometimes forwarded telephone records to CAU requesters [redacted] Some of these records sent to CAU requesters [redacted] were associated with high-value terrorists.[55]

---

[54] Although the FBI's requirements for the Company B contract stated that Company B "would deliver at least [redacted] of historical records," the on-site Company B employee told us that in some instances he was able to obtain records for up to [redacted]

[55] The OIG informed the FBI Inspection Division about this practice and raised concerns about possible breaches of FBI internal policies, as well as security concerns raised by the [redacted] The Inspection Division informed us that the telephone [redacted] did not contain any classified information and that the CTD did not consider the matter to be a security issue. We disagree, and believe that [redacted] does raise security concerns.

We also determined that the telephone records received by the CAU were routinely uploaded into the [redacted] database without being compared to the FBI's original request. The CAU employee in charge of the CAU team that uploaded the records told us that there was no mechanism in place to verify that the records were for the target telephone numbers and within the date ranges specified in the original request. He also stated that his team did not receive a copy of the FBI's original request. The team therefore was not in position to check whether any information had been mistakenly supplied to the FBI or had been mistakenly requested due to FBI errors. Several CAU SSAs and Intelligence Analysts told us that they sometimes informally checked the records to see whether the records matched the requests, but none of these individuals said there was any formal protocol requiring such a review.[56]

After the CAU team uploaded the records to the [redacted] database, a CAU employee would deliver the CD to the CAU requester, who was responsible for forwarding the CD to the FBI field or Headquarters' operating unit that had initiated the request. The CD containing records was considered by the CAU to be the "original" evidence.

[redacted]

The results of the CAU's analysis are used to create documents called "trace reports" or "[redacted] reports" that were normally forwarded to requesters as attachments to an EC. However, field office requesters sometimes preferred to conduct their own analysis and would specify that the CAU not perform any analytical work. In these instances, the CAU sent requesters a

---

[56] In response to our first NSL report, the FBI OGC directed that FBI case agents ensure that, in the future, the records obtained in response to NSLs match the NSL requests. The CAU's policy now requires CAU requesters to certify to the database manager by e-mail that responsive records have been verified as accurately encompassing both the target telephone numbers and date ranges specified in the NSLs.

summary report from the database of all the data related to a particular telephone number.

C. Community of Interest/Calling Circle [redacted]

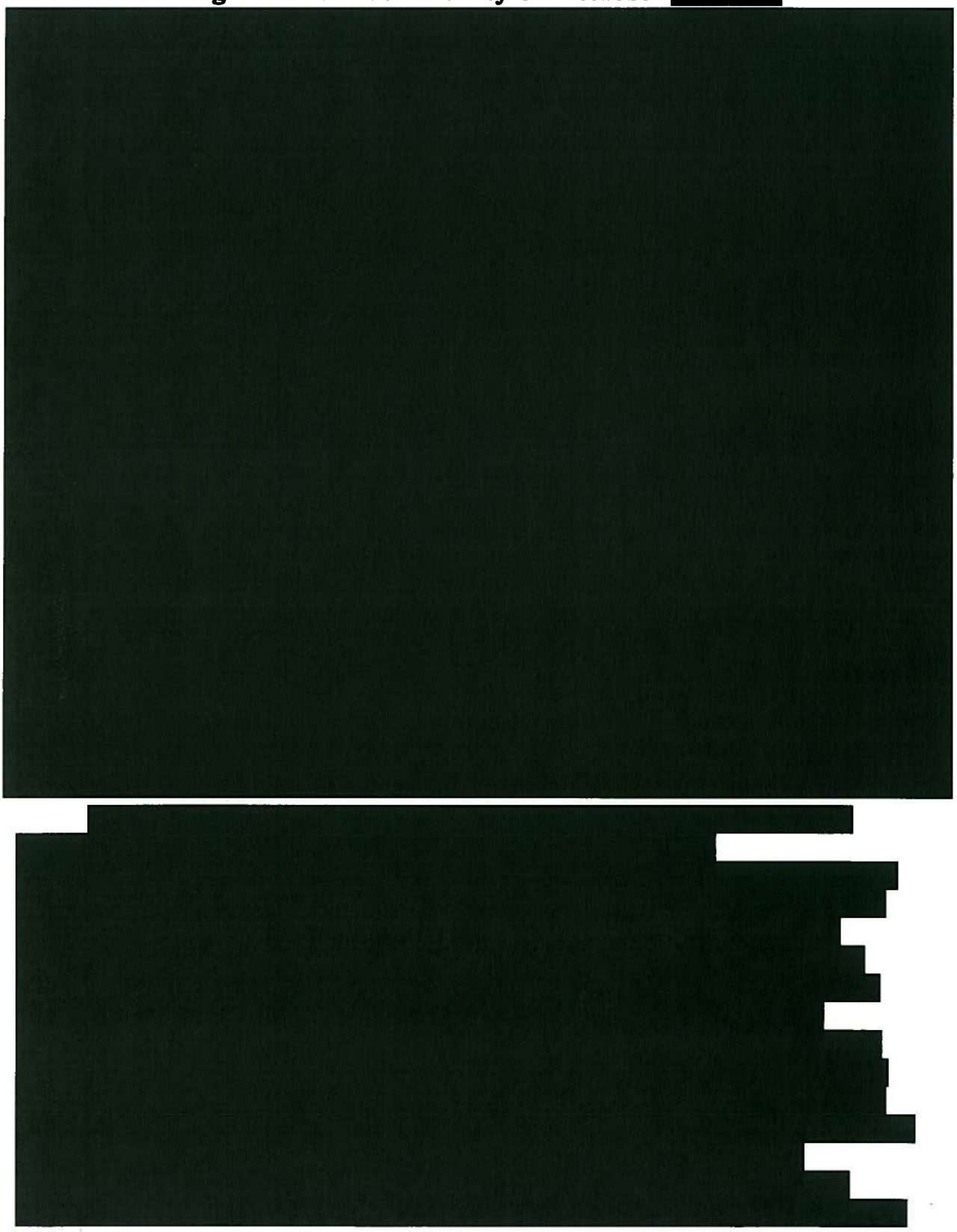
In addition, we found that the FBI often asked Company A's on-site employees [redacted] what were termed "community of interest" or "calling circle" [redacted] These requests were conveyed to Company A in NSLs, grand jury subpoenas, exigent letters, and e-mails. We determined that as part of its [redacted] contract with the FBI, on-site Company A analysts used Company A's community of interest [redacted] on records that were not identified in FBI requests. However, the FBI did not maintain documentation of how often these community of interest requests were made, and we could not determine how often the FBI acquired records in response to these [redacted]

1. Community of Interest [redacted]

[redacted]

DIAGRAM 2.1

Calling Circle or "Community of Interest" [redacted]



[redacted]

2. Community of Interest [redacted] for the FBI

We found that FBI requests for records often included requests for community of interest [redacted] We identified 52 exigent letters (of the 514 signed by CAU personnel) served on the on-site Company A analysts that included requests for community of interest [redacted][57] We also identified more than 250 NSLs and over 350 grand jury subpoenas served on the 3 on-site providers that requested community of interest [redacted]

Prior to mid-May 2006, the FBI issued to the 3 on-site providers 107 NSLs that included in the body of the letters community of interest requests. After May 2006, the community of interest requests appeared in "boilerplate" attachments appended to over 150 NSLs. The standard attachment listed 18 types of records, including a "'calling circle' . . . based

---

[57] Even though Company B and Company C did not [redacted] community of interest [redacted], we identified 25 exigent letters to Company B and 20 exigent letters to Company C that requested such [redacted]

on a [redacted] community of interest" that the attachment stated "may be considered by you to be toll billing records pursuant to § 2709." The FBI Assistant General Counsel had drafted this attachment for the CAU. It was retained on the CAU's share drive and accessible by all CAU personnel and the on-site providers.[58]

We determined that community of interest [redacted] generally were [redacted] after the Company A analyst confirmed with CAU personnel that such a [redacted] was needed. In addition, in some instances, prior to [redacted] such [redacted], CAU personnel asked that the community of interest [redacted] In other instances, the [redacted][59] Thus, it appears that community of interest [redacted] requests often were included as boilerplate language in NSLs served on the on-site Company A analysts, although Company A did not necessarily [redacted] such [redacted] in each instance.

We found evidence that some FBI officials who signed NSLs that contained community of interest [redacted] requests were not even aware that they were making such requests. For example, NSLB Deputy General Counsel Julie Thomas, who signed at least four NSLs dated from February 2005 to August 2005 requesting in the body of the letters community of interest [redacted], told us that she was not aware of Company A's community of interest capability until June 2006, when Company A representatives briefed her and other FBI OGC attorneys on Company A's capabilities under its contract with the FBI. Thomas said that if she had signed NSLs prior to June 2006 containing a community of interest [redacted] request, the request would "probably not" have meant anything to her

---

[58] This NSL attachment was similar to a model standard NSL attachment the FBI's National Security Law Branch (NSLB) in FBI OGC had previously circulated to FBI personnel and posted on its Intranet website. The previous standard NSL attachment listed all of the records identified in the post-May 2006 attachment except calling circle records.

[59] We reviewed exigent letters and NSLs that contained the following text: "In addition, please provide a 'calling circle' for the foregoing telephone number(s) [redacted]

because she had not yet had the briefing from Company A.[60] The approval ECs we obtained that accompanied these NSLs did not mention community of interest [redacted] or [redacted] records.

Similarly, two NSLs signed by then Acting CTD Deputy Assistant Director Arthur Cummings III in October 2006 and an NSL signed by then CTD Assistant Director Joseph Billy, Jr., in January 2006 contained community of interest [redacted] requests, although the corresponding approval ECs did not address that community of interest [redacted] were to be [redacted] or the predication for these [redacted] requests under the ECPA.[61] Thomas told us that there "appears to be the strong potential" that other FBI personnel made community of interest [redacted] requests without "understanding what it means" and that "the appropriate relevance inquiry is not being done."

We requested the approval ECs for 28 NSLs issued between July 28, 2004, and May 2, 2006, to the 3 on-site providers that included requests for community of interest records in the body of the NSLs. The FBI located approval ECs for only 21 of these NSLs. Of these 21 approval ECs, only 4 stated that community of interest records were being requested and only 2 described the relevance of [redacted] records to the investigation.

We also requested the approval ECs for 25 NSLs issued between May 22, 2006, and December 21, 2006, to the 3 on-site providers that included standard attachments requesting community of interest records. The FBI located approval ECs for only 17 of these NSLs. Of these 17 approval ECs, none stated that community of interest records were being requested or described the relevance of [redacted] records to the investigation. This indicates that officials who signed NSLs containing community of interest requests in the letters or attachments often were unaware that they were making such requests.

Senior CTD officials we interviewed said they did not know how often community of interest [redacted] had been [redacted] by Company A. Although most CAU SSAs and Intelligence Analysts said they knew about

---

[60] In contrast, Thomas said she performed a relevancy analysis when she signed NSLs that included community of interest [redacted] requests in late 2006 in connection with a major FBI counterterrorism operation.

[61] Cummings told us that he did not understand the concept of Company A's community of interest [redacted] until after release of the OIG's first NSL report in March 2007. Billy said that he knew about Company A's community of interest [redacted] by 2004 or 2005.

Company A's ability to [redacted] community of interest [redacted], none told us that they had ever personally requested community of interest [redacted] from the on-site Company A employees.

The CAU Intelligence Analyst responsible for the team that uploaded toll billing records into the [redacted] database told us that when the responsive data was delivered to his team for uploading, the team could not distinguish [redacted] numbers provided by Company A in response to community of interest requests. He said he would only be able to identify the records derived from the community of interest requests by analyzing the information accompanying the original request and other background information. This CAU Intelligence Analyst told us that no one in the FBI had ever asked him to segregate records obtained in response to community of interest [redacted] requests or asked any questions about the practice.

Based on our review, we believe that in most instances when CAU personnel asked the on-site Company A analysts to [redacted] community of interest [redacted], Company A initially provided toll billing records for only the target numbers ([redacted] records). We found some e-mails showing that the CAU or other FBI requesters reviewed these records and identified [redacted] telephone numbers for which they requested [redacted] records. However, in responding to these requests for [redacted] records, the on-site Company A analysts did not request and the FBI did not provide separate legal process for the [redacted] records.[62] For example, we found e-mails showing that Company A analysts interpreted community of interest requests as authority to run [redacted] telephone numbers without requiring [redacted] legal process.[63] Similarly, a CAU Intelligence Analyst told us that community of interest requests "could be used to obtain the [redacted] [toll records] without a new NSL or grand jury subpoena."

---

[62] [redacted]

[63] In a September 2006 e-mail to CAU personnel, an on-site Company A analyst wrote that "the [community of interest] language in the [attachment] will allow [Company A] to provide call detail records without [redacted] authority."

Thus, while the NSLs containing the community of interest [redacted] request language were signed by FBI officials who were delegated the authority to sign NSLs, the actual decisions about which [redacted] records were [redacted] were made by CAU Intelligence Analysts, Supervisory Special Agents, and Special Agents who were not among those to whom the FBI Director delegated authority to sign NSLs.[64] As a result, in cases where the NSL signer was unaware that the NSL or attachment contained a community of interest request, the decisions to [redacted] the [redacted] records were made without the appropriate official having made the determination required by the ECPA that the [redacted] telephone numbers were relevant to authorized national security investigations.

As we describe in the analysis at the end of this chapter, if the FBI was able to establish before issuing the NSL that the [redacted] telephone numbers were relevant to an authorized national security investigation, we believe a separate NSL for the [redacted] telephone numbers was not required before requesting or obtaining records on the [redacted] telephone numbers. However, if the FBI did not establish the relevance of the [redacted] telephone numbers prior to the initial [redacted], reliance on the original NSL to obtain [redacted] telephone records violated the ECPA, the Attorney General's NSI Guidelines, and FBI policy.

NSLB attorneys told us that prior to the FBI's implementation of an automated system to facilitate the issuance of NSLs and collection of data on NSL usage for required reports to Congress, the FBI had not determined whether it had acquired any [redacted] records on U.S. persons that should have been reported to Congress.[65] The FBI's automated NSL system

---

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

[65] The FBI's new NSL "subsystem" for creating NSLs is described in the OIG's second NSL report. OIG, NSL II, 21.

implemented in January 2008 requires the user to enter the total number of telephone numbers for which toll billing records are requested in each NSL.[66]

3. Company A's Use of Community of Interest [redacted]

Based on information provided by the on-site Company A analysts and other information from Company A, we found that Company A's on-site analysts used the community of interest [redacted] services Company A provided to the FBI. One Company A analyst estimated he may have used the community of interest [redacted] for up to 25 percent of the [redacted] he [redacted] Company A records show that from 2004 to 2007, Company A analysts used its community of interest [redacted] to review records in its database for 10,070 [redacted] telephone numbers. We believe that most of these numbers were [redacted] by Company A analysts without community of interest requests from the FBI but did not generate records that were provided to the FBI. A Company A attorney told us, based on information provided to him, that the majority of the community of interest [redacted] by the on-site Company A analysts did not result in disclosure of any data to the FBI. However, we found that Company A did not request and the FBI did not provide legal process or exigent letters in connection with Company A's use of its community of interest [redacted] as part of its [redacted] support services.

[redacted]

[66] After reviewing a draft of this report, FBI officials told us that they expect to add a feature to the automated system to capture data on [redacted] numbers.

[redacted]

4. FBI Guidance on Community of Interest [redacted] Requests

Glenn Rogers, who was the CAU's first permanent Unit Chief beginning in March 2003, told us that the NSLB had approved the use of community of interest [redacted], although he said he could not recall the name of the NSLB attorney who had approved their use. Bassem Youssef, who succeeded Rogers as the CAU Unit Chief in November 2004, told us that he was present at a June 2006 briefing by Company A representatives for FBI OGC attorneys and DOJ personnel on Company A's capabilities, which included a reference to the community of interest [redacted] Youssef said that no one in the FBI OGC raised any questions about community of interest [redacted] at the time and that he never heard from FBI OGC attorneys about the issue until it was raised during the OIG's first NSL review.

We determined that in November 2004 and December 2004, the NSLB Assistant General Counsel first exchanged e-mails with several CAU employees regarding the use of language such as "a 'calling circle' based on a [redacted] community of interest" in the body of NSLs or the accompanying attachments to NSLs.[67] After reviewing the language used in the CAU's community of interest requests, the Assistant General Counsel expressed concern to a CAU SSA that the [redacted] information may be "running a little far a field." The Assistant General Counsel thereafter checked with then NSLB Senior Counsel for National Security Affairs Marion Bowman about the CAU's practice of obtaining [redacted] telephone records using NSLs. Bowman replied that he thought the FBI's acquisition of records on [redacted] numbers was authorized if the records "related" to an investigation, but stated that [redacted] records [redacted] Thereafter, by e-mail dated March 7, 2005, the Assistant General Counsel told Rogers and Youssef that NSLB could "make an argument" that [redacted] records are relevant, but that [redacted] records would require additional information supporting the position that the records were relevant.

---

[67] Although the first e-mail exchanges we found on this topic were in November 2004, we found that community of interest [redacted] requests were contained in exigent letters, grand jury subpoenas, and NSLs as early as February 2003.

While no formal legal review of community of interest [redacted] was undertaken by the FBI, the Assistant General Counsel stated that, "we had generally allowed the CAU to do it because, as we understood it, their cases are often more serious and involve immediate threats." However, she said she believed the community of interest feature was used by the CAU only in urgent circumstances "where you don't have time to do an investigation kind of piece by piece." The Assistant General Counsel stated, "The only reason you do a [redacted] in the very beginning is because you don't really have the time and you think the situation is serious enough that you need to get that information right away." She explained that NSLB had approved the community of interest attachment for NSLs served on the on-site providers based on a relevancy analysis that took into account the immediacy and seriousness of the underlying threats for which the CAU provided operational support, rather than on a relevancy analysis of the [redacted] telephone numbers that would [redacted]

FBI General Counsel Caproni and NSLB Deputy General Counsel Thomas told us that while the FBI has not issued written guidance on community of interest [redacted] requests, they concluded based on their own legal analysis that community of interest [redacted] records could satisfy the ECPA relevance standard. Caproni stated that the ECPA relevance requirement does not necessarily mean that only [redacted] records are relevant to an investigation. Thomas also stated that any relevance assessment of the [redacted] telephone numbers would be "very fact specific" and that, based on the nature of the [redacted] target, the [redacted] records could be relevant under the ECPA.

In March 2007, after the OIG raised questions about community of interest [redacted] requests in connection with our ongoing exigent letters investigation, the FBI directed its employees [redacted] In April 2007, the Assistant General Counsel instructed all Chief Division Counsels (CDC) in FBI field divisions to contact NSLB if they saw any community of interest requests.[68]

---

[68] CDCs in all 56 FBI field divisions report to the Special Agents in Charge of the field division and are responsible for reviewing all NSLs prepared for the signature of the Special Agent in Charge. The Assistant General Counsel stated in her April 9, 2007, e-mail to the CDCs that NSLB had "opined to CAU that in certain situations, they can ask for and obtain from the embedded carriers information on a [redacted] of calls, i.e., [redacted] She stated that such requests must be made in the NSL attachment (which lists the type of information the provider "may consider to be 'toll billing records'," not the body (Cont'd.)

Beginning in May 2007, several draft policies on community of interest [redacted] requests were circulated between the CTD and the FBI OGC. The latest draft dated November 23, 2007, addressed circumstances in which community of interest [redacted] would be authorized using NSLs or subpoenas. The draft policy stated that [redacted]

On December 16, 2008, the FBI issued the FBI's Domestic Investigations and Operations Guide (DIOG), which provides specific guidance for requesting community of interest records. The DIOG requires that NSLs requesting community of interest records must be approved by the NSLB Deputy General Counsel and served on the CAU, and that [redacted] telephone numbers for which information is obtained must be reported to the NSLB for congressional reporting purposes.[69]

The DIOG further provides that "if an NSL is seeking [redacted] records, the NSL [approval] EC must clearly state that [redacted] information is being sought and must demonstrate the relevance of the [redacted] information to the national security investigation."[70] We agree with this requirement and concluded that in order to satisfy the ECPA this relevance assessment must be made before issuance of NSLs seeking [redacted] records.

VI. OIG Analysis

A. Requests for Telephone Records through Exigent Letters and Other Informal Requests

To protect the confidentiality of telephone and e-mail subscriber information and telephone toll billing records information, the ECPA states that wire or electronic communications service providers "shall not

---

of the NSL, and that the attachment required legal sign-off on the relevancy of the information sought to the investigation.

[69] Federal Bureau of Investigation, Domestic Investigations and Operations Guide (FBI DIOG), §§ 11.9.3(E) & (E)(3).

[70] FBI DIOG, § 11.9.3(E)(3).

knowingly divulge a record or other information pertaining to a subscriber or customer of such service . . . to any government entity."[71] The ECPA NSL statute contains an exception to the confidentiality of such records by requiring communications service providers to provide covered records to the FBI if the FBI Director or his designee certifies in writing that the records sought are

> relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the constitution of the United States.[72]

During the period covered by our review, the Attorney General's NSI Guidelines authorized the use of NSLs only during investigations of international terrorism or espionage, upon the signature of a Special Agent in Charge or other designated senior FBI official.[73] In order to open such investigations, the FBI must satisfy certain evidentiary thresholds, which must be documented in FBI case files and approved by supervisors.[74] If case agents want to issue NSLs, FBI policies require a 4-step approval process. Case agents must secure the approval of their supervisors, the Chief Division Counsel, an Assistant Special Agent in Charge, and the Special Agent in Charge (or equivalent supervisors and attorneys at FBI Headquarters), who signs the NSL.

We concluded in our first NSL report that the CAU's use of exigent letters was a circumvention of the ECPA NSL statute.[75] We found that neither the ECPA, the Attorney General's NSI Guidelines, nor FBI policy authorize the FBI to obtain ECPA-protected records by serving this type of informal letter prior to obtaining the records, with "legal process to follow." In limited circumstances a separate provision of the ECPA authorizes the FBI to obtain non-content telephone records from communications service

---

[71] 18 U.S.C. § 2702(a)(3).

[72] 18 U.S.C. §§ 2709(a) and 2709(c).

[73] The Attorney General's NSI Guidelines were replaced by a new set of Attorney General Guidelines, the Attorney General Guidelines for Domestic Operations, which became effective on December 1, 2008. The new guidelines do not alter the requirement for NSLs issued in national security investigations.

[74] OIG, NSL I, 17-18.

[75] OIG, NSL I, 95-98.

providers. During 2003 through March 8, 2006 – the period when most of the exigent letters were issued – that provision authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably believe[d] that an emergency involving immediate danger of death or serious physical injury to any person justifie[d] disclosure of the information."[76] However, we did not agree with the FBI's after-the-fact rationale that the letters could be justified under this provision for several reasons, including that the letters were sometimes used in non-emergency circumstances and that senior CAU officials and FBI attorneys told us they did not rely on the emergency voluntary disclosure provision to authorize the exigent letters at the time.[77] We discuss the potential application of the emergency voluntary disclosure provision to exigent letters and other informal requests in greater detail in Chapter Six.

In this review, we found that many FBI supervisors and employees issued or approved these exigent letters even though the letters on their face contained statements that were inaccurate, such as that a grand jury subpoena had already been submitted to the U.S. Attorney's Office and would be served as expeditiously as possible. Yet, when we asked these FBI supervisors and employees why they issued such letters stating that subpoenas were forthcoming, no one could satisfactorily explain their actions. Instead, they gave a variety of unpersuasive excuses, contending either that they thought someone else had reviewed or approved the letters, or that they had inherited the practice and were not in a position to change it, or that the communications service provider accepted the letters. But with few exceptions, no one objected to the inaccurate statements in the letter. Moreover, we found instances in which the signers of exigent letters did not know whether there were exigent circumstances.

In Chapter Five of this report, we assess the accountability of individual FBI supervisors and employees for these improper practices. However, we believe it is important to note here the widespread failure to object to letters that contained inaccurate statements on their face. For FBI officials and employees to unquestioningly issue hundreds of these improper

---

[76] 18 U.S.C. § 2702(c)(4) (Supp. 2002). In March 2006, the provision was amended by the *PATRIOT Improvement and Reauthorization Act of 2005* to allow voluntary disclosure "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006).

[77] OIG, NSL I, 96-97.

and inaccurate letters over a 3-and-a-half-year period is both surprising and troubling.

Moreover, not only did the FBI issue exigent letters to obtain records from the three on-site communications service providers, the FBI used even less formal means to request or obtain telephone toll billing records or other information. We found that the FBI obtained records or information from each of the on-site communications service providers in response to e-mail, face-to-face requests, requests on pieces of paper (including post-it notes), and telephonic requests without first providing legal process or even exigent letters. These informal requests were made in connection with major operations as well as other international terrorism, domestic terrorism, and criminal investigations. As described in Chapter Six, like exigent letters, these other types of informal requests did not constitute legal process under the ECPA and FBI policy.

We noted in our first NSL report that FBI personnel were required by FBI policy to document information demonstrating the FBI's authority to use NSLs in national security investigations. The predication for an NSL request was supposed to be documented in NSL approval memoranda, known as approval ECs. These approval ECs, which were routinely uploaded into the FBI's Automated Case Support System, identified the underlying national security investigation, summarized the facts establishing the predication for the requests, and described the relevance of the information requested to the investigation.[78] The steps required to complete these approval ECs and the chain of command required to approve each NSL request were designed to ensure that the FBI satisfied statutory and Attorney General Guidelines' requirements for using NSLs.

In contrast, when CAU personnel issued exigent letters or made other types of informal requests for records and information from the on-site providers, they did not document the authority for their requests or explain the investigative reasons why the records were needed. The exigent letter requests also were not subject to any supervisory or legal review. Specifically, exigent letters and other informal requests were *not*: (1) accompanied by approval ECs documenting the predication for the requests, specifying the date range of the records requested, and certifying the relevance of the information sought to pending national security investigations; (2) reviewed and approved by FBI attorneys; (3) approved by FBI supervisors; or (4) signed by one of the limited number of senior FBI

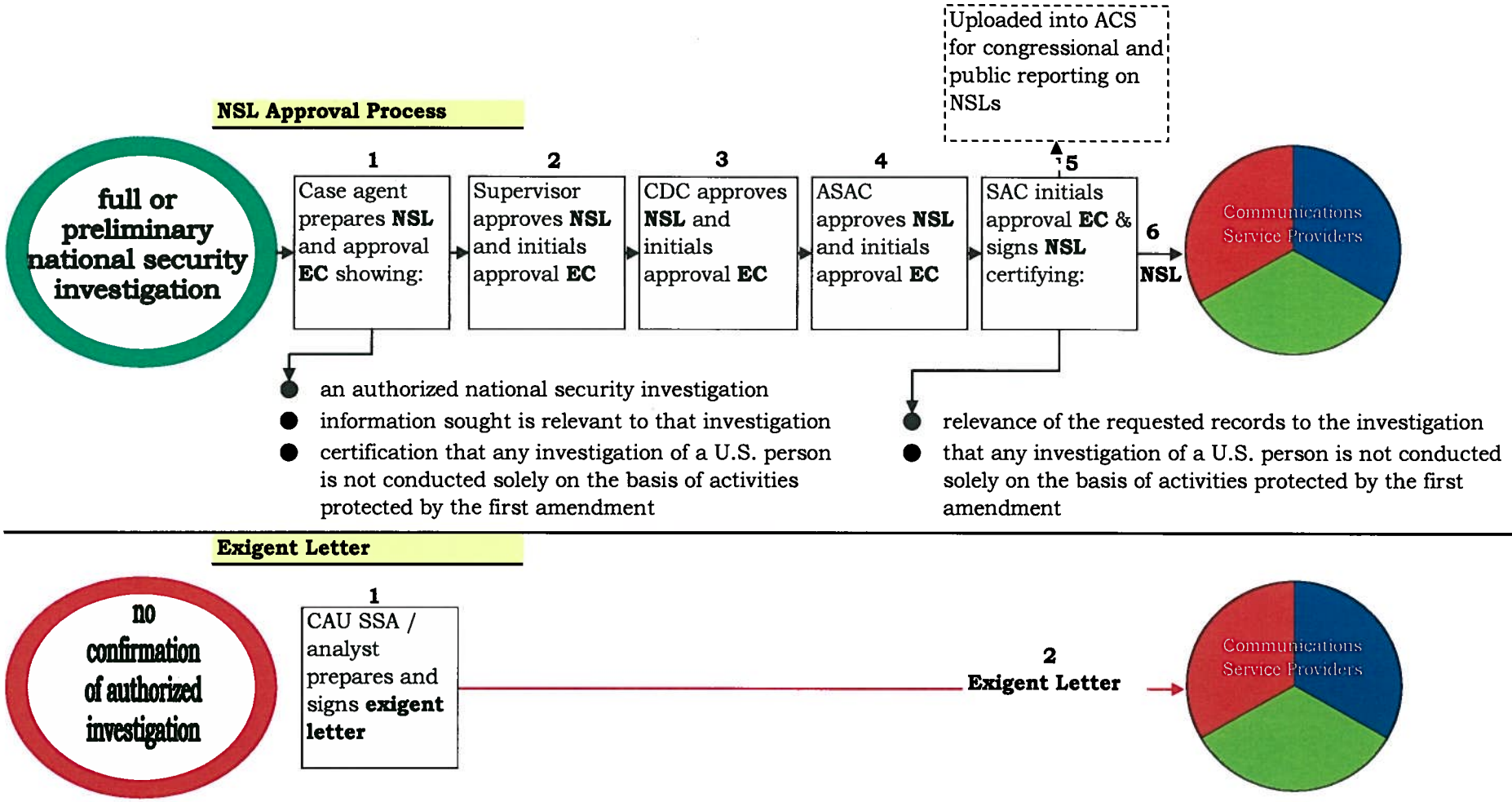
---

[78] OIG, NSL I, 23-25.

personnel authorized to sign NSLs.[79] Similarly, the exigent letters did not meet the legal requirements in the Patriot Act and Patriot Reauthorization Act that senior FBI officials certify in writing the relevance of the records sought to authorized national security investigations and that any investigations of U.S. persons are not based solely on activities protected by the First Amendment. We illustrate in Diagram 2.2 (next page) the differences between the 4-step approval process required for issuing NSLs and the 1-step process used by CAU personnel to issue exigent letters to obtain the same information:

[79] Prior to June 1, 2007, a legal review and approval by an FBI attorney was not required. However, guidance issued by the FBI OGC in November 2001 recommended such a review. Office of the General Counsel, Federal Bureau of Investigation, electronic communication to All Field Offices, Counterterrorism, and National Security, November 28, 2001.

DIAGRAM 2.2
Comparison of NSL Approval Process with Exigent Letters



In fact, the procedure for preparing and issuing exigent letters was so lax that employees of the on-site providers told us that they frequently prepared the exigent letters themselves. Indeed, a Company A analyst told us that to facilitate his preparation of exigent letters he created an icon on his computer desktop so he could easily retrieve and generate the form letter. We believe this is an egregious breakdown in the responsibility assigned to the FBI to obtain ECPA-protected records, and it further illustrates the lack of appropriate controls by the FBI on this important and intrusive investigative tool.

Another result of the abbreviated, unsupervised procedures for issuing exigent letters and other types of informal requests was that FBI requesters did not document whether there was an open national security investigation to which the request was relevant – a key certification required to issue an NSL for toll billing records or subscriber information under Section 2709 of the ECPA. Indeed, as the FBI's analysis of whether it will retain records acquired through exigent letters and other informal requests has shown (which we describe in Chapter Four of this report), the FBI has concluded that records for hundreds of telephone numbers must be purged from FBI databases because there was no open national security investigation at the time of the request and no open national security investigation to which the request could be tied when the retention issue was analyzed years later.

Also troubling was that most of the exigent letters and other informal requests did not include date ranges for the records requested. Of the 722 exigent letters signed by CAU personnel from 2003 through 2006, only 77 (11 percent) specified a date range for the records requested. Similarly, the CAU's other informal requests to the on-site communications service providers (such as those communicated by e-mail, in person, on pieces of paper, or by telephone) frequently did not have date parameters. As further described in Chapter Four of this report, the absence of date restrictions in many exigent letters and other types of informal requests had significant consequences. First, it meant that the FBI often obtained substantially more telephone records, covering longer periods of time, than FBI agents typically obtain when serving NSLs with date restrictions. Second, in cases where the date range established the relevance of the information sought to the investigation, its omission violated the ECPA's relevance requirement.[80]

---

[80] The ECPA NSL statute requires a certification that "the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities . . . ." See 18 U.S.C. § 2709(b)(1). Similarly, the emergency voluntary disclosure provision requires, since March 2006, that the information disclosed be "relat[ed] to the emergency." 18 U.S.C. § 2702(c)(4).

Moreover, by not reviewing records obtained in response to exigent letters and other types of informal requests, CAU personnel compounded problems arising from the lax procedures at the front end of these requests. CAU personnel told us, and documents we reviewed confirmed, that records obtained in response to exigent letters and other informal requests were routinely uploaded into a [redacted] database when received from the on-site communications service providers. However, this uploading normally occurred without verification that the records obtained matched the requests. Further, the original FBI requesters often did not have access to this database or know that CAU personnel were uploading records into the database.

We found in our first NSL review that the FBI did not always examine records obtained in response to NSLs prior to uploading the records into FBI databases.[81] However, in those instances where the communications service providers responded to routine NSLs issued by FBI field offices, the case agents or Intelligence Analysts who had initiated these requests would sometimes review the records before they were uploaded into FBI databases. Because of their familiarity with the underlying investigations, these case agents or Intelligence Analysts could identify records the FBI did not request, or had requested by mistake, and take corrective action before the records were uploaded or placed in investigative case files.

In contrast, CAU personnel routinely uploaded records obtained in response to exigent letters and other informal processes into the [redacted] database upon receipt, without any review. The CAU SSAs and Intelligence Analysts said they were for the most part unaware of the facts of the investigations and were acting merely as conduits between the requesters and the on-site communications services providers. Indeed, CAU personnel did not even retain copies of the exigent letters or documentation of the other types of informal requests and therefore were unable to confirm that they received responsive records. This meant that neither CAU personnel nor anyone else in the FBI determined whether the FBI had received unauthorized

---

[81] FBI personnel were not required until June 1, 2007, after the OIG's first NSL report was issued, to confirm that records obtained in response to NSLs matched the requests in the NSLs before uploading them into FBI databases. We found in our first and second NSL reports that the FBI obtained unauthorized collections in response to many NSLs, findings confirmed by the FBI's review of a statistical sample of NSLs issued from 2003 through 2006. The unauthorized collections included records not requested in the NSLs. See OIG, NSL I, 73-84; OIG, NSL II, 26-28, 82-99.

collections, handled the overcollected materials appropriately, and made required reports to the President's Intelligence Oversight Board (IOB).[82]

B. "Sneak Peeks"

We also identified the FBI's practice of obtaining "sneak peeks" for telephone toll records in the providers' databases, a practice that we concluded violated the ECPA statute (18 U.S.C. § 2702(a)(3)). There is no provision in the ECPA allowing the FBI to obtain information about these records without either issuing legal process or making requests for voluntary disclosure in qualifying emergencies, pursuant to 18 U.S.C. § 2702(c)(4).

Because CAU personnel failed to keep records of sneak peek requests, we were unable to determine how often such requests were made during the period covered by our review, whether the requests were pertinent to FBI investigations, in what circumstances they were made, and what, if anything, the providers were told about the reasons for these requests. However, we found that these requests were routine. One Company A analyst told us he responded to these requests on a daily basis, a Company C employee told us that these requests were approximately one-half of the requests he received from the CAU, and a Company B employee told us that he responded to these requests up to three times per week. The on-site Company C employee's log and e-mails of the employees of all three on-site providers also demonstrate that such requests were routine.

Although CAU Unit Chief Rogers was aware of and approved sneak peek requests, we found that he issued no guidance and failed to require supervisory review or establish internal controls regarding their use. Rogers said he understood sneak peeks to be requests to see if the providers "even had

---

[82] Executive Order 12863, which has since been modified, requires the Department to report intelligence violations to the President's Intelligence Oversight Board. According to Executive Order 12863, possible intelligence violations include any activities that "may be unlawful or contrary to Executive Order or Presidential Directive."

"Unauthorized collections" is a phrase used 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 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. See NSL II at 141.

data at all" and whether it was worthwhile pursuing an NSL. Youssef said he had no "first-hand knowledge" that CAU personnel requested sneak peeks from the on-site providers and did "not know for a specific fact . . . that it actually happened." However, Youssef added that "maybe someone [in the CAU] has used it."

We found that FBI supervisors in the CTD's chain of command, above the CAU Unit Chief, either did not know about the practice, did not have an accurate understanding of the practice, or did not understand the legal implications of providing responsive information without legal process. For example, former CXS Assistant Section Chief John Chaddic believed, incorrectly, that in response to sneak peek requests, the providers only informed the FBI whether the number was or was not a valid telephone number, but no further details. Former CTD Deputy Assistant Director John Lewis said it was his understanding that the FBI could use sneak peeks to "get records that would be of interest to us" without legal process, stating, "it's also why I think the phone company was there."

On August 28, 2007, the FBI OGC requested a legal opinion from the Department's Office of Legal Counsel (OLC) regarding three questions relating to the FBI's authority under the ECPA, including sneak peeks. One question stated that, "on occasion, FBI employees may orally ask an electronic communications provider if it has records regarding a particular facility (e.g., a telephone number) or person." The request asked whether under the ECPA the FBI can lawfully "obtain information regarding the existence of an account in connection with a given phone number or person," by asking a communications service provider, "'Do you provide service to 555-555-5555?' or 'Is John Doe your subscriber?'"

However, based on information we developed in our investigation, we determined that the hypothetical example used by the FBI OGC in the question it posed to the OLC did not accurately describe the type of information the FBI often obtained in response to sneak peek requests. As described above the FBI sometimes obtained more detailed information about calling activity by target numbers, such as whether the telephone number belonged to a particular subscriber, the number of calls to and from the telephone number within certain date parameters, the area codes [redacted] called, and call duration.

On November 5, 2008, the OLC issued its legal opinion on the three questions posed by the FBI. In evaluating if a provider could tell the FBI consistent with the ECPA "whether a provider serves a particular subscriber or

a particular telephone number," the OLC concluded that the ECPA "bars providers from complying with such requests."[83] In reaching its conclusion, the OLC opined that the "phrase 'record or other information pertaining to a subscriber' [in 18 U.S.C. § 2702(a)(3)] is broad" and that since the "information [requested by the FBI] is associated with a particular subscriber, even if that subscriber's name is unknown" it cannot be disclosed under the ECPA unless the disclosure falls within one of the ECPA exceptions.

As described in Chapter Two, the information the on-site providers gave to CAU personnel in response to their sneak peek requests often included more detailed information about the subscribers or customers than simply whether the provider had records regarding particular telephone numbers or persons. Therefore, we concluded that this information also was information "associated with a particular subscriber" within the meaning of 18 U.S.C. § 2702(a)(3).

As described above, the ECPA prohibits the disclosure to the government of toll records or information related to a subscriber except in certain limited circumstances set forth in the statute. The relevant exceptions require providers to disclose such information in response to compulsory legal process, such as national security letters, and also permit voluntary disclosures based upon the providers' good faith belief of a qualifying emergency.[84] We found that the FBI did not serve legal process under the ECPA for the information it received pursuant to sneak peeks.

In addition, we do not believe that the FBI's sneak peek practice complied with the ECPA's emergency voluntary disclosure provision for several reasons. First, the practice was described to us as a routine occurrence in the CAU, not limited to "exigent" circumstances. Second, some of the specific instances where the sneak peek practice was used included media leak and fugitive investigations, which clearly did not meet the emergency voluntary disclosure provision. Third, the FBI's lack of internal controls over the sneak peek practice made it impossible for us – or the FBI – to reliably determine how many or in what circumstances sneak peek requests were made, and what the providers were told or believed about the reasons for these requests. Therefore,

---

[83] The OLC identified a very narrow exception under 18 U.S.C. § 2702(a)(3) for disclosure of whether a particular telephone number was among those assigned or belonging to the provider but not "whether the provider has given [the number] to a subscriber."

[84] As described previously, prior to March 2006, this exception required the provider to have a "reasonable belief" that a qualifying emergency existed.

we found that the FBI's sneak peek practice violated the ECPA in many cases.[85]

C. Calling Circle/Community of Interest [redacted]

In addition, we believe that the community of interest [redacted] practices used by the FBI were improper.

First, the FBI's lack of documentation made it difficult to determine under what circumstances and how often community of interest [redacted] were conducted. We identified 52 exigent letters and over 250 NSLs and 350 grand jury subpoenas containing requests for community of interest [redacted] However, we could not determine whether Company A in fact [redacted] such [redacted] in response to all these requests and, if so, whether the [redacted] were limited on an ad hoc basis, for example, [redacted] Nor could we determine how often records or information about the telephone numbers other than the numbers listed in the legal process or exigent letters were provided to the FBI. Similarly, while Company A records show that from 2004 through 2007 the on-site Company A analysts used the Company A community of interest [redacted] to review records for 10,070 [redacted] telephone numbers, Company A could not distinguish whether these numbers were [redacted] as part of Company A's [redacted] service or in response to FBI requests. Company A also could not tell us whether these [redacted] records were actually provided to the FBI.[86]

Second, when FBI personnel issued NSLs that included requests for community of interest [redacted], they did not consistently assess the relevance of the [redacted] numbers before making the request. Instead, community of interest requests were often included in the boilerplate attachments to NSLs. The FBI issued NSLs that requested community of interest [redacted] without conducting, or documenting in the approval ECs, any

---

[85] In a draft of this report given to the FBI in April 2009, the OIG recommended that the FBI issue guidance specifically prohibiting the use of sneak peeks. In June 2009, the FBI posted guidance on its Corporate Policy Intranet prohibiting sneak peek practices. The guidance referred to the OLC legal opinion and also stated that FBI employees "may not informally seek statutorily protected information prior to the issuance of process." The FBI told us that this guidance will be incorporated into the next revision of its Domestic Investigations and Operations Guide.

[86] As noted above, we believe that most of Company A's community of interest [redacted] without requests from the FBI as part of Company A's [redacted] service, and records were not provided to the FBI. (S//NF)

assessment of the possible relevance of [redacted] telephone numbers to the underlying investigation. Absent such an assessment, we believe the FBI did not satisfy the ECPA requirement to issue NSLs in national security investigations only upon certification by those authorized to sign NSLs that the records are relevant to authorized national security investigations.[87] Moreover, although we identified instances in which some community of interest [redacted] requests were limited to telephone numbers with [redacted] or from [redacted], we do not believe these limitations necessarily satisfied the ECPA certification requirement or corresponding provisions of the Attorney General's NSI Guidelines and FBI policy.[88]

Third, FBI personnel who made the decisions to request community of interest [redacted] after reviewing [redacted] records were not among the officials to whom the FBI Director delegated authority under the ECPA to sign NSLs. CAU Intelligence Analysts and SSAs are subordinate to the FBI officials who are authorized to sign NSLs. Yet, after reviewing the [redacted] records, these subordinate FBI employees sometimes asked the on-site Company A analysts to provide [redacted] records. We believe that if the signers of the NSLs did not themselves determine that the [redacted] records were relevant to an authorized counterterrorism investigation, the [redacted] of the [redacted] records would violate the ECPA, even if the community of interest request was included in the NSL attachment.

Fourth, when the FBI received digital records from Company A in response to its community of interest [redacted] requests, the records did not identify or otherwise distinguish toll billing records [redacted] in legal process or exigent letters. Moreover, the FBI uploaded responsive records into a [redacted] database, and the FBI did not separate records on the target numbers listed in legal process from the records [redacted] and provided in response to community of interest [redacted] requests. It is therefore likely that the records of thousands of calls to and from [redacted] telephone numbers were uploaded into the [redacted] database without the required relevance assessment by an authorized FBI official. Without additional research on these telephone

---

[87] See 18 U.S.C. § 2709(b).

[88] Limiting a community of interest [redacted] request to calls to or from [redacted] numbers by itself is not necessarily a relevance assessment. Similarly, limiting community of interest [redacted] requests to the [redacted] calls from a [redacted] would not necessarily satisfy the ECPA relevancy requirement.

numbers, the FBI is unable to identify which records are associated with [redacted] numbers and whether those numbers were relevant to the underlying investigations for which they were requested.

Fifth, when Company A [redacted] its community of interest [redacted] to review [redacted] telephone numbers as part of its [redacted] services in the absence of specific [redacted] requests from the FBI, the on-site Company A analysts sometime provided to the FBI information pertaining to a subscriber or a customer of its service. This also appears to violate the ECPA statute, which prohibits communications service providers from divulging "a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." See 18 U.S.C. § 2702(a)(3).

Finally, FBI e-mails indicate that in late 2004 FBI OGC attorneys became aware of but did not object to community of interest [redacted] requests for [redacted] telephone numbers. In May 2006, these attorneys also approved use of a boilerplate attachment for NSLs served on the on-site providers. This attachment listed community of interest records and 17 other types of information that "may be considered by [the providers] to be toll billing records." Although FBI General Counsel Caproni and NSLB Deputy General Counsel Thomas concluded that community of interest [redacted] requests for [redacted] telephone numbers could satisfy the ECPA relevance standard such that the FBI would not have to issue separate NSLs for the [redacted] records, the FBI did not issue written guidance on when such requests were appropriate. In March 2007, on the advice of the FBI OGC, the CTD directed that such requests [redacted]

In November 2007, the FBI OGC and the CTD generated draft guidance that incorporates the principle that the [redacted] Although this guidance has not yet been finalized, current FBI policy as stated in the Domestic Investigations and Operations Guide (DIOG) requires that the NSLB Deputy General Counsel approve community of interest requests and that [redacted] telephone numbers for which information has been obtained be reported to NSLB for congressional reporting purposes. In addition, the DIOG requires that the NSL approval EC demonstrate the relevance of [redacted] information to the national security investigation.

We agree with the principles articulated in the November 2007 draft guidance and the DIOG, [redacted] We concluded that in order to satisfy the requirements of the ECPA, relevance must be determined before the request is made.[89] We also agree that senior FBI officials and a Department attorney should approve such requests and that the record of telephone numbers [redacted] pursuant to these requests should be created for purposes of congressional reporting on NSL usage by the Department. However, CTD's guidance still has not been issued.

In sum, we concluded that the FBI's community of interest [redacted] practices were inappropriate and likely resulted in the FBI obtaining and uploading into a [redacted] database thousands of telephone records for [redacted] telephone numbers without the required certifications of relevance to an authorized international terrorism investigation by an authorized FBI official. In addition, we found that the FBI is unable to identify with certainty today which records in the database are associated with [redacted] numbers and whether those numbers were relevant to the underlying investigations for which they were requested. We also concluded that the FBI failed to review the implications of Company A's community of interest [redacted] capability when Company A first posted its analysts on-site at the CAU; failed to issue written guidance in coordination with the FBI OGC about the circumstances in which such requests were appropriate under the ECPA; failed to establish an approval process for such requests or ensure that the predication for these requests was properly documented in approval ECs; and failed to ensure that records sought in community of interest [redacted] requests were included in required reports to Congress on NSL usage.

---

[89] After reviewing a draft of this report, the FBI identified for us another draft policy, dated February 2008, that did not require approval by a Department attorney. We believe that the approach in the November 2007 draft guidance is superior. No final guidance has yet been issued by the FBI.

CHAPTER THREE
ADDITIONAL USES OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS

We found other irregularities in the way the FBI obtained telephone records and used the on-site communications services providers located in the Counterterrorism Division's (CTD) Communications Analysis Unit (CAU). As described in this chapter, we determined that the FBI obtained calling activity information from Company A and Company C on pre-determined "hot numbers" without legal process. In addition, in three media leak investigations, the FBI requested [redacted] and in two instances obtained reporters' toll billing records or calling activity information without prior approval by the Attorney General, in violation of federal regulation and Department policy.

We also determined that FBI Supervisory Special Agents (SSA) made inaccurate statements to the Foreign Intelligence Surveillance Court (FISA Court) in characterizing the source of records that the Department of Justice relied upon to support applications for electronic surveillance or pen register and trap and trace orders. In addition, an SSA assigned to the CAU signed administrative subpoenas to cover the FBI's earlier acquisition of telephone toll billing records through exigent letters or other informal requests in violation of the ECPA and the statute authorizing the use of administrative subpoenas in narcotics investigations (21 U.S.C. § 876). This CAU SSA and an SSA assigned to the FBI's [redacted] Field Division together signed 5 administrative subpoenas for telephone records that were dated from 7 to 44 days after the FBI had obtained the records without legal process, in violation of the ECPA.[90]

I. Obtaining Calling Activity Information on "Hot Numbers"

From 2004 through 2006 the FBI used a service offered by Company A and Company C referred to as "hot number [redacted]." When using this service, the FBI asked Company A or Company C to provide calling activity information for telephone numbers that CAU or other FBI personnel had identified as "hot numbers." As described below, the FBI sometimes included specific parameters in its requests – such as whether there were calls to or from a particular area code [redacted] After the [redacted] were set on the hot numbers, and without receiving court orders or any type of legal process

---

[90] As described below, some of these problems occurred in combination with the use of exigent letters or other informal requests.

authorizing release of this information, the on-site Company A and Company C employees informed CAU personnel when the hot numbers [redacted] In addition, the providers sometimes gave the FBI more information than just the fact that calling activity existed, such as call originating and terminating information. Based on records we examined from Company A, Company C, and the [redacted], we determined that the FBI requested calling activity information on at least 152 telephone numbers and obtained calling activity information for at least 42 hot numbers from 2004 through 2006.[91]

A. Legal Authority for Obtaining Calling Activity Information

The *Stored Communications Act*, 18 U.S.C. § 2701 *et.seq.*, a subtitle of the ECPA which includes the ECPA NSL statute, authorizes the FBI to obtain historical, stored data from communications service providers. However, the case law is unsettled whether legal process issued under the *Stored Communications Act* can also be used prospectively to obtain records that come into existence after the issuance of the legal process.[92]

---

[91] As described below, Company A told us that 87 telephone numbers were placed on a "hot" list by Company A for the FBI, but only 42 telephone numbers [redacted] We found documentation indicating that Company C placed at least 65 telephone numbers on a list for [redacted] and we found evidence that at least some of these numbers [redacted]

[92] This issue has arisen in the context of government requests to obtain prospective cell site location information. Courts are divided on whether the government can obtain such information through legal process issued pursuant to the *Stored Communications Act* (and the *Pen Register Act*), or whether the government must obtain a warrant based on probable cause. See, e.g., *In the Matter of the Application,* 534 F. Supp. 2d 585, 599-600 (W.D. Pa. 2008)(W.D. Pennsylvania decision), *aff'd,* 2008 WL 4191511 (W.D. Pa. 2008). Several cases denying the government's requests for prospective cell cite location information pursuant to the *Stored Communications Act* rely in part on the fact that the Act does not authorize collections of prospective information. See, e.g., *In re U.S. for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers,* 416 F. Supp. 2d 390, 395 (D. Md. 2006); *In re Application of the U.S. for an Order (1) Authorizing the Use of Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information,* 396 F. Supp. 2d 294, 311-14 (E.D.N.Y. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F. Supp. 2d 747, 760-62 (S.D. Tex. 2005). But see, *In re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone,* 460 F.Supp2d 448, 452-459 (S.D.N.Y. 2006)(holding that the *Stored Communications Act* contains no explicit limitation on the disclosure of prospective data, while acknowledging that a majority of courts to have addressed the government's theory that the *Pen Register Act*, in combination with the *Stored Communications Act*, supports disclosure of prospective cell site location information have denied the government's applications); and *In re U.S. for an Order Authorizing the Use of Two* (Cont'd.)

The Pen Register Act, which authorizes court-ordered electronic monitoring of non-content telephone calling activity, can be used to obtain prospective calling activity information.[93] The Pen Register Act authorizes the installation of pen register and trap and trace devices in both criminal investigations and also in national security investigations pursuant to the Foreign Intelligence Surveillance Act (FISA).[94] Pen registers identify outgoing dialed telephone numbers, while trap and trace devices identify incoming telephone numbers. Pen registers and trap and trace devices require court orders (pen/trap orders) and are issued for a fixed period of time, not to exceed 60 days.

B. Hot Number [redacted]

We found that Company A and Company C [redacted] During the period covered by our review, the FBI identified 87 "hot numbers" for Company A to [redacted] and at least 65 hot numbers for Company C to [redacted]. The FBI did not provide legal process to Company A or Company C either before or after it identified the numbers and received calling activity information.

We describe below details about the FBI's acquisition of this information, what the CAU Unit Chiefs and attorneys in the FBI Office of the General

---

Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 207 (E.D.N.Y. 2008) (granting prospective cell site location information and stating the *Stored Communications Act* does not preclude the ongoing disclosure of records to the government once they are created.

Recent cases have questioned whether any cell site location information – historical or prospective – is available under the *Stored Communications Act*, or whether cell site location information is excluded because the cell phone is then a "tracking device' excluded under the Act. The W.D. Pa. decision has been appealed, and the 3rd Circuit's ruling will be the first appellate decision on the issue. Prior to the appeal to the 3rd Circuit, the Department of Justice concluded that prospective cell site location information was encompassed within the terms of the FISA pen register provision, as amended by the Patriot Reauthorization Act. However, the Department is awaiting the 3rd Circuit's decision before pursuing this position with the FISA Court.

[93] The Pen Register Act, which is part of the ECPA, authorizes the FBI to obtain court orders for the real-time interception of outgoing or incoming telephone numbers to a target telephone. See *Electronic Communications Privacy Act of 1986*, Title III ("Pen Register Act"), Pub. L. No. 99-508, codified as amended at 18 U.S.C. §§ 3121 – 27 (2000 & Supp. 2002). In criminal cases, the courts are authorized to enter ex parte orders for pen registers or trap and trace devices upon certification that the information likely to be obtained "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2).

[94] See 18 U.S.C. §§ 3121 – 27; 50 U.S.C. § 1842(e).

Counsel (FBI OGC) knew about the practice, and our analysis of this practice.

1. Company C

Company C's hot number [redacted] feature was described in a May 23, 2003, proposal of work that led to a contract between the FBI and Company C for the provision of Company C's on-site services in the CAU. A CTD Electronic Communication (EC) dated May 28, 2003, that requested funding for this contract stated that the "statement of work also allows for the [redacted]"[95] However, we found that the FBI did not establish any procedures, guidance, oversight, or training for CAU personnel regarding the use of hot number [redacted] We also found no evidence that NSLB attorneys conducted any legal review of the proposed Company C contract in 2003, including the legal implications of hot number [redacted] Further, we found no evidence that FBI attorneys evaluated the legal implications of hot number [redacted] after Company C posted its on-site employee in the CAU in April 2004, or thereafter, until 2007.[96]

A CAU SSA told us that to obtain information on targeted numbers he provided a list of telephone numbers to Company C [redacted] Company C would then notify him of calling activity by the targeted numbers. The on-site Company C's employee's log indicates that in some instances the Company C employee provided more information than just the fact of calling activity, such as call originating and terminating information.

A Company C representative confirmed for us that Company C did not receive legal process from the FBI to initiate any hot number [redacted] and also did not receive legal process after it had provided information to the FBI about the hot numbers. The Company C representative also said that Company C could not determine how often the feature was used or [redacted] at the request of the FBI during the 4-year period covered by our review. However, based on information provided to us by a CAU SSA who used the Company C service and our review of Company C documents, we estimated that the FBI asked Company C to [redacted] for at least 65 telephone numbers between May 2004 and September 2006.

---

[95] The EC was initiated by the CAU and was approved by Thomas Harrington, the Deputy Assistant Director of the CTD.

[96] As described below, we found that based on inaccurate information provided to her in April 2007, FBI General Counsel Caproni came to the erroneous conclusion that hot number [redacted] had not been used by the CAU.

Company C records also show that the FBI was billed for and paid a separate fee to Company C for this hot number [redacted] We found that the FBI paid Company C [redacted] for hot number [redacted] during the period from 2002 through 2006.[97]

2. Company A

Documents that Company A provided to the FBI as part of Company A's 2004 contract proposal for on-site services in the CAU described Company A's capability to "track, follow, and capture fugitives, terrorists and other criminals" and [redacted] to search for known fugitives (i.e. [redacted]) . . . ." One of Company A's stated goals in the proposal was to create a report "to be customized specifically for the FBI based upon input data such as hot target list, significant numbers, secure data, etc."

An on-site Company A analyst told us that Company A's [redacted] capability was [redacted] Company A [redacted] He said he could not recall when information on "hot numbers" was requested by the CAU.[98] Use of this capability enabled the FBI to learn in [redacted] that there was calling activity by the hot numbers. Additionally, if specified by the FBI requesters, Company A would [redacted] the requesters only to calling activity within certain parameters, such as calls to or from a particular area code [redacted] The on-site Company A analyst said that while he received details of the calling activity by the hot numbers – including the date, time, and duration of the calls – he informed the FBI requesters only that there had been calling activity. The Company A analyst told us that he typically notified the CAU or other FBI requesters of the calling activity verbally.

The on-site Company A analyst who set many of the Company A hot number [redacted] told us that he did not discuss with anyone in the FBI or Company A whether legal process would be served before he provided calling activity information. He also said that he did not receive any type of legal

---

[97] Company C's schedule of payments shows that Company C billed the FBI at a rate of [redacted] per month in fiscal year (FY) 2006 for [redacted] for a maximum of 1,000 telephone numbers. A Company C representative told us that Company C also billed the FBI at a flat rate in FY 2002 and FY 2004.

[98] Company A's [redacted] was different from another Company A capability called "hot number [redacted]." Hot number [redacted] permits Company A to collect all toll billing records at set intervals, such as every 4, 8, or 12 hours, while [redacted] provided [redacted] information about calling activity on particular telephone numbers. Company A told us that the FBI never received information or records from Company A in connection with its "hot number [redacted]" service, and we found no contrary evidence.

process or exigent letters for the calling activity information that he provided to the FBI.

Based on information we obtained from Company A, we found that from June 2005 until December 2006, FBI personnel asked Company A to [redacted] for at least 87 telephone numbers. A Company A representative told us that of the 87 telephone numbers, 42 telephone numbers generated calling activity information. The attorney stated that information [redacted] was conveyed to the Company A analyst [redacted] of the calling activity. A CAU SSA who used the [redacted] feature told us that typically he did not receive notification of the calling activity generated on his hot numbers [redacted], usually through an e-mail from the on-site Company A analyst.

Unlike Company C, Company A provided its hot number [redacted] service as part of its overall contract for services to the FBI, and Company A did not impose separate charges for setting hot number [redacted]

A CAU SSA told us that CAU Unit Chief Rogers told him to use Company A's and Company C's hot number [redacted] service in connection with the [redacted] fugitive investigation being conducted by the FBI's [redacted] Field Division and in connection with another fugitive investigation being conducted by the FBI's [redacted] Field Division.[99] Related to the [redacted] investigation, the SSA recalled attending a "meet and greet" session with a [redacted] Field Division supervisor in the CAU that was also attended by CAU Unit Chief Bassem Youssef. The SSA said that the purpose of the meeting was for the CAU to describe its resources and how the CAU could support the [redacted] fugitive investigation.[100] Several months after this meeting, the FBI began identifying hot numbers associated with the [redacted] investigation and giving them to the on-site Company A analyst. The Company A analyst thereafter notified both the CAU SSA and the [redacted] Field Division case agent by e-mail [redacted] of the telephone numbers.

---

[99] The CAU SSA told us that several other CAU personnel used the hot number [redacted] feature in other FBI investigations. We received independent information that corroborated the CAU SSA's statement regarding other CAU personnel using the hot number [redacted] for other CAU cases.

[100] [redacted]

The CAU SSA said that if the case agent was interested in obtaining toll billing records or subscriber information on the hot numbers, the FBI would issue administrative subpoenas or exigent letters for those records.[101] The CAU SSA estimated that he gave Company A a total of 20 telephone numbers in connection with both the [redacted] and the other fugitive investigation.[102]

In our investigation, we found no evidence that the FBI established procedures, guidance, oversight, or training to ensure that CAU personnel sought appropriate legal authority when they asked Company A or Company C to provide calling activity information in response to the FBI's requests [redacted] on hot numbers.

C. FBI OGC and CAU's Unit Chiefs' Knowledge of Hot Number [redacted]

In this section we examine what CAU Unit Chiefs and FBI OGC attorneys knew about hot number [redacted]

CAU Unit Chiefs and FBI OGC attorneys told us they were unaware of the use of hot number [redacted] by CAU personnel. CAU's first Unit Chief, Glenn Rogers, said he thought Company A offered a hot number [redacted] capability [redacted] However, Rogers said he was not certain whether Company A's hot number [redacted] was ever utilized by the FBI and also was not certain what authority the FBI would use to acquire the calling activity information.

---

[101] The CAU SSA told us that before notifying FBI requesters of calling activity by the hot numbers, Company A used "sneak peeks" to first determine whether the calling activity was associated with [redacted] have investigative value. After the Company A analyst made this determination, he notified the FBI of calling activity by telephone numbers that might be of investigative interest.

[102] The CAU SSA said he recalled first learning about hot number [redacted] at a meeting in 2004 he attended with CTD Section Chief Michael Fedarcyk, CAU Unit Chief Rogers, and a female NSLB attorney whose name he could not recall. He stated that they discussed the use of "forward-looking subpoenas" or "anticipatory search warrants" that would request information [redacted] The CAU SSA told us that the NSLB attorney said that she approved of forward-looking subpoenas. He said he was not certain whether the legal processes discussed at the meeting were grand jury subpoenas or NSLs, but that the NSLB attorney said that there was no legal problem with forward-looking subpoenas. He also said that no FBI attorneys ever told him that they had legal reservations about hot number [redacted] We could not identify any NSLB attorney at this meeting, and the FBI could not locate documentation of any legal review by the NSLB of hot number [redacted] or other features of the Company A contract from 2003 through 2007.

Rogers's successor as CAU Unit Chief, Bassem Youssef, told us that hot number [redacted] was a feature offered by Company C whereby the FBI "would have authority on a particular target number" [redacted] However, Youssef said he did not know what the authority was for hot number [redacted] He said that after making inquiries with an FBI field division in 2006 and 2007, he believed that the FBI had never used Company C's hot number [redacted] capabilities.

On September 12, 2006, a CTD Contracting Officer's Technical Representative (COTR) sent an e-mail to Youssef asking him whether the CAU still needed Company C's hot number [redacted] service for which the FBI was then paying [redacted] per month.[103] Youssef responded that he no longer needed the hot number [redacted] feature and, in the event it were needed in the future, "we would ask for it on a month to month basis." The COTR asked Youssef to contact Company C and let it know that the FBI was cancelling the service.

On September 18, 2006, Youssef informed the Company C on-site employee by e-mail that "we no longer need the hot # [redacted] feature and we'll re-institute it in the future if we need it again." The Company C employee replied by e-mail that Company C was then using the feature for two FBI investigations: the [redacted] fugitive investigation being conducted by the FBI's [redacted] Field Division and a second fugitive investigation being conducted by the [redacted] Field Division. The Company C employee asked Youssef to confirm that he wanted to terminate hot number [redacted] for both investigations, which Youssef confirmed.

Marion Bowman, who was the National Security Law Branch (NSLB) Deputy General Counsel when the contracts were executed, told us that he was unaware of and did not review the contracts with Company A, Company B, or Company C to provide on-site services at the CAU and did not know the specifications for the contracts. Bowman's successor as NSLB Deputy General Counsel, Julie Thomas, told us that she recalled reviewing the contracts with the on-site providers for the first time in late 2006, after receiving a draft of the OIG's first NSL report. She stated that she recalled identifying the provision of the contract discussing hot number [redacted] and concluding that the FBI could obtain this type of information only through a pen register. She said that

---

[103] Youssef had co-signed the Company C monthly invoices that included charges for this feature for 12 consecutive months prior to the COTR asking him whether Company C's hot number feature was needed. However, the invoices only referenced a lump sum amount and did not itemize the particular services provided for the charges.

she also recalled learning in April 2007 that Caproni had been informed at that time that the service had never been used. Thomas said she did not learn until shortly before her final OIG interview for this report in August 2008 that the FBI had paid Company C for hot number [redacted]

Caproni told us that based on information she had received from FBI personnel in April 2007, she believed that hot number [redacted] had never been used by the FBI. In an April 2007 e-mail to CTD Assistant Director Joseph Billy, Jr., and other CTD personnel, Caproni instructed that if the CTD sought to use hot number [redacted] CTD must first contact the FBI OGC. She added that the FBI OGC needed to understand the technical aspects of the feature before providing a legal opinion about its use. In 2008, Caproni told us that her concern at the time was that the feature "might be an unlawful pen register."[104]

D. OIG Analysis

We found that the FBI sought calling activity information on 152 "hot" telephone numbers from Company A and Company C and was provided information on at least 42 of those numbers. Company A provided information that there had been calls made to or from the numbers identified by the FBI, sometimes in response to specific inquiries from the FBI about whether calling activity existed to or from a particular area code [redacted] We also found evidence that Company C also may have provided more information than just the existence of calling activity, such as call originating and termination information.

We believe that the calling activity information requested by and conveyed to the FBI about these hot numbers required legal process. Although the information given to the FBI by Company A and Company C on these hot numbers was less extensive than the type of information typically provided in response to NSLs or pen register/trap and trace orders, it constituted "a record or other information pertaining to a subscriber or a customer" under the ECPA.[105]

As discussed in Chapter Two of this report in connection with our analysis of "sneak peeks," the Department's Office of Legal Counsel concluded, and we agree, that the ECPA ordinarily bars communications service providers

---

[104] After reviewing a draft of this report, the FBI stated that, subsequent to her OIG interview, Caproni concluded that as a matter of law, hot number [redacted] did not implicate the Pen Register Act.

[105] 18 U.S.C. § 2702(a)(3).

from telling the FBI, prior to service of legal process, whether a particular account exists. We also concluded that if that type of information falls within the ambit of "a record or other information pertaining to a subscriber to or customer of such service" under 18 U.S.C. § 2702(a)(3), so does the existence of calling activity by particular hot telephone numbers, absent a qualifying emergency under 18 U.S.C. § 2702(c)(4).

We found no evidence that the FBI requested or the providers gave the FBI this information pursuant to the emergency voluntary disclosure provision of the ECPA. Instead, it appears that the information was disclosed as part of the contractual arrangement between the providers and the FBI, and was primarily used in connection with fugitive matters that did not qualify as emergency situations under 18 U.S.C. § 2702. Therefore, we believe that the practice of obtaining calling activity information about hot numbers in these matters without service of legal process violated the ECPA.

We also found it both surprising and troubling that Rogers, as Unit Chief of the CAU and the official responsible for knowing and assessing the tools used by his subordinates to obtain information from the on-site providers, said he was not certain whether Company A's hot number [redacted] feature was ever utilized by the FBI. We likewise were troubled that Youssef, Roger's successor as CAU Unit Chief, told us that he did not believe that hot number [redacted] was used.

In addition, from the inception of the FBI's contractual relationship with the three providers beginning in 2003, senior FBI officials knew that the CAU would be handling telephone transactional records which the FBI could lawfully obtain pursuant to the ECPA. However, the FBI failed to ensure that responsible officials in the CTD and the FBI OGC's NSLB reviewed the proposed and final contracts with the providers to ensure that the agreements conformed to the requirements of the ECPA and other relevant laws and policies. The General Counsel and the NSLB Deputy General Counsel did not review the contracts or associated documents with the on-site providers until late 2006 or early 2007. We believe that the absence of timely legal review was a significant management failure by the FBI. In part because NSLB attorneys did not review the contract proposals with the on-site providers, they were unaware of the specific services provided, including the hot number [redacted] service.

In Chapter Six of this report we provide recommendations to address our findings from this portion of our review. We believe the FBI should carefully review the circumstances in which FBI personnel asked the on-site communications service providers [redacted] "hot numbers" to enable the Department to determine if the FBI obtained calling activity information under circumstances that trigger discovery or other obligations in any criminal investigations or prosecutions. Our recommendations also are

designed to ensure that FBI personnel receive periodic training on the FBI's authorities to obtain telephone records from communications service providers and that FBI OGC attorneys and program managers, including successor officials serving in these positions, are fully familiar with any FBI contracts with communications service providers.

II. Seeking Reporters' Telephone Records Without Required Approvals

We determined that in three media leak investigations the FBI requested, and in two of these instances obtained from the on-site communications service providers, telephone records or other calling activity information for telephone numbers assigned to reporters. However, the FBI did not comply with the federal regulation and Department policy that requires Attorney General approval and a balancing of First Amendment interests and the interests of law enforcement before issuing subpoenas for the production of reporters' telephone toll billing records.[106]

In the sections that follow, we describe the federal regulation and Department policies governing the issuance of subpoenas for the telephone toll billing records of members of the news media, the facts we found regarding each of these three leak investigations, and our analysis of each of these three cases.

A. Federal Regulations and Department Policies

Because of the First Amendment interests implicated by compulsory process to obtain reporter's testimony or their telephone records, 28 C.F.R. § 50.10 (2004) requires special approvals and other advance steps before Department employees are permitted to issue subpoenas for reporters' testimony or the production of their telephone records.

Specifically, this regulation requires that before issuance of such subpoenas, "all reasonable attempts should be made to obtain information from alternative sources."[107] This regulation also requires the Department to attempt to negotiate the voluntary appearance of the news media personnel or the voluntary acquisition of their records. If the records are needed for a criminal investigation, the regulation requires "reasonable grounds to believe, based on information obtained from non-media sources, that a crime has

---

[106] See 28 C.F.R. § 50.10.

[107] 28 C.F.R. § 50.10(b).

occurred, and that the information sought is essential to a successful investigation . . . ."[108] Any requests for such subpoenas must be approved by the Attorney General in accordance with principles specified in the regulations.[109]

The regulation also requires that if the telephone toll records of members of the news media are subpoenaed without the required notice, the affected member of the news media must be notified "as soon thereafter as it is determined that such notification will no longer pose a . . . substantial threat to the integrity of the investigation" and, in any event, within 45 days of any return in response to the subpoena.[110] Finally, the regulations state that failure to obtain the prior approval of the Attorney General "may constitute grounds for an administrative reprimand or other appropriate disciplinary action."[111]

Department policies supplement this regulation by specifying the information required to be included in requests seeking Attorney General approval for issuance of such subpoenas.[112]

At the time of the investigations at issue, the FBI's media leak investigations were governed by the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations.[113] In addition, at the time of these investigations, leak investigations involving

---

[108] 28 C.F.R. § 50.10(f)(1).

[109] 28 C.F.R. § 50.10(g).

[110] Section 50.10(g)(3) of 28 C.F.R. states:

> When the telephone toll records of a member of the news media have been subpoenaed without the notice provided for in paragraph (e)(2) of this section, notification of the subpoena shall be given to the member of the news media as soon thereafter as it is determined that such notification will no longer pose a clear and substantial threat to the integrity of the investigation. In any event, such notification shall occur within 45 days of any return made pursuant to the subpoena, except that the responsible Assistant Attorney General may authorize delay of notification for no more than an additional 45 days.

[111] 28 C.F.R. § 50.10(n)(2004).

[112] See United States Attorneys' Manual § 9-13.400, "News Media Subpoenas; Subpoenas for Telephone Toll Records of News Media; Interrogation, Arrest, or Criminal Charging of Members of the News Media."

[113] As noted previously, several sets of Attorney General Guidelines were revised and consolidated into the Attorney General's Consolidated Guidelines, which took effect in December 2008.

classified information were categorized by the FBI as espionage investigations because they potentially involved violations of the Espionage Act.

B. First Matter

1. Background

[redacted] An FBI squad supervisor told us that in response the FBI CTD opened a counterterrorism investigation into [redacted]

[redacted] the Washington Post and The New York Times published articles [redacted][114] The Washington Post article referred to [redacted] indicating that, [redacted] The New York Times article referred to information from a [redacted] given to FBI investigators about [redacted]

2. The Investigation of the Leak of Information to the Media

The FBI's [redacted] Field Office initiated a leak investigation [redacted] to determine whether U.S. government employees or others had violated criminal laws prohibiting the release of classified information in connection with the Washington Post and The New York Times articles. The investigation was assigned to a [redacted] Field Office counterintelligence squad, and a case agent was assigned to the matter. The U.S. Attorney's office in [redacted] assigned an Assistant United States Attorney (AUSA) to the investigation on or about October [redacted].

---

[114] [redacted]

According to our interviews and review of FBI documents, in November [redacted] the AUSA assigned to the investigation discussed with the FBI case agent the possibility of seeking Department approval to subpoena the telephone toll billing records of the reporters who wrote the two articles in the Post and the Times. The case agent and the AUSA told us that they were both aware at that time of the Department's regulation that requires Attorney General approval for obtaining reporters' telephone toll records, and they recalled discussing the possibility of seeking such approval. They both stated that before taking this step they believed they should determine whether the toll billing records of [redacted] calls made by the reporters and others [redacted] could be obtained from the on-site communications service providers located in the CAU.

a. The [redacted] Field Office Requests CAU Assistance

On November 5, [redacted], the case agent sent an e-mail asking another Special Agent in the [redacted] Field Office to inquire, in the other agent's capacity as his squad's liaison to the CAU, whether the on-site communications service providers could obtain telephone toll records of U.S. persons making [redacted] calls [redacted]. The case agent's November 5 e-mail listed 12 [redacted] telephone numbers, 8 of which were identified in the e-mail as belonging to Washington Post reporters [redacted] and Washington Post researcher [redacted] and New York Times reporters [redacted] The e-mail identified a 7-month time period – a few months before and a few months after the published articles – as the time period of interest for the leak investigation.

Three days later, the Special Agent who had received the e-mail from the case agent forwarded the e-mail to a CAU SSA – also copying the case agent. The Special Agent asked the CAU SSA in his forwarding e-mail whether, as a general matter, [redacted] calls generated by the identified telephone numbers originating [redacted] would be captured by the on-site providers' systems.

The CAU SSA replied by e-mail on November 10, [redacted], asking whether the Special Agent wanted him "to start pulling these tolls" and, if so, "what is the source of the request . . . NSL or FGJ subpoena?" The CAU SSA's e-mail was copied to the case agent's supervisor, but not to the case agent.

We found no e-mail response to the CAU SSA's questions, either from the Special Agent or anyone else. When we asked the Special Agent about this e-mail, he told us that he did not recall it.

In September and December [redacted], a CAU SSA and other CAU personnel provided briefings to the [redacted] Field Office's [redacted] squads, including the case agent assigned to the leak investigation (who attended one of the briefings), about the resources available to support FBI investigations from the on-site communications service providers.

Five days after the December [redacted] briefing, the case agent on the leak investigation sent an e-mail to a CAU Intelligence Analyst who had participated in the briefing, asking the same questions that had been previously posed to the CAU SSA by the Special Agent: could the on-site providers obtain toll records on [redacted] calls originating [redacted] telephone numbers [redacted] The case agent stated in his December 14 e-mail to the CAU Intelligence Analyst, "You suggested that we run this past you before we send the subpoena." The e-mail also stated, "We likely will proceed with a federal grand jury subpoena, with the AUSA requesting DOJ approval before issuing the subpoena." The case agent also noted in the e-mail that the Special Agent who had originally forwarded this request to the CAU had already "touched base with [the CAU SSA] preliminarily on this matter."

In response, on December 14, [redacted], the CAU Intelligence Analyst sent the case agent a sample NSL for toll billing records. The Intelligence Analyst also stated in his e-mail that he would check with the CAU SSA "to make sure he hasn't already pulled the tolls." We found no evidence indicating that the CAU SSA received this e-mail or that he was informed about any planned request for DOJ approval.

However, in the absence of any request from the case agent or anyone in the FBI, the CAU SSA issued an exigent letter dated December 17, [redacted], to Company A for telephone records of the reporters and others listed in the case agent's November 5, [redacted], e-mail. We determined that the SSA did this without further discussion with the case agent or the Special Agent who had asked only whether such records could be obtained through the on-site providers, not that the records should be obtained.[115]

The CAU SSA's exigent letter sought records on nine telephone numbers, seven of which were identified in the e-mail exchanges described above as belonging to Washington Post and New York Times reporters or their news organizations' bureaus in [redacted] The other two numbers were associated

---

[115] We determined that this SSA had issued a total of 115 exigent letters, the second highest number of exigent letters signed by any CAU personnel.

with persons suspected of leaking classified information to the reporters.

The exigent letter did not specify the 7-month interval noted in the case agent's November 5 e-mail, or contain any date restrictions. The exigent letter also stated that the request was made "due to exigent circumstances" and that "subpoenas requesting this information have been submitted to the U.S. Attorney's office who will process and serve them formally on [Company A] as expeditiously as possible." However, this statement was not accurate. A subpoena request had not been sent to the U.S. Attorney's Office at the time the exigent letter was served, or at any time thereafter.

The CAU SSA told us he could not recall why he sent this exigent letter and acknowledged that the case agent had not asked him to do so. He also acknowledged that he knew at the time he signed the letter, based on information previously given to him, that the request included reporters' numbers. He stated that he "had never even read the content of these [exigent] letters," but was "just using the standard forms . . . ." The CAU SSA told us that he used exigent letters based on the guidance he had received from a Company A analyst who told him "explicitly that this was the approved process between the attorneys for [Company A], as well as, you know, . . . the attorneys for the Bureau." He said that when he was assigned to the CAU, his prior experience had been working on Columbian drug trafficking and money laundering and Asian organized crime under the FBI's criminal programs, and he was not aware of any special policies or approval levels needed to obtain reporters' toll billing records.

The CAU SSA also said he did not recall the case agent making any representations about exigent circumstances underlying his inquiry about the availability of the toll billing records. The CAU SSA told us that he could imagine circumstances in which the leak of classified information could present exigent circumstances.[116] He also told us that the case agent's squad supervisor, who was on the initiating e-mail to the CAU for this request, would have known from CAU briefings she attended at the [redacted] Field Office that the CAU would be obtaining telephone records before legal process in a request of this type. However, the case agent told us that he did not tell the CAU SSA who signed the exigent letter that there were any exigent circumstances associated with his inquiry. Similarly, the squad supervisor told us that no one had told her of any exigent circumstances being presented to the CAU SSA in connection with this request.

---

[116] The SSA stated that he considered the leak of "national defense information" to be the type of circumstance for which an exigent letter would be appropriate.

The CAU Intelligence Analyst who had sent the case agent a sample NSL for toll billing records said he did not recall any conversations with the CAU SSA about the exigent letter, but he speculated that he probably discussed it with the CAU SSA. The Intelligence Analyst also told us that he was not aware in December [redacted] about any special approval requirements for obtaining reporters' toll billing records and that the case agent's e-mail reference to obtaining DOJ approval "went over my head." The Intelligence Analyst said that, in hindsight, he thought he and others in the CAU would have proceeded differently had they noticed the case agent's reference to getting DOJ approval. He said he did not recall any discussions at the time about special requirements for obtaining DOJ approval, although he said that he understood that the case agent was working with the AUSA and a subpoena was "in the works."

On December 20, [redacted], the case agent, not aware that an exigent letter had been issued by the CAU SSA and following up on his earlier question whether Company A had the capacity to retrieve the records, sent an e-mail to the CAU Intelligence Analyst asking if there was "any word on whether calling activity for the below listed numbers is retrievable? I will advise you as soon as I get the GJ subpoena from the AUSA on the case." The "below-listed numbers" was a reference to the 12 numbers contained in the agent's November 5, [redacted], e-mail request to the analyst, which was included in the December 20 e-mail chain.

b. FBI Obtains Reporters' Toll Billing Records

On approximately December 22, [redacted], the on-site Company A analyst provided to the CAU the toll billing records requested in the December 17 exigent letter. The analyst provided records for seven of the eight telephone numbers associated with reporters or their news organizations' bureaus in [redacted][117]

We determined that the Company A analyst gave the FBI 22 months of records for Washington Post reporter [redacted] telephone number, of which only 38 days fell within the 7-month period of interest initially identified by the case agent as relevant to the leak investigation. In addition, 22 months of records were provided to the FBI for the telephone number assigned to the Washington Post's [redacted] bureau, of which only 20 days fell within the

---

[117] The Company A analyst advised the CAU that Company A had no toll billing records for the eighth of the reporters' telephone numbers identified in the e-mail, which the FBI believed to be used by [redacted] Company A also produced records for two other telephone numbers specified in the e-mail that were not associated with reporters.

7-month period of interest. For the remaining five numbers, none of the retrieved records provided to the FBI fell within the 7-month period of interest.

In total, Company A provided the FBI with toll billing records for 1,627 telephone calls. Of this total, only three calls (.2 percent) fell within the 7-month period of interest identified by the case agent as relevant to the investigation (two calls in [redacted] records and one call in records of the Washington Post's bureau in [redacted]

We determined that CAU personnel uploaded all of the reporters' and news organizations' records for the 1,627 telephone calls provided by Company A into a [redacted] database on December 22, [redacted], where they were available for searching by authorized FBI and other [redacted] personnel.[118]

We also determined that on January 5, [redacted], the CAU Intelligence Analyst replied to the case agent's December 20, [redacted], e-mail asking whether the toll billing records of interest were retrievable. In his January 5 response, the Intelligence Analyst forwarded to the case agent two CAU "trace reports for the calling activities associated with your [redacted] target numbers."[119] One of the files attached to the e-mail was titled, "CAU3983FBItollsonly.xls." The analyst also stated in the e-mail, "We didn't have any [Company A] data" for three of the target numbers. The January 5 e-mail also stated that the analyst would send the "raw data" to the agent when he received the grand jury subpoena.

We found that both trace reports attached to the CAU analyst's January 5 e-mail contained all of the telephone data acquired by Company A concerning seven telephone numbers the case agent had identified as belonging to reporters or media organizations in his original e-mail request of November 5,

---

[118] Our investigation found that prior to June 2008 the only FBI personnel who queried these records in the [redacted] database were the CAU Intelligence Analyst and two FBI employees who were assigned to the FBI OGC's review team that in 2007 was charged, in response to the OIG's first NSL report, with analyzing the FBI's basis for acquiring records through exigent letters and blanket NSLs. As discussed below, the prosecutor, CTD management, and the FBI OGC were not aware that the FBI had acquired reporters' records until the OIG informed the FBI General Counsel in June 2008. The administrator of the [redacted] database also told us that there is no evidence that non-FBI personnel who have access to the [redacted] database queried these records.

[119] "Trace reports" contain the results of CAU Intelligence Analysts' research on telephone data.

[redacted], and three other numbers.[120] The second trace report contained all of the telephone data acquired on the 10 telephone numbers, as well as available information in the [redacted] database related to 11 of the 12 telephone numbers listed in the case agent's November 5, [redacted], e-mail.

We also found that no grand jury subpoena was issued for these reporters' records, either before or after the records were produced. In addition, no Department personnel sought Attorney General approval for subpoenaing these reporters' records, as required by federal regulations and Department policy.

c. AUSA and FBI Field Division Personnel Knowledge that Reporters' Records Were Obtained

When we interviewed the case agent, his squad supervisor, and the [redacted] Field Office Assistant Special Agent in Charge who supervised the squad conducting the leak investigation, they told us that they were unaware that CAU personnel had asked Company A to provide the reporters' and news bureaus' telephone records or that anyone had sent an exigent letter to Company A for these records.

We asked the case agent about the January 5 e-mail from the CAU Intelligence Analyst to him forwarding the toll billing records from Company A and the trace reports on the records. He said that he had not opened the attachments to this e-mail and had not recognized from the e-mail that the attachments might have included toll billing records.[121] He told us that he "did not know exactly what trace reports meant," and that he interpreted another portion of the e-mail as meaning that the analyst had run the numbers against previously established databases.

The case agent also told us that he did not open the attachments, because he "just wanted to make sure that we did not proceed until we had sent the subpoena," adding, "there is no exigency so I was just content to wait and see what my deliberations with [the AUSA] would yield." The agent said that if he had "perceived it at the time as violating DOJ regulations or the law, [he] would have notified appropriate parties."

---

[120] Nine of these 10 numbers also appeared on the December 17, [redacted], exigent letter to Company A.

[121] The Intelligence Analyst said that the only difference between what he sent with his January 5 e-mail and the raw data he received from Company A was the formatting of the data.

The case agent also told us that he never told the CAU SSA or anyone in his management chain that exigent circumstances existed regarding the need to obtain the telephone records listed in his November 5 e-mail. He also said that he had no idea where the CAU SSA obtained the language in the exigent letter stating that requests for subpoenas had already been submitted to the U.S. Attorney's Office. He further stated that the only representations he made to the CAU regarding a subpoena were contained in his e-mails, which stated that a subpoena was contemplated and would be provided in the future.

The AUSA who directed the leak investigation told us that he did not know anything about the FBI having obtained any reporters' records in the investigation until the OIG identified this issue and interviewed him in 2008. The AUSA also said he did not recall if the case agent had ever sent the reporters' telephone numbers to the CAU to determine if their records were available. The AUSA said he did not know that the CAU SSA had sent an exigent letter to Company A seeking the reporters' and news organizations' toll billing records, that Company A had provided responsive records, that a CAU Intelligence Analyst had sent the records and his analysis to the case agent in an e-mail, or that the reporters' records had been uploaded into a [redacted] database.

The final e-mail we found relating to the reporters' telephone records was sent by the case agent to the CAU Intelligence Analyst on March 24, [redacted]. The subject line of the e-mail stated, "Important question." The e-mail referenced the CAU Intelligence Analyst's January 5, [redacted], e-mail and stated:

> I am working closely with the United States Attorney's Office . . . and we are contemplating getting a grand jury subpoena for certain telephone toll records ([redacted] telephone numbers) that will require special approval from the Department of Justice before issuance. Before we undertake getting the approval for the subpoena, **the AUSA wants to know with certainty whether telephone toll records for [redacted] telephone calls can be obtained.** [redacted]
> This is a key question for us going forward. [Emphasis in original.]

The Intelligence Analyst replied by e-mail on the same day, stating, "Back in January I sent you two products which reflected [Company A] toll records on

several of the [redacted] numbers you had targeted, so we can get the data if the calls were carried on [Company A] lines." The e-mail also stated that one of the two reports "was only the [Company A] tolls."[122] The Intelligence Analyst added, "So, basically, you already have the records that we have."

When we asked the case agent about this e-mail, he told us he did not recall what his reaction to the e-mail was at the time. When we asked him at the time of his OIG interview whether, looking at the e-mail, he understood that the e-mail stated that the analyst had previously sent the agent two products that reflected Company A toll records, as distinguished from value-added analysis of existing databases, the agent acknowledged, "that is what this e-mail says, yeah."

d. FBI Conducts [redacted]

In [redacted] after the CAU Intelligence Analyst had provided the reporters' telephone records and accompanying trace reports to the case agent – the FBI sent the case agent [redacted] The FBI squad supervisor who supervised the leak investigation told us that the agents [redacted] – the leak investigation [redacted]

The squad supervisor told us that she instructed the case agent to [redacted] information that would assist

---

[122] The e-mail stated that "one of the reports was only [Company A] tolls, which you could use in court, and the other one was an intelligence product with [sic] encompassed everything in [an [redacted] database].

the FBI in identifying the leaker or leakers and [redacted]

The squad supervisor told us that the plan for conducting [redacted] was discussed with her Division's chain of command and probably with a Unit Chief in the FBI's Counterintelligence Division at FBI Headquarters. An e-mail from the Unit Chief to the case agent and the squad supervisor on [redacted], noted that the [redacted]

We determined that on [redacted] the case agent and [redacted] According to the [redacted] Field Office squad supervisor and documentation of [redacted] article was a classified U.S. government intelligence document [redacted]

On [redacted] the case agent and [redacted]

The case agent's e-mail summarizing "key points" of [redacted] stated that he believed the [redacted] was successful, noting that the [redacted] The e-mail also stated that the [redacted] article was U.S. government classified information.

The squad supervisor told us that even though [redacted] classified U.S. government information.

[redacted], this media leak case was transferred from the original case agent to another FBI Special Agent in the [redacted] Field Office.[123] According to the U.S. Attorney's Office in [redacted], the leak investigation is still open.

3. FBI Notifies the Reporters That Their Records Were Obtained

In April 2008, during our investigation of the use of exigent letters, we discovered the e-mail exchanges described above concerning the reporters' toll billing records. The following month we determined that the FBI had acquired the reporters' and news bureaus' toll billing records without any legal process or Attorney General approval.

In June 2008, the OIG informed the FBI General Counsel and the Acting Assistant Attorney General in charge of the Department's National Security Division (NSD) that we had determined that the FBI had requested and obtained the toll billing records of members of the news media in this leak investigation without legal process or the required Attorney General approval. As discussed above, federal regulations also require that the FBI notify reporters if their toll billing records are subpoenaed without providing required advance notice.[124]

In response to our notifications of these violations, on August 8, 2008, FBI General Counsel Valerie Caproni wrote letters to the editors of the Washington Post and The New York Times, and to the reporters whose records were acquired, stating that the FBI, as part of an authorized FBI investigation, had obtained the telephone records of reporters and of their bureaus in [redacted][125] The letters stated that the OIG had informed the FBI in the course of its investigation that the FBI had acquired the telephone records in response to an exigent letter. Additionally, the letter stated that, based on currently available information, the FBI had made no investigative use of the reporters' telephone records. The letter noted that while the exigent letter stated that

---

[123] The case agent was later assigned to a second leak investigation described below.

[124] See 28 C.F.R. § 50.10(g)(3).

[125] See Valerie Caproni, General Counsel, Federal Bureau of Investigation, letters to [redacted] Leonard Downie, Executive Editor, Washington Post, and [redacted] Bill Keller, Executive Editor, The New York Times, August 8, 2008.

Because our investigation of this issue was on-going, the OIG asked the FBI to briefly defer notification to the reporters and news organizations, from June until August 2008, until all significant OIG interviews related to this matter had been completed.

subpoenas had been requested for the records and would be forthcoming, no subpoena was ever issued for the reporters' telephone toll billing records. The letters also stated (and the FBI confirmed to us) that the FBI has purged these records from FBI databases.[126]

However, the FBI did not disclose to the reporters or their editors that [redacted]

4. OIG Analysis

As discussed above, federal regulation and Department policy requires a balancing of First Amendment interests and the interests of law enforcement before issuance of subpoenas for the production of reporters' telephone toll billing records. The regulation also requires the Department to take reasonable alternative steps to obtain the records, and if those efforts fail, to request Attorney General approval before issuing any such subpoena.[127]

We determined that the FBI did not comply with these legal requirements. As detailed above, without any request from the FBI case agent or anyone in his chain of command and without the knowledge of any prosecutor, a CAU SSA issued an exigent letter to an on-site Company A analyst for the telephone toll billing records of Washington Post and New York Times reporters and their bureaus in [redacted] Company A provided the records to the FBI, and the FBI uploaded the records into a [redacted] database without complying with these requirements. The records remained in that database for over 3 years, unbeknownst to the prosecutor, CTD management, and FBI OGC attorneys, until OIG investigators determined that the records had been acquired and notified the FBI General Counsel. The FBI subsequently purged the records from the [redacted] databases and notified the reporters and their news organizations that their records had been acquired without following required procedures.

We believe that the actions of the FBI personnel involved in this matter were negligent in various respects. Moreover, the manner in which the

---

[126] In addition to the letter, Director Mueller called the editors of the two newspapers to express regret that the FBI agents had not followed proper procedures when they sought the reporters' telephone records. [redacted]

[127] See 28 C.F.R. § 50.10 (2004).

reporters' telephone toll records were acquired by the FBI illustrated the absence of internal controls in the CAU for requesting records from the on-site communications service providers, the lack of training and guidelines at the CAU as to what constituted an emergency request, and the use of exigent letters that contained inaccurate statements.

First, we found that for the purpose of obtaining reporters records, the CAU SSA issued a factually inaccurate exigent letter without the knowledge or approval of the case agent or the AUSA. This was a complete breakdown in the required Department procedures for approving the issuance of grand jury subpoenas for reporters' toll billing records. Apparently on his own initiative, the CAU SSA requested these records even though he was not asked to obtain them – he was only asked to find out if [redacted] calls [redacted] were captured by the on-site communications providers' systems.

Second, we were troubled by the two inaccurate statements in the exigent letter, which stated that there were exigent circumstances and that a request for a grand jury subpoena had been submitted to the U.S. Attorney's Office. Notwithstanding these assertions of fact, the CAU SSA told us he did not recall the case agent making any representations about any exigent circumstances underlying his inquiry about the availability of records, and the case agent said he made no such representations. The CAU SSA speculated that he could imagine circumstances in which the leak of classified information could present exigent circumstances. Such speculation cannot justify requesting telephone records protected by the ECPA without the required Attorney General approval and compliance with federal regulation.

Third, we concluded that the case agent should have exercised greater attention to detail when he received the e-mail from the CAU Intelligence Analyst that included the toll records of the reporters and U.S. media organizations. The January 5, [redacted] e-mail sent by the CAU Intelligence Analyst to the case agent referred to "two trace reports for the calling activities associated with your [redacted] target numbers." These were references to the [redacted] telephone numbers the case agent had inquired about in his November 5, [redacted] e-mail. The attachments to the e-mail contained all of the telephone data acquired by Company A concerning several of the telephone numbers the case agent had identified as belonging to reporters or media organizations in his original e-mail request of November 5, [redacted]

The case agent told us that he did not open the attachments to the January 5 e-mail or realize then that they contained reporters' toll billing records. He also stated that he interpreted the e-mail as meaning that the analyst had run the numbers against pre-existing databases. However, the CAU Intelligence Analyst sent another e-mail to the case agent on March 24, [redacted] stating that the January 5 e-mail contained "two products which reflected [Company A] toll records on several of the [redacted] numbers that

you have targeted." The agent acknowledged to us that this e-mail stated that the analyst had sent him toll records, as opposed to a value-added analysis, but he said he did not realize that at the time. We believe that had the agent exercised more care at the time he received the March 24 e-mail, he would have realized then that the analyst had sent him reporters' toll records without a subpoena and without obtaining the required Attorney General approval.

Fourth, in addition to the individual FBI agents' failings in this case, we believe that this matter demonstrated how the CAU's lax and sloppy practices led to serious abuse of the FBI's authority to obtain information from the on-site communications service providers. For example, the exigent letter issued by the CAU SSA failed to specify any time period for the records requested. As a result, although the case agent had identified a 7-month period as being relevant to the investigation, Company A provided the FBI 22 months of records for a Washington Post reporter, only 38 days of which fell within the 7-month period. Similarly, Company A provided the FBI 22 months of records for the Washington Post's bureau in [redacted], only 20 days of which fell within the 7-month period. For the remaining five telephone numbers, *none* of the records given to the FBI included calls made during the 7-month period. Yet, neither the CAU Intelligence Analyst who received the records from Company A, the case agent who received the records by e-mail, nor anyone else in the FBI recognized that the FBI had acquired and uploaded records far outside the time period considered to be relevant to the investigation.

Furthermore, both the CAU Intelligence Analyst who received the records and the CAU SSA who signed the exigent letter told us they did not know about the federal regulation and special approval requirements for obtaining reporters' toll billing records. This suggests a lack of training and oversight of the operational support personnel responsible for interacting directly with the on-site communications service providers.[128]

C. Second Matter

1. Background

In connection with another media leak investigation a U.S. Attorney's Office issued grand jury subpoenas to one of the on-site providers for telephone

---

[128] We discuss these training and oversight failures further in Chapter Five of this report.

toll billing records. The subpoena listed various target telephone numbers. As we describe below, attachments to the subpoenas contained [redacted] language [redacted] that would have resulted in the production of reporters' toll billing records in violation of federal regulation and Department policy. However, after service of the subpoenas, and before looking at the records, the prosecutors realized the error and impounded the records. Our investigation revealed that reporters' records were not included in the records that were produced in response to the subpoenas.

The following sections describe the circumstances surrounding the request for a [redacted] and the actions taken by the Department after it realized that this request may have resulted in the receipt of telephone records of reporters.

2. The Leak Investigation

Believing that someone may have illegally disclosed information to reporters, the Department opened a media leak investigation into the matter. It assigned two federal prosecutors (who we refer to as Prosecutor 1 and Prosecutor 2) to lead the investigation. These attorneys were assisted by an AUSA (who we refer to as the local AUSA) from the judicial district where a grand jury was convened to pursue the investigation, and FBI agents and Intelligence Analysts.[129]

After the leak investigation was opened, the investigative team sought to obtain records related to various telephone numbers. The FBI case agent assigned to the investigation told us that he spoke with a CAU SSA about the investigative team's interest in obtaining "to-and-from [redacted] calls [redacted]" for particular telephone numbers. The case agent told us that the CAU SSA had advised him to contact the on-site employees of Company A and Company B to obtain the language for the subpoenas necessary to obtain those calls.

The case agent went to the CAU and met one of the on-site Company A analysts. The case agent told us that he explained to the Company A analyst that "we were focused on to-and-from [redacted] calls [redacted] for a single target." The case agent said he believed that they "also

---

[129] Pursuant to Rule 6(e) of the Federal Rules of Criminal Procedure, we have excluded grand jury information, including any identifying details about the leak under investigation, from this summary of the matter.

discussed the fact that there is a media leak case and that . . . we are not getting at reporters' numbers. . . ."

Following the meeting, the case agent sent an e-mail to the Company A analyst seeking "boiler plate" language he could use in forthcoming subpoenas related to the leak investigation. Specifically, the case agent's e-mail asked for "language you like to see in the subpoena to insure that it is as encompassing as possible."

The case agent told us, and e-mail records confirm, that he received suggested text for the subpoenas from an on-site Company A analyst. The suggested text requested, among other things, a [redacted] The case agent told us that he recalled "maybe a quick perusal" of Company A's suggested language, but he said that there was "nothing about the specific language that I would have remembered reading."[130]

The case agent told us that he merely forwarded the suggested text to Prosecutor 1 for his consideration and was not "prescribing that that text be used." However, Prosecutor 1 told us he used that text in typing attachments to subpoenas to Company A seeking the target telephone numbers' records. The facsimile cover sheet the case agent used to transmit the suggested language to Prosecutor 1 stated, "more boiler plate language per discussion Friday."

Our investigation determined that the case agent, his supervisor, and Prosecutor 1 knew at the time the subpoenas were issued that the target numbers had been in telephonic contact during the period specified in the subpoenas with a reporter who had obtained the leaked information.

Moreover, [redacted] the language [redacted] would cover [redacted]

---

[130] The case agent stressed that Prosecutors 1 and 2 made it clear to the investigative team that they were the legal advisors on the investigative team. Therefore, he said, "we never reviewed draft subpoenas" and "we were not asked to review any language for sufficiency or adequacy from a legal or investigative perspective. We were merely advised when the subpoena was ready to be served."

[redacted] the records of reporters who may have contacted the target numbers.[131]

Shortly after receiving the facsimile from the case agent with Company A's suggested language, Prosecutor 1 drafted grand jury subpoena attachments. Each subpoena attachment requested [redacted]

[redacted]

The subpoenas themselves were initialed by the local AUSA.[132] The subpoenas both stated, "please see attachment," and Prosecutor 1 had notified the local AUSA by e-mail that Prosecutor 1 would draft the "riders" and add them after the subpoenas were drafted.[133] The local AUSA stated that these were the first subpoenas he had signed in the investigation. He said at the time, he did "not know anything" about the reasons for the subpoenas. He told us that he did not draft the attachments to the subpoenas and that the attachments were added without his knowledge (after he had initialed the subpoenas). Prosecutor 1, who drafted the attachments, confirmed that he did not think the local AUSA would have seen the attachments.

The case agent served the subpoenas, with the attachments, on the on-site Company A analyst. The case agent told us that he had no discussion with the on-site Company A analyst about the meaning of Company A's suggested language [redacted] before the subpoenas were served.

We received conflicting information about whether the case agent and Prosecutor 1 discussed the meaning of the [redacted]

---

131 [redacted]

132 During this leak investigation, the local AUSA was not involved in the day-to-day work of the investigative team other than being asked to initial grand jury subpoenas.

133 We reviewed two e-mails that the local AUSA received from Prosecutor 1 concerning procedures to be followed for grand jury subpoenas issued by the media leak investigative team. Both e-mails stated that Prosecutor 1 would draft and add "riders" or attachments to the subpoenas after the subpoenas were drafted.

[redacted] language used in the attachment before the subpoenas were issued.

When we first interviewed Prosecutor 1, he told us that his only conversation with the case agent about the language in the subpoena attachment was when he received from the case agent a "muddled" explanation of what the language meant. Prosecutor 1 told us that the case agent's explanation was unclear and that, as a result of this confusing explanation, he only later realized that he did not accurately understand what a [redacted] meant.[134]

In our second interview of Prosecutor 1, he told us that after he had been interviewed by the OIG and reviewed relevant handwritten notes, he recalled more details of his conversation with the case agent, and that this conversation occurred before the subpoenas were issued. He said he recalled the case agent informing him that use of the suggested language would obtain the "incoming and outgoing calls to and from the target number." Prosecutor 1 said he specifically asked the case agent

> whether [Company A's suggested language] would get [redacted] phone records and I recall him specifically assuring me that he had spoken to people about this language [redacted] and that it was the language . . . that was just necessary to get local incoming and outgoing calls between the target number and anyone that they called . . .

During this second interview, Prosecutor 1 also produced an undated document, which Prosecutor 1 said was the subpoena attachment he had typed based on the facsimile he had received from the case agent with the suggested language from the on-site Company A analyst.[135] The document contained handwritten notes of Prosecutor 1 stating, "[Case agent] says – it wouldn't include [redacted] phone record." Prosecutor 1 said he made these notes shortly after a conversation with the case agent before the subpoenas were issued and that these notes refreshed his recollection of the conversation with the case agent.

---

[134] The first interview of Prosecutor 1 was not recorded.

[135] Prosecutor 1 was only told in general terms the nature of the first interview and was not asked to bring relevant documents to the interview. Prosecutor 1 volunteered the document at the second interview, which was recorded.

Prosecutor 1's notes seem to corroborate his assertion that the case agent had told him, erroneously, that the language in the subpoena referring to a [redacted] would not generate [redacted] records, which would have included the records of reporters.

The case agent told us that he did not recall any discussion with Prosecutor 1 or Prosecutor 2 before the subpoenas were issued about the meaning of the text suggested by the on-site analyst. He said that he never told any of the prosecutors assigned to this case that the language in the subpoenas or the attachments would not request telephone records of reporters.[136] The case agent also said he did not recall ever telling the prosecutors that Company A told him it was necessary to add the suggested language to ensure that the FBI obtained the local and long distance calling activity. He stated that he had forwarded the language provided by an on-site Company A analyst to Prosecutor 1 "merely for [the attorneys'] consideration" and was "not prescribing that the text be used."

Prosecutor 1 said that, after the subpoenas had been served on Company A, he had a conversation with an FBI Special Agent assigned to another counterintelligence squad in the division who explained the resources available from the CAU to support the servicing of subpoenas for telephone records. Prosecutor 1 said that it was only during this conversation (not in the earlier conversation with the case agent) that he realized that if Company A produced all records [redacted] as had been requested in the subpoena, Company A could have produced the toll billing records of reporters [redacted] Prosecutor 1 said that the Special Agent told him that by requesting [redacted] Company A could provide the [redacted] Prosecutor 1 said that as a result of this conversation, "I now knew that [the case agent's] explanation [that the subpoena needed to request [redacted] in order to get the [redacted]

---

[136] The case agent told us that he was unaware of any other member of the leak team telling the prosecutors that the language in the subpoenas and accompanying attachments would not request reporters' records. He also said that he thought it was "very unlikely" that such a conversation occurred.

was incorrect."[137] The Special Agent also told us that she recalled describing [redacted] to Prosecutor 1 at about this same time.[138]

Prosecutor 1 told us that subsequent to this conversation with the Special Agent, he met with several DOJ attorneys and supervisors in the Criminal Division to discuss what steps should be taken to address his concern that reporters' records may have been obtained by the subpoenas. Prosecutor 1 said that all participants agreed that any records obtained in response to the grand jury subpoenas should be sealed and that the Criminal Division's Office of Enforcement Operations (OEO) should be consulted on the matter.

Prosecutor 1 and another federal prosecutor spoke to the Criminal Division's OEO Director about the circumstances surrounding issuance of the subpoenas. Prosecutor 1 said that the OEO Director concurred that they should take certain actions (described below) to address the records obtained in response to the subpoenas.

Prosecutor 1 told us that he went to the case agent and directed the agent to copy from his computer the telephone records obtained from the subpoenas and save them to CDs, then delete from his computer's in-box the e-mail from the on-site Company A analyst to which the records were attached. The case agent and Prosecutor 1 told us that the case agent deleted the records from his computer in the presence of Prosecutor 1 and also deleted the items from his "deleted items" folder. Prosecutor 1 placed the CDs in an envelope and sealed it. Prosecutor 1 and the case agent each signed and dated the envelope, and Prosecutor 1 then placed the envelope in a safe at the Criminal Division. The case agent told us that he did not recall reviewing the records before they were deleted from his computer. Prosecutor 1 said that the case agent had assured him that no one had looked at the records.

However, the case agent told us that neither he nor anyone else had asked the Company A analyst who had sent the records to the case agent to delete his "sent" e-mail (attaching the records), and they did not know what CAU personnel had done with the records. They also said they did not inquire whether the responsive records had been uploaded by CAU personnel into any FBI or other databases to which FBI personnel had access, as typically occurs when such records are received by the CAU.

---

[137] After the meeting, the Special Agent sent Prosecutor 1 by facsimile the [redacted] language they had discussed at the meeting.

[138] The Special Agent told us that she had learned about Company A's special resources from an employee of another member of the [redacted]

Based on advice from the OEO Director, the Criminal Division did not notify the reporters about the subpoenas. According to Prosecutor 1, the OEO Director told Prosecutor 1 and other Criminal Division attorneys that the regulation requiring notification to the reporter was not triggered because any possible collection of the reporters' records was inadvertent and the records received from Company A were sealed and not reviewed. The OEO Director also opined that the Attorney General did not have to be notified about the matter since the records had been impounded and would not be used unless Attorney General approval was sought.

Prosecutor 1 briefed members of the investigative team that [redacted] were prohibited from being used in connection with the leak investigation. The Assistant Special Agent in Charge of the Division's counterintelligence squads also sent an e-mail to all FBI personnel assigned to the investigation directing that the language suggested by the on-site Company A analyst referring to [redacted] not be used in the leak investigation because it could capture records of reporters.[139]

3. OIG Investigation

During our investigation of exigent letters, the OIG interviewed Prosecutor 1 about another media leak investigation that we describe in the next section, and we learned about the [redacted] grand subpoenas issued to Company A in this case.

We then informed Criminal Division officials that we believed that it should be determined whether the records Company A had provided to the FBI actually included any reporters' records. However, Criminal Division officials did not believe that any of the responsive records they had sequestered should be unsealed or reviewed.

We therefore suggested that, without examining the electronic or hard copy records that the Criminal Division had sequestered, the OIG and the Criminal Division should jointly determine whether Company A had provided any [redacted] records in response to the subpoenas because if all the [redacted] records were provided, they would contain the records of reporters.

---

[139] Prosecutor 1 told us that he and others also reviewed all grand jury subpoenas issued by the investigative team and determined that they had issued no other subpoenas requesting [redacted]

We then determined that Company A gave CAU personnel responsive records within approximately 1 week of service of the subpoenas and that an on-site Company A analyst e-mailed the records to the case agent. We asked the administrator of the [redacted] database to identify any records uploaded in response to the subpoenas. With the database administrator's assistance, we determined that toll billing records on the target numbers listed in the subpoenas were uploaded into the database. However, we found no evidence that the FBI received or uploaded any [redacted] telephone records [redacted] We also found no evidence that reporters' records were ever provided to the FBI in response to the [redacted] subpoenas.[140]

Because of the [redacted] during the time period specified in the subpoenas and the fact that the Department had issued subpoenas for [redacted] records for this time period that would have included reporters' records, the OIG also raised with the Criminal Division and other Department officials the question whether notification of the reporters was required under 28 C.F.R. § 50.10(g)(3). As described above, that regulation requires that if telephone toll billing records of reporters are subpoenaed without the required advance notice, the affected reporter must be notified "as soon thereafter as it is determined that such notification will no longer pose a . . . substantial threat to the integrity of the investigation" and, in any event, within 45 days of any return in response to the subpoena.[141]

The Criminal Division and the OIG asked the Department's Office of Legal Counsel (OLC) to opine on the question when the notification provision in the regulation would be triggered. OLC concluded in an informal written opinion dated January 15, 2009, that the notification requirement would be triggered if, using an "objective" standard and

> based on the totality of the circumstances, a reasonable Department of Justice official responsible for reviewing and approving such subpoenas would understand the language of the subpoenas to call for the production of the reporters' telephone toll

---

140 [redacted]

141 28 C.F.R. § 50.10(g)(3).

numbers, the subpoenas would be subject to the notification requirement of subsection (g)(3), regardless of the subjective intent of the individuals who prepared them.

The OLC opinion also concluded that the notification requirement would be triggered even if reporters' toll billing records were not in fact collected in response to such a subpoena.

Based on the OLC opinion, the Criminal Division concluded that it was not required to notify the reporters because it believed that neither Prosecutor 1 nor the case agent understood at the time the subpoenas were issued that the subpoenas called for reporters' records.

4. OIG Analysis

If Company A had in fact produced the [redacted] records as requested in the grand jury subpoenas, responsive records would have included reporters' toll billing records. Because Company A did not produce all records requested by the subpoenas, the reporters' records were not provided. However, we believe that the way in which the Department drafted and issued the subpoenas was deficient and troubling for several reasons.

First, the FBI agent provided, and Prosecutor 1 drafted and approved, language in the subpoena attachments that neither the FBI agent nor Prosecutor 1 correctly understood. Prosecutor 1 said he relied on the case agent's explanation of the phrase [redacted] The case agent told us he did not recall having a conversation with any prosecutor about what the language meant, and that he did not tell any of the prosecutors that the language would not request reporters' telephone records. The case agent also said that he expected Prosecutor 1 to perform any legal analysis of the language.

In addition, the local AUSA initialed the grand jury subpoenas without reviewing the attachments, which were prepared by Prosecutor 1 and attached after the local AUSA initialed the subpoenas. We believe the Department should ensure that the reviews by prosecutors who are asked to approve grand jury subpoenas are meaningful and complete. That did not happen with respect to these grand jury subpoenas and their attachments.

Second, our investigation found that but for the conversation about Company A's capabilities between a field division Special Agent assigned to a counterintelligence squad and an [redacted] employee, FBI and Criminal Division attorneys would likely not have learned about the problems with the language in the grand jury subpoenas. Once the Special Agent explained to Prosecutor 1 what [redacted] meant, Prosecutor 1 took several appropriate steps in alerting Criminal Division supervisors to the

potential problem with the subpoenas. We believe that the actions subsequently taken by the Criminal Division in consulting with the OEO Director and sequestering the responsive records were reasonable corrective measures.

However, the Criminal Division did not evaluate what steps should be taken to address the e-mail sent by the on-site Company A analyst to the Intelligence Analyst or others, attaching the records. We believe that in addition to the steps described above, the Criminal Division should have ensured that all copies of the records were permanently deleted from FBI e-mails, share drives, servers, or other electronic records.

Our investigation did not find that FBI personnel or Department attorneys intended to obtain reporters' records. Nonetheless, had Company A's analyst provided all the records requested in the subpoenas, the records would have included reporters' toll billing records since there was telephonic contact between the target telephone numbers and reporters during the period specified in the subpoenas.

Applying the standard articulated by the OLC for when reporters must be notified that their records were subpoenaed, we concluded that the Criminal Division's decision not to notify the reporters was reasonable. Given the technical terms used in the subpoenas, we did not find that a reasonable Department of Justice official would understand the language of the subpoenas to call for the production of reporters' toll billing records. We therefore agree, based on the objective standard articulated by the OLC, that the Department was not required to notify the reporters pursuant to 28 C.F.R. § 50.10(g)(3) that they were not afforded advance notice of the subpoenas. We also note that the Criminal Division informed the Court that had empanelled the grand jury of the subpoenas and the corrective actions it had taken, which we believe was an appropriate step to take.

As discussed further in Chapter Six of this report, we recommend that the FBI provide periodic guidance to FBI personnel on the special regulations and policies governing subpoenas for reporter's toll billing records.

D. Third Matter

1. Background

In an investigation of a third media leak matter, a U.S. Attorney's Office issued a grand jury subpoena to Company A for telephone records. In addition to providing records in response to the subpoena, an on-site Company A analyst, without any request from the FBI (or any legal process), [redacted] for records of telephone calls of a cellular phone used by a reporter, and provided information about his [redacted] of the reporter's records to the FBI in the absence of legal authority to do so. Also, at the request of a CAU supervisor but

without legal process, Company B and Company C employees [redacted] their databases for the telephone records of the reporter's cellular phone calling activity.[142]

2. The Leak Investigation (U)

An FBI Special Agent participated in an interview of a witness relating to the potential leak of information to a reporter. Based on information that was provided by the witness, the Special Agent sought additional information from the on-site analyst from Company A.

a. The Subpoena for [redacted]

The Special Agent served a grand jury subpoena on an on-site Company A analyst for the toll billing records of [redacted] To generate the subpoena, the Special Agent had faxed a subpoena request form to an administrative support employee in a U.S. Attorney's Office who was responsible for preparing subpoenas for a related investigation.[143] The Special Agent's subpoena request stated that a prosecutor assigned to the investigation would draft the attachment to the subpoena. The Special Agent noted on the facsimile cover sheet accompanying the subpoena request form, "We need Company A [redacted]

As a result of the request, the subpoena, on its face, requested [redacted] The subpoena contained no limiting date range.

The Special Agent served the subpoena by facsimile on an on-site Company A analyst. A cover letter addressed to Company A that accompanied the subpoena was signed by a prosecutor in the U.S. Attorney's Office, but the subpoena itself did not bear his signature or initials.

The Special Agent told us that he was "probably directed" to request the subpoena by his supervisor or one of the prosecutors associated with the related investigation. However, the prosecutors and the Special Agent's supervisor told us they did not recall approving the subpoena or discussing it with the Special Agent. The prosecutors said they did not know how the subpoena came to be issued.

---

[142] As with the second matter, pursuant to Rule 6(e) we have excluded grand jury information, including any identifying details about the leak under investigation, from this summary.

[143] The Special Agent who made the subpoena request was not assigned to the related investigation.

The copy of the subpoena and related documents provided to us by Company A contained an attachment requesting, among other information, a [redacted] This request, if filled, would result in the [redacted] and provision to the FBI of the telephone records of [redacted] However, we do not believe the attachment to the subpoena was included in the material faxed to the Company A employee. We noted that the subpoena, the cover letter, and the return of service all included header information listing the date, time, and telephone number from which they were faxed. The attachment did not include any corresponding information indicating that it had been faxed. In addition, the subpoena itself did not indicate it contained an attachment.[144] Further, copies of the subpoena maintained in the files of the prosecutors and the U.S. Attorney's Office did not contain this attachment.

When we showed the prosecutors the attachment that was in the on-site provider's files, they said they did not recall ever seeing this type of attachment in their grand jury investigation or any other investigations. Moreover, the Special Agent told us that he would not have prepared the attachment and that he did not recall previously seeing the attachment. We believe that the Company A employee may have obtained the attachment from CAU personnel or from the CAU share drive. The CAU share drive, which was accessible by all CAU personnel and the on-site providers, included a boilerplate attachment that was nearly identical to the one Company A provided to us with the subpoena. The attachment on the share drive had been approved by the FBI OGC National Security Law Branch and included with numerous NSLs and grand jury subpoenas.

b. Company A [redacted] Cellular Phone Calling Activity

After the subpoena was served, the Special Agent sent an e-mail to the on-site Company A analyst that included the name and cellular phone number of a reporter, facts explaining the relevance of calling activity by the reporter to the investigation, and information indicating that the cellular phone number of the reporter was in contact [redacted] of the subpoena during a particular period.

The Special Agent told us that he provided the cellular phone number of the reporter to the Company A analyst because the analyst "asked for" it and

---

[144] The subpoena did not state "see attachment" and the box on the face of the subpoena for "additional information" was not checked.

"just to make the [redacted] easier [redacted][145] The Special Agent also told us that he believed that because he was "only looking for the [redacted] DOJ approval was not required.[146]

The Company A analyst reviewed the [redacted] records and concluded that they did not include calling activity between the [redacted] and the reporter's cellular phone number. Before informing the Special Agent of that conclusion, the Company A analyst asked the Special Agent to provide the specific date that the Special Agent believed the reporter had called [redacted] The Special Agent responded with a date range.

Then, without any request from the FBI (or any legal process), the Company A analyst [redacted] Company A's database and downloaded records for the reporter's cellular phone number and informed the Special Agent by e-mail that there was no calling activity between the [redacted] telephone numbers during the specified date range. The Company A analyst told us that he did not print out the downloaded records since he did not find the suspected calling activity between the reporter [redacted] We found no evidence that the analyst informed the Special Agent or others in the FBI that he had [redacted] the Company A database for calling activity of the reporter.

The Special Agent told us that he had not asked the Company A analyst to [redacted] records of the reporter's calling activity and was not told of the [redacted] He also said he understood that absent a grand jury subpoena, reporter's telephone records could not be [redacted] and that "we were not asking for [a reporter's] records here." The Special Agent said that if the Company A analyst had found records of calls between the reporter [redacted] he would have told the analyst, "[w]e have got to stop at that. [redacted]

---

145 [redacted]

146 [redacted]

The Company A analyst who [redacted] the [redacted] told us that it was helpful to have the reporter's telephone number prior to [redacted] the records [redacted] listed in the subpoena so that he could "give [the case agent] an answer really quickly as to whether we had the data or not." The analyst also told us that after he [redacted] the [redacted] records and did not discover telephone contact between the [redacted] and the reporter, he was concerned that he had missed the telephone call. He said that he therefore [redacted] the provider's database for calling activity by the reporter to determine whether there was any activity between the reporter [redacted][147] The analyst told us, "The only way to make sure that I did not mess up was to take a look at the records for [the reporter's] number . . . ."

The Company A analyst told us that if the Special Agent had not given him the reporter's telephone number, he would not have [redacted] those records. However, he also said he had no reason to believe that the Special Agent knew he had [redacted] the reporter's telephone number.

The Company A analyst e-mailed a [redacted] chart with the analyst's calling circle [redacted] to the Special Agent. This chart was attached to an e-mail that included multiple e-mails between the Company A analyst and the Special Agent in which the Special Agent had provided facts about suspected contact between the reporter [redacted] the reporter's cellular phone number, the time frame of the suspected contact, and the Company A analyst's notification to the Special Agent that records were not located during the specified period. The CAU Primary Relief Supervisor was copied on this e-mail.

The Special Agent's supervisor said he did not know the Special Agent had provided the reporter's cellular phone number to the Company A analyst. The supervisor also said he did not recall learning from the Special Agent or anyone else that the analyst had [redacted] the records of the reporter's cellular phone number.

The CAU Primary Relief Supervisor said he did not know that the Company A analyst had [redacted] for telephone calls made by the reporter. Yet, the CAU Primary Relief Supervisor had received the e-mail with the [redacted] chart described above that provided all these facts. The CAU Primary Relief

---

[147] The Company A analyst explained why reviewing [redacted] calling activity records using the [redacted] might not disclose calling activity between the reporter [redacted] However, by reviewing calling activity records of the reporter's telephone number, the Company A analyst said, he could be certain to capture telephonic contact between the [redacted] numbers.

Supervisor also said he was not sure if a grand jury subpoena could be used for such records and did not know what the process was to get a grand jury subpoena for such records in conjunction with the U.S. Attorney's Office.

c. Company B and Company C Also [redacted] the Reporter's Cellular Phone Calling Activity

We determined that the Company A analyst who had [redacted] for telephone calls made by a reporter sent an e-mail to the CAU Primary Relief Supervisor with the subject line, "Requested Information." The e-mail listed [redacted] the reporter's cellular phone number, and a 3-day date range.

Company B records show that 2 minutes after this e-mail was sent, the on-site Company B employee [redacted] Company B's records for calling activity by the reporter's cellular phone number for a date range 1 day before and 1 day after the 3-day period identified in the Company A analyst's e-mail. Two minutes after that [redacted] the Company B employee [redacted] Company B's records for calling activity by [redacted] for the same period. Based on these e-mail records and other documents we reviewed, we believe that the Primary Relief Supervisor asked Company B to [redacted] its records for this purpose.

A Company B attorney told us that the Company B [redacted] of the reporter's calling activity found responsive records although the on-site Company B employee did not recall whether he provided any information about the records to the FBI. However, in response to our request to determine whether records from Company B responsive to this [redacted] were uploaded into FBI databases, the FBI database administrator told us that he did not find any evidence of such records.

According to an entry in the Company C employee's log, 2 days later the CAU Primary Relief Supervisor asked the on-site Company C employee to [redacted] for records of calls by both the reporter's cellular phone number [redacted] for the same 3-day period previously identified to the on-site Company A analyst. The Company C employee's log indicates that the CAU Primary Relief Supervisor told him the telephone numbers pertained to a leak case. The Company C employee [redacted] Company C's database for calling activity [redacted] and the reporter's cellular phone number, but did not identify any responsive records.

The CAU Primary Relief Supervisor told us he did not recall interacting with the Company C employee on this investigation, but that it was "possible" he conveyed a request to the Company C employee to [redacted] the records shown in the log. He added that he could not recall "when or why" he would have

made the request but he did not think the Company C employee would write his name in the Company C log "without having some justification."

The Special Agent told us that he did not ask the CAU Primary Relief Supervisor or the on-site Company B or Company C employees to [redacted] for the reporter's calling activity in their databases, and we found no evidence that employees of Company B or Company C, or anyone in the CAU, informed the Special Agent that they had done so.

3. OIG Analysis

We determined that the Department issued a grand jury subpoena to Company A seeking [redacted] that a reporter was believed to have called. The subpoena in Company A's file had an attachment that requested a [redacted] If Company A had had records of calls [redacted] Company A would likely have produced calling activity information of the reporter in response to the subpoena. This subpoena was issued without the required Attorney General approval or compliance with Department regulations governing the acquisition of reporters' toll billing records.

We also determined that the grand jury subpoena to Company A was issued without substantive review by a prosecutor. The subpoena cover letter was signed by an Assistant United States Attorney (AUSA), but the subpoena itself was not initialed by that AUSA (or any prosecutor), and the AUSA said he did not recall focusing on [redacted] Further, although the subpoena request form that the Special Agent faxed to the U.S. Attorney's Office stated that a prosecutor assigned to the investigation would draft the attachment, we do not believe any of the prosecutors drafted, reviewed, or approved the attachment.[148]

In addition, we found that the on-site employee of Company A [redacted] Company A's database for records of cellular phone calling activity by the

---

[148] As noted above, while the copy of the subpoena maintained in the prosecutors' files had no attachment, the subpoena that was found in Company A's files had an attachment that requested a [redacted] However, the attachment in Company A's files did not bear a facsimile header indicating that it was faxed to the provider along with the subpoena. Further, the subpoena itself did not include the words "see attachment," or otherwise indicate that there was an attachment. No one from the FBI or the Department could explain to us when or how the attachment was appended to the subpoena.

reporter. The evidence indicates that the Company A analyst [redacted] the database on his own initiative after the FBI Special Agent provided detailed information to him about the investigation and the dates of possible contacts between the reporter [redacted] listed in the grand jury subpoena. The Company A analyst then provided information about the [redacted] to the FBI in the absence of legal authority to do so.

We determined that Company B and Company C also [redacted] their respective databases for records of cellular phone calling activity by the reporter's cellular phone number. They did so after the Company A analyst gave the CAU Primary Relief Supervisor the reporter's cellular phone number, [redacted] and dates of suspected calling activity between the [redacted] numbers. However, we did not find evidence to conclude that the Special Agent or any of the prosecutors assigned to the related investigation asked the on-site communications services providers to do [redacted] or that they knew that any of the providers' employees had done so. Rather, according to the Company C employee's log, he [redacted] the Company C databases for records related to the reporter's cellular phone number at the direction of the CAU Primary Relief Supervisor.

We concluded that the CAU Primary Relief Supervisor either directly asked or prompted the on-site employees of both Company B and Company C to [redacted] the calling activity of the reporter without legal process. The CAU Primary Relief Supervisor told us he was not sure if a grand jury subpoena could be used to obtain such records and did not know what the process was for getting such a grand jury subpoena. As noted above in our analysis of the first leak investigation, we found that the FBI failed to properly train and provide guidance to CAU personnel about the lawful means to acquire toll billing records, reporters' toll billing records, and other information from the on-site employees of Company A, Company B, and Company C.

In sum, we believe that the [redacted] of the reporter's cellular phone calling activity at the prompting or direction of a CAU Supervisor in this case were a clear abuse of authority, in violation of the ECPA, federal regulation, and Department policy. We believe the FBI's actions demonstrated inadequate training for CAU employees, inadequate controls over the issuance of subpoenas, and inadequate supervision of CAU personnel by the CAU and CTD management. As discussed further in Chapter Six of this report, we recommend that the FBI periodically train FBI personnel and issue periodic guidance on the special approval requirements for subpoenaing the telephone toll billing records of news reporters.

We also recommend that the Department determine if, in addition to the grand jury subpoenas identified in this review, the Department has issued other grand jury subpoenas in media leak investigations that included a request for [redacted] community of interest or calling circle [redacted].

If so, the Department should determine whether at the time the subpoenas were issued responsible Department personnel were aware of or suspected contacts between the target numbers in the subpoenas and reporters and whether the Department obtained the toll billing records of reporters in compliance with Departmental regulations, including the notification requirements.

III. Inaccurate Statements to the Foreign Intelligence Surveillance Court

As noted in our first NSL report, one of the uses of NSLs is to obtain evidence to support DOJ applications to the Foreign Intelligence Surveillance Court (FISA Court) for electronic surveillance, physical searches, or pen register/trap and trace orders.[149] For example, information obtained in response to NSLs seeking subscriber information under the ECPA is routinely used to help establish the required elements for Foreign Intelligence Surveillance Act (FISA) applications seeking electronic surveillance or pen register/trap and trace orders on a telephone number.

Based on our concern that the FBI may have used records obtained from exigent letters and other informal requests to seek such FISA Court orders, we asked the Department's National Security Division (NSD) to help us determine whether the Department had sought orders from the FISA Court based on any information obtained in response to exigent letters or other requests as described in Chapter Two of this report.

The NSD and the OIG determined that four FISA applications contained a total of five inaccurate statements. As discussed below, in the small sample of FISA applications that we reviewed, we found that FBI personnel filed inaccurate sworn declarations with the FISA Court to the effect that subscriber or calling activity information was obtained in response to NSLs or a grand jury subpoena, when in fact the information was obtained by other means, such as exigent letters.

In our review, we identified a sample of 37 applications to the FISA Court, which sought FISA electronic surveillance or pen register/trap and trace orders for 35 unique telephone numbers which were examined by the NSD and the FBI.[150] Our review attempted to determine on what basis the FBI had

---

[149] See OIG, NSL I, 48.

[150] These 37 applications were selected for review because they referred to telephone numbers that either were listed in the 11 blanket NSLs that are described in Chapter Four or were referred to in CAU e-mails as record requests associated with FISA applications.

stated it had acquired information pertaining to the subscribers or other calling activity information for these telephone numbers.

Specifically, the NSD and the OIG examined the sample of applications to determine whether they inaccurately stated that NSLs were the source of the subscriber or calling activity information presented to the FISA Court.[151] In these 37 applications, the NSD and the OIG identified 4 FBI declarations that together contained 5 inaccurate statements as to the source of the subscriber or calling activity information relied upon to support the declarations. The four declarations containing these inaccurate statements were signed by four different FBI SSAs.[152]

These four declarations stated that NSLs were the source of the subscriber or calling activity information, when, in fact, NSLs were not the source for the information contained in the FISA application. Rather, for two of these inaccurate statements, exigent letters not NSLs were used to obtain records that were the sources of the information in the FISA applications. In another inaccurate statement, the records cited in an application to the FISA Court were obtained in response to a letter referring to the FBI's emergency voluntary disclosure authority, not in response to an NSL as the application stated. In another inaccurate statement, the FBI obtained the information informally by a verbal request, not in response to an NSL as the application stated. In another application, the NSD determined that a "trash cover" was the source of the FBI's information about the subscriber information, not an NSL as the application stated.[153]

We discuss these four declarations below, describing in more detail the five inaccurate statements we identified.

---

[151] Applications to the FISA Court for pen register/trap and trace or electronic surveillance orders typically include declarations signed by FBI personnel stating the basis for asserting that the telephone number referenced in the application belongs to a particular subscriber. These declarations are signed under oath.

[152] The NSD identified 4 other misstatements in the previously mentioned 37 FISA declarations. These declarations all misstated either the dates of the NSLs seeking subscriber information or the dates when the FBI obtained responsive records from the providers. However, in contrast to the five misstatements described in this section, in these four other instances the statements that the subscriber information had been obtained through NSLs were accurate. The NSD notified the FISA Court of these inaccuracies in August 2008, calling the inaccurate dates "non-material" under Rule 10(b) of the FISA Court's Rules of Procedure.

[153] A trash cover is the search by law enforcement personnel of trash outside the land or yard adjoining a house left to be picked up by garbage collectors.

A. FISA Case No. 1

In this case, the Department applied to the FISA Court for a pen register/trap and trace order in connection with an FBI counterterrorism investigation. The declaration, signed by an Acting FBI SSA, stated that the FBI had obtained the subscriber information contained in the application in response to an NSL served on the carrier. On [redacted] the FISA Court approved the application and issued the order for a pen register/trap and trace device on the subscriber's telephone number.

However, working with the NSD and the FBI, we determined that the only NSL served on the carrier seeking subscriber information for this telephone number was dated [redacted] – 6 weeks after the FISA Court order was issued. Rather, we determined that the subscriber information on which the Department's FISA request relied was obtained in response to an exigent letter dated [redacted]

In August 2008, as a result of our review, the NSD notified the FISA Court of the inaccurate statement in the declaration, stating that the NSD considered the statement to be "non-material" for purposes of Rule 10(b) of the FISA Court Rules of Procedure.[154]

B. FISA Case No. 2

In this case, the Department filed with the FISA Court an emergency application for an electronic surveillance order on [redacted] in connection with a national security investigation.

The supporting declaration by an FBI SSA stated that the FBI had verified the subscriber information through information obtained on [redacted] in response to an NSL served that day on a carrier. The FISA Court's order was entered on [redacted].[155]

However, working with the NSD and the FBI, we determined that the only NSL to the carrier seeking records for this telephone number was dated [redacted] – 2 months after the FISA Court order was issued. We found

---

[154] Rule 10(b) of the FISA Court requires the government to report misstatements or omissions of "material" facts. Neither the FISA Court rules nor the FISA defines what constitutes a "material" fact.

[155] On [redacted] a CAU SSA sent to all three on-site providers an e-mail with this telephone number and asked them to [redacted] for records. The telephone number was subsequently included in the Operation Y blanket NSLs, which we describe in Chapter Four of this report.

that the only documentation of a request for these records sent to the carrier prior to the date of the application was an "exigent situation" letter dated [redacted] that was signed by a Special Agent assigned to the FBI office in [redacted] The letter stated that the request was made pursuant to an emergency situation and that the FBI would provide "required legal process by the end of the next business day."[156] However, the subsequent NSL was dated [redacted] over 2 months after the FISA order had been issued.

In August 2008, as a result of this review, the NSD notified the FISA Court of the inaccurate statement in the declaration, stating that the NSD and the FBI considered the inaccurate statement to be "non-material" for purposes of Rule 10(b) of the FISA Court Rules of Procedure."

C. FISA Case No. 3

In this case, the Department filed an emergency application with the FISA Court on [redacted] for electronic surveillance in connection with a counterterrorism investigation. The supporting declaration by an FBI SSA stated that the FBI had verified the subscriber information through information obtained in response to an NSL served on a carrier. The FISA Court's order was issued on [redacted]

However, working with the NSD and the FBI, we determined that the FBI had obtained the subscriber information from the carrier, prior to the filing of the FISA application for electronic surveillance, in response to an FBI field agent's oral request for telephone records, not in response to an NSL as was asserted in the application to the FISA Court. FBI records showed that the NSL seeking subscriber information for the telephone number was not drafted until [redacted] and was served on the carrier on [redacted] – 2 weeks after the inaccurate FISA application was filed. On [redacted] in response to this NSL, the carrier gave the FBI the identical information that had been described in the declaration supporting the application.

In August 2008, as a result of this review, the NSD notified the FISA Court of the inaccurate statement in the declaration, stating that the NSD and the FBI considered the statement to be "non-material" for purposes of Rule 10(b) of the FISA Court Rules of Procedure."

---

[156] The letter was a form from the carrier that contained a recital tracking the standard for emergency voluntary disclosure of non-content telephone records in 18 U.S.C. § 2702(c)(4). We were unable to determine the identity of the employee who signed the letter.

D. FISA Case No. 4

In this case, the Department filed an emergency application with the FISA Court for electronic surveillance on four telephone numbers in connection with a counterterrorism investigation.

First Inaccurate Statement: The supporting declaration by an FBI SSA stated that the FBI had obtained telephone calling activity information from records obtained in response to NSLs served on a carrier. The FISA Court's order was issued on [redacted]

However, working with the NSD and the FBI, we determined that the only NSL served on the carrier seeking records on three telephone numbers connected to a target of the investigation referenced in the application was dated [redacted] the day after the FISA Court had issued its order, and the only NSL served on the carrier for a fourth telephone number also connected to the target was dated [redacted] 2 months after the FISA Court issued its order. We determined that the calling activity information on which the Department relied in its FISA Court application was obtained in response to an exigent letter to the carrier dated [redacted]

In November 2008, as a result of this review, the NSD notified the FISA Court of the inaccurate statement in the declaration, noting that the NSD and the FBI considered the statement to be "non-material for purposes of Rule 10(b) of the FISA Court Rules of Procedure."

Second Inaccurate statement: The declaration in this application inaccurately stated that pursuant to a grand jury subpoena the FBI had received records from a communications carrier on an unspecified date confirming subscriber information for two telephone numbers. In response to our inquiry, the FBI located a grand jury subpoena to the carrier dated [redacted] for one of the telephone numbers, but said that neither the FBI nor the pertinent U.S. Attorney's Office could locate any grand jury subpoena for the second telephone number.[157] However, the declaration also stated that the

---

[157] The declaration also stated that the FBI had received subscriber information on an unspecified date for two of the four telephone numbers discussed in Case No. 4 above from a carrier, but did not specify the legal process or other basis for this assertion. We found that the FBI served an exigent letter on the carrier dated [redacted] seeking records for the four telephone numbers discussed above in Case No. 4, including a request for a [redacted] community of interest [redacted] for a 24-month period. The only NSL or other legal process we identified that was served on the carrier for this information was an NSL dated [redacted] seeking toll billing records and subscriber information, and included a request for a [redacted] community of interest [redacted] for two of the four telephone (Cont'd.)

FBI had obtained subscriber information for the second telephone number (the one for which a grand jury subpoena could not be located) from a trash cover.

In November 2008, as a result of this review, the NSD notified the FISA Court of the inaccurate statement in the declaration regarding the second telephone number, stating that the NSD and the FBI considered the statement to be "non-material" for purposes of Rule 10(b) of the FISA Court Rules of Procedure."

E. OIG Analysis

Based on our concern that the FBI may have used records obtained from exigent letters and other informal methods to seek FISA Court orders, we examined a small sample of the FISA Court applications that referred to telephone numbers for which records had been requested from the on-site communications service providers. Our investigation showed that FBI personnel had filed inaccurate sworn declarations with the FISA Court about the source of subscriber or calling activity information referenced in applications seeking electronic surveillance or pen register/trap and trace orders. While the declarations signed by 4 FBI SSAs in the 37 applications the NSD and the FBI reviewed stated that the information relied upon in seeking Court orders had been obtained in response to NSLs or a grand jury subpoena, in fact the information was obtained in response to exigent letters, an emergency disclosure letter, and a verbal request to the communications service providers.[158] Moreover, as detailed above, several of the NSLs referred to in the four applications were served at least 2 months after the FISA Court issued the requested orders. (U)

The NSD asserted that the inaccurate statements made in these FBI declarations were non-material because there is no exclusionary rule for statutory violations of the ECPA.[159]

---

numbers listed in the [redacted] exigent letter. We were not able to determine how many days or weeks after the date of the NSL that the NSL was served on the carrier.

[158] According to the NSD's letter to the FISA Court, the FBI obtained the subscriber information underlying the fifth misstatement through a trash cover.

[159] See 18 U.S.C. § 2708 ("the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter"); see also *United States* v. *Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *United States* v. *Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003).

After reviewing a draft of this report, NSD officials stated that in addition to concluding that the ECPA did not provide for exclusion of evidence for violations of the statute, the NSD also examined each of the applications addressed in FISA Cases 1, 2, 3, and 4 and determined that the inaccurate information was not substantive in nature but rather concerned only the manner in which information was obtained. The NSD officials stated that they concluded that the misstatements were non-material because the underlying substantive information provided in the misstatements was correct and that only the procedural manner in which it was obtained was misstated (e.g., in FISA Case 1 the declaration stated that subscriber information was obtained from an NSL rather than from an exigent letter). We agree with the NSD that the inaccurate statements were non-material for purposes of Rule 10(b) of the FISA Court Rules of Procedure.

However, while the NSD deemed these statements "non-material" for purposes of the FISA Court Rules of Procedure, we believe that inaccurate statements to the FISA Court are serious matters. They also affect the credibility of representations made by the government.

It is also important to note that we reviewed only a small percentage of the FISA Court applications that may have relied upon information derived from exigent letters or other informal means. Based on our results in these cases we believe there are likely to be other similar inaccurate statements in other applications. Moreover, no one in the FBI and the NSD who reviewed these applications prior to their submission to the Court had identified the inaccurate statements. Thus, our review also concluded that the FBI and the NSD failed to provide adequate supervision and oversight to ensure the accuracy of the FBI's declarations filed in support of applications seeking FISA Court orders.

After reviewing a draft of this report, NSD officials told us that they believe that even non-material representations to the Court are very serious matters. They also said that, to address these types of issues, the FBI instituted procedures in February 2006 to verify the factual accuracy of information contained in FISA applications. To ensure that these procedures are being followed, the NSD conducts on-site reviews of FBI field offices.

In Chapter Six of this report we provide recommendations to address the issues identified in this portion of our review.

We recommend that the FBI, in conjunction with the NSD, should determine whether any FISA Court orders for electronic surveillance or pen register/trap and trace devices currently in place relied upon declarations containing FBI statements as to the source of subscriber information for telephone numbers listed in exigent letters or the 11 blanket NSLs. If the FBI and the NSD identify any such pending orders, we recommend that the FBI

and the NSD determine if any of the statements characterizing the source of subscriber information are inaccurate or incomplete. If any declarations are identified as containing inaccurate or incomplete statements, we recommend that the FBI and the NSD determine whether any of these matters should be referred to the FBI Inspection Division or the Department's Office of Professional Responsibility for further review.

IV. Improper Administrative Subpoenas Issued to the On-site Providers

Our investigation also uncovered abuses in the FBI's use of administrative subpoenas.[160] In some instances, the FBI received records in response to exigent letters or other informal requests prior to service of administrative subpoenas. In addition, we determined that some administrative subpoenas served on the on-site communications service providers were preceded by "sneak peek" requests through which the on-site providers' employees would first check their databases to determine if records of interest were contained in the databases, and in some cases provided information prior to the service of administrative subpoenas.

We also found that in 2005 an FBI SSA in the CAU signed seven administrative subpoenas pursuant to 21 U.S.C. § 876 for toll billing records as part of the fugitive investigation conducted by the FBI's [redacted] Field Division regarding [redacted] This statute authorizes the use of administrative subpoenas in connection with an active narcotics investigation to which the records sought are relevant. However, some subpoenas were issued when the FBI's [redacted] Field Division had no active narcotics investigation to which the requested records were relevant. Rather, the [redacted] Field Division wanted these records because they were relevant to locating [redacted]

Additionally, we determined that all seven of these administrative subpoenas were signed by a CAU SSA who was not authorized to sign these administrative subpoenas. Moreover, three of the seven subpoenas were issued after the FBI already had obtained the records through exigent letters.

We also found that two additional administrative subpoenas related to a separate case were issued by the FBI's [redacted] Field Division after the FBI had

---

[160] An administrative subpoena is a judicially enforceable demand for records issued by a government authority.

obtained the records. The FBI received the records prior to issuing the subpoenas, which violated the ECPA.

In the sections that follow, we describe these improper uses of the FBI's administrative subpoena authority.

A. The FBI's Administrative Subpoena Authority

The Attorney General is authorized to issue administrative subpoenas in connection with the investigation of certain controlled substances (narcotics) offenses and offenses involving sexual abuse or exploitation of children and health care fraud.[161] Title 21, Section 876(a), of the U.S.C. provides that "in any investigation relating to his functions under this chapter with respect to controlled substances . . . the Attorney General may . . . require the production of any records . . . which the Attorney General finds relevant or material to the investigation."[162]

The Attorney General has delegated authority to issue Title 21 administrative subpoenas to the FBI Director, who in turn has delegated the authority to FBI Special Agents in Charge, Assistant Special Agents in Charge, Senior Supervisory Resident Agents, and "those FBI Special Agent Squad Supervisors who have management responsibilities over Organized Crime/Drug Program investigations."[163] This authority may not ordinarily be re-delegated.[164]

Finally, the ECPA recognizes an exception to the prohibition against divulging "a record or other information pertaining to a subscriber to or customer of such service . . . when the governmental entity uses an administrative subpoena authorized by a Federal or State statute . . . ."[165]

---

[161] See 21 U.S.C. § 876 (narcotics) and 18 U.S.C. § 3486 (sexual abuse or exploitation of children and health care).

[162] 21 U.S.C. § 876(a). The FBI's Manual of Investigative Operations and Guidelines (MIOG) has a corresponding provision stating that any Title 21 subpoena for the production of records must be relevant to a controlled substances investigation. MIOG, Pt. I § 281-7.1

[163] See 28 C.F.R. § 0.85; see also Criminal Investigative Division, electronic communication to all field divisions, Procedure and Operational Issuances, Criminal Investigative Division; Administrative Subpoenas; Proposed Change in the Manual of Investigative Operations and Guidelines, May 1, 2007.

[164] Id.

[165] 18 U.S.C. § 2703(c)(2).

B. Administrative Subpoenas Served on the On-Site Providers

We found that the FBI served over 200 administrative subpoenas for telephone records on the on-site communications service providers from 2003 to 2006. Most of these subpoenas were signed by FBI field division personnel, but some were signed by a CAU SSA. As was the case with NSLs issued after records were provided to the FBI (as described in Chapter Four), a CAU SSA told us that in some instances the communications service providers' employees gave records to the FBI in response to exigent letters prior to service of administrative subpoenas.

Documentation we reviewed from the FBI and the on-site providers showed that some of the administrative subpoenas served on the on-site providers relating to the [redacted] investigation were preceded by "sneak peek" requests through which the on-site providers' employees would first check their databases to determine if records of interest were contained in the databases. In response to sneak peeks, the on-site providers in most instances informed CAU personnel that records existed on the telephone numbers of interest, and the FBI sometimes issued administrative subpoenas for any records the FBI wanted. However, in some instances the on-site providers gave the CAU specific information about calling activity, such as the date of the last call, how many calls were found, and the date range of calls identified, before any legal process was issued.[166]

C. Improper Administrative Subpoenas Issued in Two FBI Investigations

In two FBI criminal investigations, we found that SSAs signed administrative subpoenas that were issued to the on-site providers in circumstances that violated 21 U.S.C. § 876 and the FBI regulation governing the delegation of signature authority for Title 21 administrative subpoenas. In these instances the ECPA prohibition against divulging "a record or other information pertaining to a subscriber to or customer of such service" was also violated.

1. Issuing FBI Administrative Subpoenas in the Absence of an Active Narcotics Investigation

From December 2003 to September 2006, the FBI served at least 54 administrative subpoenas related to the [redacted] Field Division's fugitive

---

[166] We describe our finding that sneak peeks violated the ECPA in Chapter Two of this report.

investigation of [redacted] on the on-site communications service providers located in the CAU. Of that total a CAU SSA signed seven FBI administrative subpoenas for telephone toll billing records between January 2005 and June 2005. At the time, this SSA served as the manager of the CAU's operational support to the FBI's [redacted] investigation.

The CAU SSA told us that no one on the [redacted] task force told him that any of the telephone numbers listed in the seven administrative subpoenas was relevant to any drug investigation. Rather, he said he understood from the [redacted] task force case agent and a task force Intelligence Analyst that the records were relevant to the FBI's attempts to locate [redacted] The SSA also said that he knew that the [redacted] investigation was classified by the FBI as a "drug case" and told us "that is what [redacted] is wanted for."

In August 2008, the OIG asked FBI OGC attorneys responsible for guidance on administrative subpoenas to describe if they believed it was appropriate to issue Title 21 FBI administrative subpoenas in a fugitive investigation where the underlying racketeering acts in the indictment included narcotics offenses. Elaine N. Lammert, FBI Deputy General Counsel for the Investigative Law Branch and Chief of Staff for the FBI OGC, told us that in order to use Title 21 administrative subpoena authority, FBI agents must have an active narcotics investigation at the time the subpoenas are issued and believe in good faith that the records requested are relevant to that investigation.

FBI OGC attorneys asked the [redacted] Field Division to provide information indicating that it had an active narcotics investigation to which telephone numbers listed in administrative subpoenas issued in the [redacted] investigation were relevant. On March 4, 2009, following review of information provided by the [redacted] Field Division, the FBI OGC notified the OIG that "while appropriate in certain aspects of the case at certain times, widespread use of administrative subpoenas in this investigation without a clear nexus to an active investigation of violations of the Controlled Substances Act could not be supported."

2. Administrative Subpoenas were Signed by Unauthorized Personnel

In addition, we determined that the CAU SSA who signed the seven administrative subpoenas in the [redacted] case was not among the FBI officials to whom the Attorney General delegated authority to sign Title 21 administrative subpoenas. The SSA told us he believed he was authorized to sign the subpoenas because CAU Unit Chief Glenn Rogers had designated him to be the CAU program manager assigned to support the [redacted] Field Division's [redacted] investigation. The SSA said he would not have signed the administrative subpoenas unless he believed he was authorized. He also said that he recalled

that the [redacted] task force members agreed that he could sign them. However, he said he did not recall any specific conversations with CAU Unit Chiefs Rogers or Youssef, or any FBI attorneys in which he was told he was authorized to sign the subpoenas.

The CAU SSA told us that he was [redacted] by an on-site Company A analyst when there was calling activity from [redacted] telephone numbers associated with [redacted] family, friends, or attorneys. The CAU SSA told us that he used Company A's hot number [redacted] capability in the [redacted] investigation. Once the CAU SSA was [redacted] to calling activity by those telephone numbers, Company A typically performed a sneak peek [redacted] to determine if the telephone number calling or receiving a call from the "hot number" was a real telephone number [redacted] If it was a relevant telephone number, the Company A analyst notified the CAU SSA, who then signed either an exigent letter or issued an administrative subpoena addressed to Company A seeking records for those telephone numbers. The SSA subsequently issued Title 21 administrative subpoenas to cover some of the records obtained through exigent letters.

FBI records show that the data provided by Company A in response to the exigent letters were uploaded into an [redacted] database before the date of the administrative subpoenas issued by the SSA to cover the records.

3. Two Additional After-the-Fact Administrative Subpoenas

We identified two additional after-the-fact administrative subpoenas in a different investigation in which the subpoenas were provided from 1 to 6 weeks after the records had already been obtained by the FBI through exigent letter or an informal request.

In an organized crime/narcotics investigation conducted by the FBI's [redacted] Field Division, another CAU SSA signed 2 exigent letters addressed to Company A dated August 9, 2004, seeking toll billing records for a total of 24 telephone numbers. Responsive records were uploaded in an [redacted] database on August 10, 2004. A [redacted] SSA issued an administrative subpoena to Company A, dated August 17, 2004, to cover these records.[167]

---

[167] As an SSA assigned to the FBI's Criminal Enterprise Program, this SSA was authorized to sign Title 21 administrative subpoenas.

In connection with the same investigation, on August 11, 2004, the CAU SSA asked the on-site Company C employee whether Company C had telephone records on the 24 telephone numbers listed on the 2 August 9, 2004, exigent letters to Company A (and 46 additional numbers). In response to this verbal request, the Company C employee delivered a CD with responsive records to the FBI on August 17, 2004. The field-based SSA who had signed the August 17, 2004, administrative subpoenas to Company A also signed an administrative subpoena to Company C dated September 30, 2004, to cover records for 4 of the 70 telephone numbers for which Company C had already provided records in response to the informal request.[168]

4. Knowledge of the Use of The Title 21 Administrative Subpoenas

We determined that the FBI OGC and CAU management were unaware of these inappropriate uses of administrative subpoenas to cover records obtained through exigent letters and other informal requests. FBI General Counsel Caproni told us that she did not know that the FBI had issued administrative subpoenas to cover records obtained in response to exigent letters. NSLB Deputy General Counsel Julie Thomas also said she did not recall being informed about administrative subpoenas in these cases. CAU Unit Chief Bassem Youssef told us that he never discussed with the CAU SSA who signed the seven administrative subpoenas, Assistant Section Chief Glenn Rogers, or NSLB attorneys the SSA's authority to sign administrative subpoenas to cover records acquired from exigent letters. Moreover, he said he did not know that administrative subpoenas were used to cover records acquired through exigent letters.

D. OIG Analysis

After the OIG raised questions about the FBI's use of administrative subpoenas in the [redacted] Field Division's [redacted] investigation, the FBI OGC responded that, in its view, in the absence of an active narcotics investigation to which the telephone numbers in the administrative subpoenas were relevant the FBI is not authorized to issue Title 21 administrative subpoenas. Further, when the FBI OGC reviewed the [redacted] Field Division's basis for issuing Title 21 administrative subpoenas in the [redacted] case, the FBI OGC concluded that the [redacted] Field Division did not demonstrate that it had an active narcotics investigation to which the records sought in all of the administrative subpoenas were relevant. Accordingly, the FBI concluded that the [redacted] Field

---

[168] We did not locate administrative subpoenas for the remaining telephone numbers referenced in the informal request.

Division had at times improperly issued administrative subpoenas in that investigation. Following the FBI OGC's review, in March 2009, the FBI General Counsel ordered the [redacted] Field Division to

> immediately conduct a comprehensive review of the use of each administrative subpoena issued in this case to determine whether it was authorized pursuant to the above discussion, and if not, to purge these records from FBI systems and the case file.

We agree with the FBI OGC's analysis and conclusion regarding the issuance of administrative subpoenas in the [redacted] investigation.

During this investigation we also found that the FBI did not establish sufficient internal controls of the use of administrative subpoenas in the CAU. A CAU SSA who was not authorized to issue Title 21 administrative subpoenas signed seven such subpoenas, and no one in the CAU or the [redacted] Field Division recognized the improper use of this authority. Moreover, the FBI OGC and CAU management were unaware that the CAU was using administrative subpoenas to cover records acquired from exigent letters.

We found that the ECPA was violated when the FBI obtained ECPA-protected telephone records in these matters without first issuing appropriate legal process. The ECPA requires communications service providers to disclose local and long distance non-content telephone records "when [the FBI] uses an administrative subpoena authorized by a Federal . . . statute . . . ." 18 U.S.C. § 2703(c)(2). However, the ECPA does not authorize the FBI to obtain ECPA-protected records and then serve an administrative subpoena. Accordingly, we believe that the FBI's receipt of records obtained prior to issuance of administrative subpoenas violated the ECPA[169].

In Chapter Six of this report we provide recommendations designed to ensure that all FBI personnel receive training and periodic guidance on the FBI's administrative subpoena authorities and the relationship between those authorities and other federal statutes, including the ECPA, that govern the FBI's authority to seek telephone records.

---

[169] The FBI has not asserted, and we found no evidence to support, that these were emergency voluntary disclosures pursuant to 18 U.S.C. § 2702(c)(4).

[PAGE LEFT INTENTIONALLY BLANK]

CHAPTER FOUR
THE FBI'S ATTEMPTS AT CORRECTIVE ACTIONS REGARDING EXIGENT LETTERS

In this chapter we describe the FBI's efforts at corrective action to address the use of exigent letters, including the FBI's efforts to provide legal process to cover records [redacted] and often acquired in response to exigent letters or other informal requests. The chapter is divided into two time periods: (1) the initial efforts from 2003 through October 2006; and (2) the efforts, beginning in November 2006, after attorneys in the FBI Office of the General Counsel (FBI OGC) National Security Law Branch (NSLB) learned about "blanket NSLs" that Communications Analysis Unit (CAU) personnel had drafted and Counterterrorism Division (CTD) officials had signed to cover previously acquired telephone records.[170]

I. The FBI's Attempts at Corrective Actions From 2003 through October 2006

We determined that CAU personnel who issued exigent letters to the on-site communications service providers for records or calling activity information, or used other informal means for requesting records without legal process, sometimes obtained after-the-fact legal process, such as NSLs, to "cover" the original requests. However, as described in Chapter Three of this report, the *Electronic Communications Privacy Act* (ECPA) does not authorize the FBI to obtain such records unless it first serves compulsory legal process, such as an NSL, or the provider makes a voluntary production pursuant to Section 2702's emergency disclosure provision.[171] There is no provision in the ECPA authorizing the issuance of

---

[170] FBI personnel first used the term "blanket NSL" in August 2006 to describe certain after-the-fact NSLs prepared by CAU personnel and signed by CTD officials. We also use that term in this report.

[171] The ECPA NSL statute requires communications service providers to comply with requests for telephone subscriber and toll billing records information if the Director or his designee

> certifies in writing . . . that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

(Cont'd.)

retroactive legal process.[172] Therefore, after-the-fact NSLs would not cure a prior improper receipt of records under the ECPA.

As described below, from 2003 through October 2006 CAU Unit Chief Glenn Rogers and his successor Bassem Youssef took steps to request the issuance of after-the-fact NSLs from FBI operating divisions to cover these records. Because the CAU was an operational support unit, CAU personnel did not conduct investigations. CAU personnel were not authorized to issue NSLs. The unit therefore depended on field or Headquarters divisions to prepare and issue the after-the-fact NSLs. However, the operating divisions often did not respond quickly and sometimes did not respond at all to the CAU's requests for after-the-fact NSLs. As a result, during Rogers's tenure as CAU Unit Chief, a backlog developed of requests for legal process for records that had been provided by the on-site communications service providers at the CAU's request. We determined that Rogers did little to address the backlog. After Rogers left and Youssef became the Unit Chief in November 2004, Youssef began taking steps in approximately April 2005 to address the backlog of legal process owed to one provider, but did not recognize or begin to address the backlog for the other providers until October 2005.

The FBI OGC also became involved in addressing the exigent letters practice during this time period. We found that in December 2004, NSLB attorneys in the FBI OGC became aware of the CAU's use of exigent letters and its difficulty in obtaining prompt after-the-fact NSLs from the operating divisions. However, NSLB attorneys failed to direct that the CAU end the practice of issuing exigent letters with the promise of legal process until March 2007, following release of the OIG's first NSL report.

Moreover, beginning in January 2005, NSLB attorneys themselves became involved with the CAU in issuing after-the-fact NSLs to cover the records acquired in response to exigent letters. The NSLB attorneys also attempted to initiate a process that would ensure prompt issuance of after-the-fact NSLs predicated on open national security investigations. However, this effort was ineffective because the issuance of after-the-fact legal process would not retroactively validate an improper disclosure of records under the ECPA, even if the legal process was served a short time after receipt of the records. In any event, the proposal was never

---

18 U.S.C. § 2709(b).

[172] See *In re Application of U.S. for Nunc Pro Tunc Order*, 353 F. Supp. 45, 46 (D. Mass. 2005).

implemented. While NSLB attorneys focused during this period on the issuance of NSLs for ongoing CAU exigent letter requests, they did not recognize and address in a timely manner the legal flaw with issuing after-the-fact NSLs.

We also describe the actions of the CAU Unit Chiefs and the NSLB attorneys regarding the CAU's use of exigent letters, the backlog of promised legal process, and the actions taken to address the backlog.

A. A Backlog First Develops During Rogers's Tenure as CAU Unit Chief

Rogers told us that during his tenure as CAU Unit Chief from March 2003 to November 2004, he regularly reminded CAU personnel to stay current on NSLs that were owed to the providers. He also said he sometimes spoke with personnel assigned to CTD operational units about the importance of issuing after-the-fact legal process for telephone records, and on one occasion spoke with a field division about providing an after-the-fact NSL to the CAU. However, Rogers did not require CAU personnel to maintain lists of telephone numbers for which the CAU had requested information from the on-site providers, or otherwise to keep track of exigent letters to ensure that legal process followed the exigent letters. Instead, CAU personnel relied on the three on-site communications service providers to tell them whether legal process had been provided to cover the records acquired in response to exigent letters.

We determined that by November 2004, the CAU had made requests for records to the on-site providers for hundreds of telephone numbers for which legal process had not been provided. The on-site Company B employee, who first came to the CAU in September 2004, told us that by November 2004 he was concerned that Company B was not receiving after-the-fact legal process for records he had provided to CAU personnel in response to exigent letters. He said he spoke to Rogers about the backlog of records requiring legal process before Rogers left the CAU in November 2004 to become the Assistant Section Chief for the CTD's Communications Exploitation Section (CXS) (the CTD Section that oversaw the CAU). According to the Company B employee, Rogers told him "these take a little time" and "you need to stay after the guys." The Company B employee said that he was surprised by Rogers's response because he did not think he should be responsible for following up with CAU personnel.

Although a backlog of record requests requiring legal process developed in the CAU, CAU personnel continued to sign and issue exigent letters to satisfy the operational support requests from FBI headquarters, the CTD's operational units, and field divisions. A significant number of these requests came from the International Terrorism Operations Section 1

(ITOS-I), which was responsible for addressing many of the international terrorism threats directed at the United States during this period.

ITOS-I managers told us that they did not know about any CAU backlog in obtaining follow-up legal process in 2004 and 2005. Several ITOS managers told us that CAU personnel attended the daily ITOS briefings at which major terrorism investigations were discussed. At the conclusion of these briefings, the CAU was often directed to analyze telephone numbers identified in the course of these investigations to determine whether they had any U.S. connections. ITOS-I managers told us they did not know the mechanics of how the CAU accomplished its work, although most of these managers told us they were generally aware that the CAU used the resources available from the on-site communications service providers and various FBI databases, [redacted] to respond to these taskings.[173]

ITOS-I witnesses also told us that while they were unfamiliar with the procedures used by the CAU to analyze telephone numbers, they assumed that CAU personnel followed appropriate legal requirements. For example, Michael Heimbach, who was the CTD Assistant Section Chief over ITOS-I from February 2003 to March 2004 and the ITOS-I Section Chief from March 2005 to January 2007, told us:

> . . . it's their lane. It's the operational support's lane, meaning this is their job. This is their business. How, what relationships they had with Company A, Company C, and [redacted], I have no clue. I mean I . . . wasn't in the weeds with them on it . . . . How they did it, what they were doing, what the process . . . wasn't my lane of traffic.

Shortly before Rogers left the CAU in November 2004 to become the CXS Assistant Section Chief, he instructed a CAU Intelligence Analyst to implement a tracking system for records requests so that the CAU would not have to rely on the on-site providers to know whether after-the-fact legal process had been served. As discussed below, the tracking system was developed and later abandoned after Rogers left the CAU.

---

[173] As described in Chapter Two of this report, CAU personnel had access to a [redacted] database that CAU analysts regularly queried for records and used to perform analytical work. CAU personnel sometimes responded to requests for assistance through data analysis in this database. At other times, CAU personnel obtained data from the on-site providers, then analyzed the results once the records were uploaded into this database.

Rogers told us that when he left the CAU he was not aware that there were any record requests that still required legal process. By contrast, as described above, the Company B employee told us that he discussed the backlog with Rogers before Rogers's departure from the CAU. In addition, the Assistant General Counsel who was the NSLB point of contact for NSL-related policies and issues told us that in late 2004 or early 2005, Rogers told her that there were about 80 NSLs or telephone numbers for which after-the-fact NSLs had not been served. The Assistant General Counsel said that she was also informed at that time that the CAU was implementing a new tracking system for exigent letters and she believed that when the system was implemented the CAU would be better able to track telephone numbers requiring NSLs.

We also determined that the CAU Intelligence Analyst who was responsible for implementing the tracking system requested and received lists from Company B and Company C in January 2005 identifying a total of 188 telephone numbers requiring legal process that the providers had previously [redacted] in response to the CAU requests. These 188 telephone numbers represented approximately two-thirds of the total number of telephone numbers that CAU personnel had included in exigent letters or other informal requests to Company B and Company C in 2004.[174]

Thus, when Youssef succeeded Rogers as the CAU Unit Chief in November 2004, there was a significant backlog of telephone records requests for which legal process had been promised but not delivered.

As we describe below, shortly after Rogers was promoted and Youssef became CAU Unit Chief, the Assistant General Counsel alerted her supervisors in the NSLB about the CAU's practice of using exigent letters. We determined that NSLB attempted to institute a process for issuing NSLs quickly – albeit still after-the-fact – to cover future CAU requests for records from the on-site providers in exigent circumstances. However, months passed before Youssef and the NSLB attorneys recognized and addressed the issue of the large backlog of requests for which the providers had [redacted] or provided the FBI records but were still awaiting legal process.

---

[174] The Company C employee first arrived at the CAU in April 2004, and the Company B employee arrived in September 2004. Company A did not give CAU personnel a list of telephone numbers requiring legal process in January 2005; however, we have no reason to believe that the CAU was any more successful in obtaining after-the-fact legal process for Company A than for the other providers.

B. NSLB Knowledge of Exigent Letters and Involvement in Issuing After-the-Fact NSLs

We determined that although the CAU began using exigent letters in March 2003, FBI attorneys were not alerted to the practice until July 2004. On July 19, 2004, a CAU Intelligence Analyst sent an e-mail to the Assistant General Counsel stating that the CAU had a Company A analyst on-site. The e-mail described the services that Company A provided, noting that in time-sensitive threat matters the CAU could obtain information from the on-site Company A analyst by using "an exigent letter" and following up later with an NSL.

However, the Assistant General Counsel told us she believed she first became aware of the use of exigent letters in December 2004. She said that she must have overlooked the reference to exigent letters in the July 19 e-mail from the CAU analyst.

The Assistant General Counsel said that she recalled learning about exigent letters in December 2004 in connection with a specific request from the CAU that NSLB prepare an after-the-fact NSL. FBI e-mails reflect that in mid-December 2004, a CAU SSA asked the NSLB to prepare an NSL to cover records for telephone numbers that had been previously obtained. The CAU SSA told the Assistant General Counsel that the telephone numbers included numbers that had been previously [redacted] by Company A pursuant to the CAU "form letter" requests that promised future legal process.

The Assistant General Counsel reported the CAU request to her immediate supervisor and to NSLB Deputy General Counsel Julie Thomas, in an e-mail dated December 17, 2004.[175] In that e-mail, the Assistant General Counsel informed them that in connection with the request, the CAU SSA had told her the following:

- The CAU was regularly obtaining records without legal process from the on-site communications service providers.

---

[175] In this section of the report, we rely significantly on e-mails to and from the Assistant General Counsel. She told us that because many of the issues we interviewed her about happened more than 3 years earlier, she could not recall the events with certainty. However, she stated that the e-mails accurately depicted her understanding of events at the time.

- The CAU often received emergency requests for records from senior FBI officials and used a "form letter" to obtain these records that promised after-the-fact legal process.
- The CAU attempted to obtain after-the-fact legal process from field divisions.
- Field divisions often would not respond to the CAU's requests for follow-up legal process.
- The CAU was starting a "tickler system" to track follow-up legal process requests.

However, at this time the Assistant General Counsel did not ask to see a copy of the "form letter" promising future legal process that the CAU SSA told her had been used to obtain records. However, she told us, and her contemporaneous e-mails confirm, that from the time she was told about the CAU obtaining records with exigent letters through late 2006 she consistently told CAU personnel that the exigent letters practice should be limited to emergency situations and that after-the-fact NSLs must follow promptly.

The Assistant General Counsel said she believed that in emergency situations, after-the-fact NSLs were appropriate as long as they were issued within 24 to 48 hours of the exigent letter request. She told us that she recognized that there was "no specific provision" in the ECPA authorizing issuance of after-the-fact NSLs, but she said she believed that the legislative intent of the statute would permit prompt issuance of after-the-fact NSLs in "real emergencies . . . where peoples' lives are at issue." She said that during this period, she sought to ensure that the follow-up NSLs were issued quickly, but assumed that the CAU was issuing exigent letters only in true emergencies. She also told us that she understood that her supervisors were in agreement with her analysis that after-the-fact NSLs were appropriate in emergency situations.

Although the Assistant General Counsel did not object to drafting the after-the-fact NSL for the previously obtained records, in a follow-up e-mail dated December 23, 2004, to her supervisor and Thomas, the Assistant General Counsel stated that because the NSLB knew the records had already been received she thought they should phrase the NSL to reflect that fact. She also stated in the e-mail that she was "real uncomfortable doing it any other way" and that she did not think she could issue the NSL as if she were unaware the FBI already had the information. She also noted that the CAU SSA was unhappy with her suggestion that the NSL state that records had been previously provided and the SSA told her the provider was expecting "a regular NSL."

Thomas replied to the Assistant General Counsel's e-mail, stating that she would discuss the issue with NSLB supervisory attorneys. Thomas also asked the Assistant General Counsel for proposed language for the after-the-fact NSL. However, Thomas also did not ask to see the exigent letter that had been used to obtain the records, did not at that time (or at any time until late 2006) review the contracts with the providers, and did not ask anyone in NSLB to do so.

Ultimately, Thomas signed an after-the-fact NSL dated January 18, 2005, addressed to Company A. We determined that this NSL included some telephone numbers that were listed in exigent letters dated July 13, 14, and 15, 2004, that were given to an on-site Company A analyst. Despite the misgivings expressed by the Assistant General Counsel to her supervisors about signing NSLs that did not disclose that the FBI had already received the records, the NSL and accompanying approval EC did not state that Company A had previously provided the records to the FBI.

We found that Thomas signed six additional after-the-fact NSLs over the next 4 months in which the NSLs themselves and the accompanying approval ECs did not disclose that these records had previously been requested and received by the FBI. Thomas signed an NSL dated February 2, 2005, addressed to Company A, which included a list of 63 telephone numbers related to Operation "W."[176] We determined that this NSL included some telephone numbers that were listed in exigent letters given to the on-site Company A analysts as early as [redacted] Thomas also signed an after-the-fact NSL dated February 2, 2005, addressed to Company B, which related to Operation W and listed one telephone number. The FBI had previously requested records for this telephone number in an exigent letter dated [redacted]

Thomas signed two NSLs dated June 28, 2005, addressed to Company A and Company C. These NSLs sought records from each provider for 163 telephone numbers related to another major FBI operation. All of these telephone numbers had previously been [redacted] and records for many of them had been provided to the CAU as early as [redacted] On June 30, 2005, Thomas signed at least two more after-the-fact NSLs in connection with another counterterrorism investigation. These two NSLs covered records for telephone numbers that the CAU had requested from the providers in October 2004. E-mails show that the Assistant General Counsel had informed Thomas prior to her signing the NSLs that these

---

[176] The name of this operation is classified.

records had been provided to the FBI 8 months earlier. Thomas told us that she did not recall the e-mails or these two NSLs, but she characterized the investigation to which the NSLs were related as "the greatest of emergencies."

In an interview in August 2008, Thomas acknowledged that she signed these seven after-the-fact NSLs, although she told us that she did not have a specific recollection of any of the NSLs themselves. Thomas said she has signed thousands of NSLs and therefore could not recall specific NSLs. She said that the CAU was one of nearly 100 FBI units that NSLB supported, and she noted that these NSLs were dated up to 3½ years ago. She also said she relied on the accompanying approval ECs, which are reviewed by at least one and sometimes two NSLB attorneys, for the facts relating to the NSLs she signed.

Thomas also said she did not recall being told that the telephone numbers listed in the NSLs had been previously [redacted] and that records already had been provided to the CAU. When we showed her the December 23, 2004, e-mail exchange between her and the Assistant General Counsel described above, in which the Assistant General Counsel raised her concern that the NSL should document that the FBI already had the records, Thomas said she did not recall the exchange and also did not recall having any discussions about that issue with NSLB supervisors.

In August 2008, Thomas also told the OIG that she did not believe that follow-up NSLs were required regarding this information because she believed during the period when these NSLs were signed that the CAU's requests to the on-site providers "were likely all emergency circumstances." Thomas said she therefore concluded that the requests the CAU made to the on-site providers fell within the emergency voluntary disclosure statute, 18 U.S.C. § 2702(c)(4), and that "follow-on NSLs would not be required." However, when probed on whether she and other FBI OGC attorneys relied on Section 2702 in 2004 and 2005, Thomas stated that she could not separate what she knew at the time of her interview from what she knew then.[177] Thomas said the reason the FBI provided follow-up NSLs in these cases was because the on-site providers wanted them.

---

[177] As noted, prior to March 2006, 18 U.S.C. § 2702(c)(4) provided that a communications service provider could voluntarily provide telephone records to the FBI if the provider "reasonably believes that an emergency involving danger of death or serious physical injury justifies disclosure of the information." We discuss in Chapter Six of this report our conclusion regarding the applicability of the emergency voluntary disclosure (Cont'd.)

Thomas also said that since the follow-up NSLs she signed were not legally required, she saw no need for the NSLs to document that the records requested had been previously provided. She said she was confident that the on-site providers were aware that the records had been previously provided and were not misled by the absence of any reference to this fact in the follow-up NSLs.

C. NSLB Attorney Meets with CAU Personnel Regarding Exigent Letters

In addition to learning about the problems in obtaining after-the-fact NSLs and addressing the request for an after-the-fact NSL, the Assistant General Counsel learned in early 2005 that in some instances CAU personnel had issued exigent letters to communications service providers in the absence of any authorized and open national security investigation.[178] The Assistant General Counsel was concerned about this practice because the ECPA NSL statute and the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) required that information sought in NSLs be relevant to an "authorized investigation to protect against international terrorism or clandestine intelligence activities . . . ."[179] The Assistant General Counsel believed that after-the-fact NSLs could not be issued unless they were relevant to an open, authorized national security investigation.

On January 6, 2005, the Assistant General Counsel met with CXS Assistant Section Chief Rogers and a CAU SSA to discuss the CAU's process for obtaining records from the on-site providers.[180] E-mail records show

---

statute to the CAU's acquisition of ECPA-protected records from the on-site providers pursuant to exigent letters or other informal requests.

As discussed below, FBI General Counsel Caproni and the Assistant General Counsel told us that they did not discuss amongst themselves or conclude in 2004, 2005, or 2006 that the acquisition of subscriber and toll billing records in response to exigent letters qualified as emergency voluntary disclosures pursuant to 18 U.S.C. § 2702(c)(4).

[178] Many of the signers of these exigent letters told us that in these instances they were concerned about addressing the exigency and did not consider whether an investigation had yet been opened. One signer told us that he anticipated an investigation would be opened shortly after the exigent letter was issued.

[179] NSI Guidelines, Section V(12)("use of National Security Letters in conformity with . . . 18 U.S.C. § 2709 (relating to subscriber information, toll billing records . . . . " See 18 U.S.C. § 2709(b).

[180] Youssef's attorney has asserted to the OIG that Youssef was "excluded" from or "not invited to" this meeting. However, Youssef's FBI e-mails show that he was invited to the meeting and that the time of the meeting was changed at his request in order to (Cont'd.)

that they discussed issues concerning the emergency records requests CAU personnel had been receiving, including the fact that CAU personnel were given little information about the requests. In an e-mail to Thomas on January 6 shortly after the meeting, the Assistant General Counsel reported that Rogers and the SSA told her they were "inundated" with emergency requests, including requests from Gary Bald, the Executive Assistant Director of the FBI's National Security Branch. She stated they told her that in response to Bald's requests, the CAU would obtain records from the on-site providers "with very little background as to why the telephone number is important." The Assistant General Counsel informed Thomas that she told Rogers and the SSA that they should tell Bald that they needed more information about the requests and that they could tell Bald that NSLB attorneys required predication for obtaining the information. The Assistant General Counsel added in her e-mail, "But I know that's not going to happen."[181]

Bald confirmed to us that he often requested information regarding telephone numbers from the CAU. He said that the CAU provided valuable information and that he had repeatedly encouraged his subordinates in CTD operational units to utilize the CAU and the on-site providers' resources. However, he said he was unaware of the procedures the CAU used to comply with his requests. He said he did not know that the CAU used exigent letters and assumed that NSLs were issued to the providers prior to release of information to the FBI. He also said he was never told that the on-site providers were providing information to the CAU before they received an NSL.

In her January 6 e-mail to Thomas, the Assistant General Counsel proposed that NSLB personnel be made available to the CAU to help get NSLs signed quickly after the FBI acquired records from the on-site providers in emergency situations. She acknowledged that under her proposal the CAU would still receive records prior to issuance of the NSLs, but stated that her plan would ensure that NSLs would be issued "very shortly after" any information was provided.[182]

---

facilitate his attendance. However, Youssef did not attend and later apologized for missing the meeting.

[181] Thomas told us that while she did not recall this particular e-mail and did not speak with Bald about this issue, she agreed with the Assistant General Counsel's advice. She said that on numerous occasions she has provided similar advice to FBI personnel so that "they can use the lawyers as the 'fall guy'."

[182] The Assistant General Counsel also informed Marion Bowman, who had previously served as NSLB Deputy General Counsel, of her concern that the CAU was not (Cont'd.)

In mid-January 2005, Thomas agreed to a proposal from the Assistant General Counsel's supervisor that two NSLB attorneys and a paralegal serve as the NSLB points-of-contact for the CAU to prepare after-the-fact NSLs to cover records obtained through exigent letters.

Also in January 2005, the Assistant General Counsel proposed a solution to her NSLB supervisors, including Thomas, which she believed would ensure that telephone numbers listed in exigent letter requests would be relevant to open national security investigations. She proposed that CTD operational units open generic preliminary national security investigations (called "umbrella files") for various types of recurring threats to the United States.[183] The Assistant General Counsel suggested that when CAU personnel were asked by field divisions or FBI Headquarters to request telephone records from the on-site providers in cases where there was no open national security investigation to which the records were relevant, CAU personnel would associate the telephone number with one of the open umbrella files based upon the nature of the threat. As discussed below, however, this umbrella file proposal was never implemented.[184]

On January 26, 2005, the Assistant General Counsel and the two NSLB attorneys designated as the points of contact met with CAU personnel to discuss their proposed assistance to the CAU. Both point-of-contact attorneys told us that the umbrella file idea was discussed at the meeting

---

obtaining predication information from FBI requesters. In a November 2006 e-mail, the Assistant General Counsel informed Caproni that Bowman had spoken to "higher ups to make sure they understood that CAU needed more information when doing a request in order for the request to allow for an NSL." Bowman told us that he spoke with CTD DAD John Lewis about the Assistant General Counsel's concern, but did not raise the issue with other FBI officials.

[183] When the FBI opens an investigation, each investigation is assigned a unique file number. If implemented, the Assistant General Counsel's proposal would have resulted in the assignment of a unique file number for each type of generic threat, such as threats against transportation facilities, infrastructure, or special events. This file number would then serve as the authorized national security investigation referred to by FBI personnel in preparing the Electronic Communication (EC) seeking approval of after-the-fact NSLs.

[184] The umbrella file proposal would have addressed only one aspect of the exigent letter problem – the ECPA requirement that records sought in NSLs be relevant to authorized national security investigations. See 18 U.S.C. § 2709(b). However, as discussed in Chapter Six of this report, the core legal problem with exigent letters was that the ECPA does not authorize the FBI to obtain telephone toll records unless it first serves compulsory legal process such as an NSL, or the provider makes a voluntary production pursuant to Section 2702's emergency disclosure provision. Thus, even if there were authorized investigations to which the records sought in exigent letters were relevant, this legal problem would remain.

and both said they understood that they would be assisting the CAU in issuing NSLs quickly in emergency situations. They both said they understood that the NSLs they would facilitate would be issued prior to the CAU obtaining records, not after the records had already been obtained. In addition, they said that they understood that they would be working on future requests for records and that they were not aware of any backlog of requests for which legal process had been promised. One of the attorneys stated that when she left the meeting she did not expect to receive any NSL requests from the CAU until the umbrella file proposal was implemented.[185]

CAU Unit Chief Youssef did not attend this meeting. He told us he did not know until 2007 that the NSLB had designated points of contact to assist the CAU with NSLs.[186] However, FBI e-mails reflect that Youssef was informed in advance about the proposed NSLB assistance and about the January 26, 2005, meeting with NSLB personnel, and that he had instructed CAU personnel to attend the meeting.

Both of the point-of-contact attorneys told us that in the months following the January 26 meeting they did not receive any requests for assistance from the CAU although they were included on various e-mails addressing the umbrella file issue. FBI e-mails also reflect that several months after the January meeting the Assistant General Counsel notified her supervisors that the NSLB attorneys had not received any requests for assistance from the CAU.

In connection with the January 26, 2005, meeting, Youssef told us that beginning in November 2004 (when he became Unit Chief), and continuing through mid-April 2005, Rogers "specifically kept me out of several communications, several e-mails between [Rogers] and NSLB." Youssef said that, "Rogers knew about the fact that I was going to be at another meeting that day . . . . This was an indication that I was not needed at this meeting." Youssef stated that Rogers generally kept him "out of the loop" and that Youssef was not able to raise concerns he had about how the CAU was being run to Rogers because Rogers was not willing to listen to his suggestions.

---

[185] We also reviewed various e-mails between the Assistant General Counsel and NSLB supervisors in which she expressed her opinion that without open umbrella files the two point-of-contact attorneys and the paralegal could not assist the CAU with preparing NSLs.

[186] FBI records reflect that Youssef was on sick leave the day of the meeting.

D. CAU Begins Implementing then Abandons a Tracking System for Legal Process

In early February 2005, CAU personnel began using a new tracking system for requests to the on-site providers that Rogers had asked to be implemented. The system, known as the "Tracker Database," was designed to collect information about each records request to the on-site communications service providers. The database contained fields to identify the:

- communications service provider;
- request date;
- CAU requester;
- pertinent telephone numbers;
- whether an exigent letter was issued;
- type of legal process to follow (NSL or grand jury subpoena);
- records receipt date;
- contact information for the field or headquarters requester; and
- date the CAU received legal process and served it on the provider.

In an e-mail message to all CAU personnel dated February 2, 2005, the CAU Intelligence Analyst who was responsible for managing the Tracker Database wrote that at Rogers's direction all CAU personnel were required to use the database. The Intelligence Analyst also wrote that there were "about 100 pending NSL[s]" for which legal process had not yet been issued to 2 of the 3 on-site providers, Company B and Company C.[187] The Intelligence Analyst added, "using the [Tracker Database] is not optional and it's a way for us to cover ourselves in case anyone starts asking questions."

---

[187] The e-mail message stated that a Company A analyst had not yet provided a list of record requests (telephone numbers) that required legal process. The e-mail also listed the number of "pending NSLs," not the number of telephone numbers awaiting follow-up legal process. As stated above, in January 2005 the Intelligence Analyst responsible for the tracking system had received a list of 188 telephone numbers which Company B and Company C had identified as still requiring legal process.

The Intelligence Analyst told us that CAU personnel showed little enthusiasm for using the Tracker Database because they did not want the responsibility for inputting the data. The Intelligence Analyst said that after she reported to Youssef several months later that the database was not being used by CAU personnel, she halted her efforts to implement the Tracker Database and no other CAU-wide tracking system for identifying the need for after-the-fact legal process was implemented.

Rogers told us that when Youssef became the CAU's Unit Chief he did not provide Youssef with any guidance or instructions on how to use exigent letters or on how to track exigent letters to ensure they were followed up with after-the-fact legal process. Rogers said he never discussed exigent letters with Youssef.

Youssef told us that he did not require CAU personnel to use the Tracker Database. He said that after he received the February 2, 2005, e-mail from the Intelligence Analyst, he held an "all-hands" meeting at which the Tracker Database was discussed. He said that at the meeting there was an "outcry" and that nobody in the CAU (other than the Intelligence Analyst who designed it) wanted to use the database because it was too cumbersome. He said that the database "died instantly" because he told Rogers no one wanted to use it, and Rogers did not instruct him that it had to be used.

Youssef also told us that when the Tracker Database issue arose in February 2005 he did not yet know that the CAU was obtaining records prior to service of legal process. We therefore asked Youssef what he was thinking at the time about the reference in the Intelligence Analyst's February 2 e-mail to "100 pending NSLs." Youssef said he could not remember, but he may have thought "there are NSLs that we still have to serve. I mean, I did not see it as pending as in NSLs we never got. That was not my understanding and frankly I do not remember much of this here."

E. CAU Unit Chief Youssef Learns that the CAU has Obtained Records in Advance of Legal Process

Youssef told us that he first learned that the CAU was obtaining records before service of legal process shortly before his first meeting with the Assistant General Counsel, which we determined occurred on March 11, 2005. On that date, Youssef and two other CAU SSAs met with the Assistant General Counsel at the off-site location where she was assigned. He said that he and the SSAs were at the off-site location for another purpose, and he decided that while there he would introduce himself to her. Youssef informed Rogers in a contemporaneous e-mail that he had discussed "streamlining the NSL process" at the March 11 meeting.

Youssef said that some time before that meeting, a Company A analyst told him "in passing" of an instance in which Rogers had requested records from the analyst prior to service of legal process. The analyst informed Youssef that Rogers had told the analyst it was an emergency and that Executive Assistant Director Bald wanted the records. Youssef told us that based on this information, he informed the Assistant General Counsel at the March 11 meeting that the CAU "may be in the practice" of obtaining records without legal process and that he thought it was wrong. Youssef said that the Assistant General Counsel told him she understood that the CAU sometimes received emergency requests and obtained information before serving a legal instrument. Youssef stated that based on the Assistant General Counsel's comments at the meeting, it was clear to him that she was already aware that the CAU was obtaining records prior to the issuance of legal process.

Youssef told us that he did not discuss with the Assistant General Counsel at the March 11 meeting the CAU's use of exigent letters or the backlog of records for which legal process had not been issued because he said that at the time he was unaware of these issues. He told us that he also was unaware at the time of the frequency of requests to the CAU from FBI upper management related to telephone records.

Youssef said that sometime after meeting with the Assistant General Counsel, the on-site Company B employee told Youssef that he had not received NSLs that were "owed" to him. Youssef told us that he believed this conversation "probably" occurred right after his meeting with the Assistant General Counsel, in late March or early April 2005, but that it could have happened in May 2005. Youssef said that the Company B employee told him that he was owed over 100 NSLs and that the conversation alarmed him.

The Company B employee confirmed that he discussed with Youssef Company B's backlog of records requiring legal process. The Company B employee said he believed that they had discussed the backlog in early 2005, shortly after Youssef arrived at the CAU. The Company B employee said that soon after speaking with Youssef about the backlog, at Youssef's request he began to send e-mails directly to CAU personnel asking for NSLs to cover the backlog. The Company B employee also said that he went back to Youssef approximately a month later because he still was not receiving legal process. He said that in response, Youssef held a unit meeting and told CAU personnel to get the proper documentation to the on-site providers.

Youssef told us that after speaking with the Company B employee he asked CAU personnel about the issue and several of them said they used exigent letters to obtain records in advance of legal process. Youssef told us

that he had heard the term "exigent letters" before, but this was the first time he was told such letters were used to obtain records from the on-site providers. He said that the first time he actually saw an exigent letter was when he signed one in November 2005.[188]

Youssef told us that within "a day or two" after learning that the CAU was using exigent letters and obtaining records prior to issuance of legal process, he had a conversation with Rogers, who at the time was his supervisor as the CXS Assistant Section Chief. Youssef said that in this conversation he told Rogers the practice was "a major issue." According to Youssef, Rogers was "nonchalant" about the matter. Youssef said that Rogers told him, "No, this is the procedure. This is how we do it. We can go get the requests from the phone companies and then we will get the NSLs later." Youssef said that after the conversation with Rogers, he concluded that, "if that is what he is telling me . . . if I went against it and said we are not going to use exigent letters for example, I would have been insubordinate."

Youssef told us that he did not bring his concern about the CAU obtaining records from the on-site providers with exigent letters rather than legal process to anyone else in his supervisory chain of command, other than Rogers.[189]

Rogers told us that Youssef never spoke with him about exigent letters or the backlog of NSLs. He said Youssef probably learned about exigent letters, like Rogers did, "when somebody came to him and . . . told him it existed." Rogers said that he never provided any oversight or guidance to Youssef about the letters.

Youssef also told us that he did not feel he could go above Rogers with his concerns to CXS Section Chief Laurie Bennett or to the Deputy Assistant

---

[188] Youssef also told us that he did not closely read the exigent letter he signed in November 2005, and that the first time that he "really scrutinized" an exigent letter was in May 2006 when he was asked by a CAU Intelligence Analyst to sign another exigent letter. Youssef said that he then read the exigent letter and realized that it referenced a follow-up subpoena. He said because the exigent letter referenced a subpoena, he did not sign the May 2006 letter.

[189] In a letter to Senator Charles E. Grassley, dated March 17, 2007, Youssef's attorney stated that in a CXS Unit Chiefs' meeting, Youssef raised the issue of the CAU's use of exigent letters to the CXS Section Chief who "was dismissive of the concern." Youssef told us that Rogers was the Acting CXS Section Chief at this meeting.

Director (DAD) for CTD, John Lewis.[190] He said that shortly after Bennett came to the CXS in August 2004, she expressed her dissatisfaction with his performance as a Unit Chief for the CXS Document Exploitation Unit and that "within three weeks [of her arrival at CXS], everything I did was wrong." Youssef also asserted that Bennett began expressing her dissatisfaction with his performance "within the same week" of when his attorney provided a list of FBI witnesses to be deposed in an connection with an Equal Employment Opportunity Commission complaint Youssef filed against the FBI. Further, Youssef said that Bennett's supervisor, DAD John Lewis, also "was after" him and was "retaliating after me mercilessly." Youssef added that he believed Lewis was "not going to pay attention to anything that I am saying." Youssef stated that he never brought his concerns about the exigent letters practice to anyone else in his chain of command because he "really did not have access to talk to anybody."

F. NSLB Attorney Provides Incorrect Advice to the CAU About the Use of Exigent Letters

On April 26, 2005, the Assistant General Counsel sent an e-mail to Youssef expressing concern that "on occasion, CAU is presuming that someone who comes to them [seeking records from the on-site providers] has an emergency." She instructed Youssef "not [to] assume that all people who come to you are in an emergency situation" and to ensure that CAU personnel were "instructed to ask for an NSL." She also reminded Youssef that if exigent letters were used, the CAU could ask the designated NSLB attorneys to draft the after-the-fact NSLs. She wrote that the NSLB could do the NSLs quickly and that she personally would do whatever it took to get NSLs done in a day or two. Finally, she wrote that "we are willing to allow these requests when there really are exigent circumstances . . . only if it is clear . . . that the requestor cannot await an NSL."

The Assistant General Counsel told us that she could not recall the circumstances surrounding this e-mail. However, we determined from her contemporaneous e-mails that her concern arose from an instance in which a Headquarters operational unit obtained toll billing records from the Company C on-site analyst using the exigent letter process and then sought an after-the-fact NSL from the NSLB.[191] The Assistant General Counsel was

---

[190] Laurie Bennett was the CXS Section Chief from August 2004 to April 2006. John Lewis was the CTD DAD from May 2004 to June 2006.

[191] After reviewing a draft of this report, Youssef's attorney suggested that the Assistant General Counsel's April 26, 2005, e-mail was in response to a request from Youssef for guidance. However, as described above, we determined through (Cont'd.)

initially uncertain about why the exigent letter process was used in this matter, and the Headquarters operational unit subsequently explained to her the exigent circumstances that led to the request.

Youssef responded by e-mail on April 27, 2005, that the Assistant General Counsel was "absolutely right" and that he would instruct the CAU staff as she had requested.[192] On April 27, Youssef also forwarded the Assistant General Counsel's e-mail to all CAU personnel and the on-site communications service providers' employees, directing them to review the e-mail. Youssef added in his forwarding e-mail, "We all need to differentiate between what is an exigent request and what is not."

We determined that after Youssef forwarded the Assistant General Counsel's e-mail to CAU personnel there was a decrease in the number of exigent letters issued by the CAU, as reflected in Chart 2.3 in Chapter Two of this report. However, as described in this chapter and in Chapter Two, field and Headquarters requests to the CAU for records or calling activity information continued, many of which were communicated to the on-site providers by informal means other than exigent letters, such as by sneak peek requests and requests communicated by telephone, e-mail, in-person, and on post-it notes.

As also discussed below and in Chapter Six, we concluded that the Assistant General Counsel's statement that an exigent letter was appropriate when "the requester cannot await an NSL" is inconsistent with both the ECPA NSL statute and the ECPA emergency voluntary disclosure statute.

G. NSLB Fails to Recognize Applicability of the ECPA's Authority for Emergency Voluntary Disclosures to Requests Sent to the CAU

On August 25, 2005, the FBI OGC issued a guidance memorandum to all FBI personnel, which described the circumstances in which the ECPA authorized the disclosure of the content and records of communications under 18 U.S.C. § 2702(b)(8) and 2702 (c)(4) in emergency circumstances. The guidance recognized that emergency voluntary disclosures were "outside of the compulsory process" and stated that such disclosures

---

contemporaneous e-mails that the Assistant General Counsel's guidance was prompted by a request from another Headquarters unit, not from Youssef.

[192] On April 27, 2005, the Assistant General Counsel forwarded her advice and Youssef's response to her immediate supervisor and Thomas.

"should not be followed with a subpoena or other compulsory process." The memorandum also stated that letters requesting emergency voluntary disclosures must be approved by Assistant Special Agents in Charge, Special Agents in Charge, or higher authority.[193] NSLB Deputy General Counsel Julie Thomas was among the approving officials on the memorandum.

We found that during the period when FBI OGC attorneys were developing this guidance they did not consider or discuss how the emergency voluntary disclosure statute related to the use of exigent letters Indeed, the Assistant General Counsel acknowledged to the OIG and her supervisors that the NSLB had not relied on the emergency voluntary disclosure statute as authority for issuance of exigent letters.

In an interview on July 20, 2006, OIG investigators asked the Assistant General Counsel about the legal basis for approving exigent letters. She stated that none of the NSL statutes "specifically addressed emergency situations." However, she said she believed that there was "an exception in national security circumstances where we think it's absolutely necessary." She said the FBI had "tried to reconcile the literal interpretation [of the NSL statutes] with the other policy considerations" that the FBI needs to deal with when "lots of lives are at stake." The Assistant General Counsel said that in making this judgment the FBI took into account its policy mandate, its mission, and the emergency voluntary disclosure statute. However, she said that she was "not pretending . . . in retrospect" that the FBI had relied on the emergency voluntary disclosure statute at the time to support the use of exigent letters.[194]

FBI General Counsel Caproni told us that she was unaware of the FBI's use of exigent letters or that the FBI had obtained records before issuing legal process until the OIG brought the issue to her attention in late

---

[193] Office of the General Counsel, Federal Bureau of Investigation, electronic communication to all Divisions, Emergency Disclosure Provision and Information From Service Providers Under 18 U.S.C. § 2702(b), August 25, 2005.

[194] We found that the Assistant General Counsel advised Thomas in an e-mail on July 20, 2006, following an OIG interview in this matter, "[a]rguably, the CAU disclosures fall under 2702 disclosures, although we have never tried to fit them under that . . . and maybe we should, and that would solve the problem." She also told us in September 2007 that the emergency voluntary disclosure statute was not considered in regard to the CAU's activities, stating, "it never came up and it is kind of curious why it did not," and that "in retrospect, we probably should have [considered 18 U.S.C. § 2702(c)(4)], but I guess we did not see the need for it at the time."

2006. She added that, "[s]o, certainly at the time, no, we had no discussions that these [exigent letter requests] – would qualify under that provision of the ECPA."[195]

As noted above, NSLB Deputy General Counsel Thomas told us in August 2008 that she believed at the time she signed after-the-fact NSLs in 2005 that the CAU's requests to the providers were likely emergency requests that fell within 18 U.S.C. § 2702. However, she qualified her statement, noting that in light of the many interviews and conversations she had had on the subject she could not separate what she knew at the time of her interview from what she knew in 2005. In light of the Assistant General Counsel's and Caproni's recollections to the contrary and the contemporaneous documentary evidence corroborating their statements, we concluded that that the NSLB did not rely on 18 U.S.C. § 2702's emergency voluntary disclosure provision during the period the CAU issued exigent letters.

In Chapter Five of this report, we describe further the management failures that led to the continued use of exigent letters until mid-November 2006, including the FBI OGC's failure to instruct CAU personnel, in coordination with CTD management, to use the ECPA emergency voluntary disclosure statute rather than exigent letters in qualifying emergencies.

H. The September 26, 2005, Meeting

Although the number of exigent letters issued by the CAU declined after April 2005, the backlog of old requests requiring legal process persisted. We found that NSLB attorneys did not recognize or focus on the existence of the backlog of requests requiring legal process. Rather, the NSLB continued to focus on the umbrella file proposal in order to ensure that future emergency requests for records were quickly followed by NSLs.

In late September 2005, the Assistant General Counsel suggested a meeting with Youssef and personnel from CTD operational units to discuss her umbrella file proposal. She said her purpose for proposing the meeting was to have the operational units agree to open the umbrella files, which in

---

[195] Caproni also told us that although she was not aware of the CAU's use of exigent letters, she believed that if they were used in true emergencies they were defensible under 18 U.S.C. § 2702(c)(4).

her view could serve as the open national security investigations for emergency requests from which after-the-fact NSLs could be issued.[196]

The meeting took place on September 26, 2005. The Assistant General Counsel, her immediate supervisor, Youssef, and personnel from CTD operational units attended. The Assistant General Counsel told us, and her contemporaneous e-mails reflect, that although the purpose of the meeting was to discuss the umbrella file proposal, Youssef told her at the meeting that umbrella files were not needed because the CAU did not have many emergency situations in which requests were made without open national security investigations.[197] The Assistant General Counsel told us that Youssef came to the meeting with a "different agenda," which was to discuss that the CAU needed the operational units to respond to the CAU's requests for NSLs. She said that Youssef stated at the meeting that the CAU needed the CTD operational units "to understand that they need to issue these NSLs promptly when they are asked."

Youssef acknowledged to us that he had told the Assistant General Counsel at the meeting that emergencies were "few and far between" and that umbrella files were not needed. Youssef told us, however, that in this comment to the Assistant General Counsel he was addressing only instances in which there was "absolutely no predication, no case open, nothing." He estimated that CAU personnel requested records for such emergencies only 10 or 12 times over a period of "several months," but said he could not tell us for sure how often such emergencies occurred.

Youssef told us that at the meeting he emphasized that the CAU was attempting to address the "significant backlog" of legal process owed to the on-site providers. He said he explained that the CAU was not obtaining the legal process from the operational units and that "this is going to kill us." Youssef told us that he did not mention at the meeting how many requests for legal process were outstanding.[198] He also said that at the time of the

---

[196] Youssef told us that several months earlier he had discussed with the Assistant General Counsel that he would like to have NSLB attend a meeting with him and the CTD operational units' leadership.

[197] In an e-mail to Youssef dated October 21, 2005, the Assistant General Counsel wrote that Youssef had stated at the meeting that emergency requests were "few and far between" and that umbrella files were no longer needed.

[198] None of the other attendees from Headquarters' operational units recalled that backlogs were discussed at the meeting. Additionally, the Assistant General Counsel's contemporaneous e-mail summarizing the meeting made no reference to any discussion of the backlog problem.

meeting he was aware only that Company B had outstanding record requests that were not covered by legal process.

Youssef said that at the meeting the operational units agreed to issue NSLs prior to future requests for telephone records, except for "extreme cases where it is an emergency." He also said that an agreement was reached that the CTD operational units would provide the NSLs upon request from CAU personnel. In fact, beginning in November 2005, the number of exigent letters issued by the CAU to the on-site providers decreased significantly.

The Assistant General Counsel e-mailed Youssef on October 21, 2005, to confirm Youssef's statement in the meeting that "there no longer seemed to be a need to create umbrella files, as we had previously discussed." We found that the umbrella file proposal was not pursued after this.

I. The CAU Efforts to Reduce the Backlog

Beginning shortly before and continuing after the September 26, 2005, meeting, Youssef and CAU personnel made various additional efforts to obtain after-the-fact legal process for the backlogged record requests. On October 5, 2005, Youssef convened an "all-hands" CAU meeting in which he encouraged CAU personnel to ensure that all outstanding requests for records from the three on-site communications service providers were covered by legal process. Contemporaneous e-mails also show that on September 6, 2005, and October 26, 2005, Company B and Company C sent to CAU personnel spreadsheets listing the record requests that still required legal process.

In subsequent e-mails to CAU personnel, Youssef assigned these telephone numbers to the pertinent CAU teams and instructed the team leaders to contact the relevant FBI field divisions and the CTD operational units to address the backlog of after-the-fact NSLs. He referred to this task as "a priority matter."

The Assistant General Counsel told us that after the September 2005 meeting she followed up with Youssef in e-mails and telephone conversations to see what the NSLB could do to assist Youssef and the CAU in ensuring that the operational units provided the necessary NSLs. She also asked what instructions he would like the FBI OGC to give the CTD operational units and the field on that subject. She said that Youssef did not respond in writing to her e-mail message, but later spoke with her and

said that there were "no problems" and that he would let the NSLB know if they needed help.[199]

On January 5, 2006, the Company B on-site employee again sent an e-mail to Youssef and CAU team leaders with a spreadsheet of telephone numbers for which Company B still had not received legal process. The Company B employee stated in the e-mail that since he had sent the previous spreadsheet in September 2005, he had only received "one to two NSLs" and that the spreadsheet contained "a few additional cases."

On February 7, 2006, the Assistant General Counsel sent an e-mail to Youssef, with the subject line "Issuance of NSLs – Follow up," in which she inquired about the status of the CAU's issuance of NSLs. She wrote:

> The last we talked, in November, 2005, we understood that there was going to be an effort by [CTD operational units] to get these NSLs out and that you would be requesting these NSLs in advance of getting the information when you were not given enough information to go on . . . . We haven't heard from you in awhile and I wanted to make sure that there was nothing that needed to be done on our part to assure that these NSLs were being issued in a timely manner and they were being issued based on enough information to assure relevance to an authorized investigation.

On February 10, 2006, Youssef responded by e-mail:

> We are actually making some reasonable headway in getting the NSLs. Our telecom reps are very happy with the results. If we run into any resistance, I'll definitely reach out to you for assistance and backing.

Youssef told us that when he informed the Assistant General Counsel that NSLs were being issued in a timely fashion, he was referring not to after-the-fact NSLs covering the backlogged record requests, but rather to after-the-fact NSLs issued to cover new exigent letters being used by CAU personnel.

---

[199] The Assistant General Counsel also sent an e-mail message to Youssef on November 18, 2005, in which she wrote, "[w]e haven't seemed to be able to get in touch" and asked whether the CAU was obtaining the information it needed from requesters of "emergency telephone information" to ensure predication for the issuance of NSLs.

Youssef also told us that he did not then inform the Assistant General Counsel of the problems the CAU was facing regarding the backlogged record requests because he knew the process of obtaining after-the-fact NSLs for backlogged numbers would "take some time," and he wanted to "give it another two or three months."

However, CAU personnel told us that the CAU had little success in obtaining after-the-fact legal process for the backlogged items. Youssef also told us that the CAU's work to address the backlog from September 2005 to May 2006 ultimately was "an exercise in futility." CAU SSAs told us that the original requesters were not motivated to provide after-the-fact legal process after they had received the records from the CAU. In addition, one SSA noted that occasionally cases were closed between the time the exigent letter was served and the requesting unit was contacted for an after-the-fact NSL.

To determine how successful the CAU was in obtaining legal process, we reviewed spreadsheets that Company B and Company C gave to CAU personnel at various times during this period. In January 2005, September 2005, January 2006, and May 2006, the on-site Company B employee provided information and spreadsheets to CAU personnel regarding telephone records requests for which Company B still had not received legal process.[200] Based on our review of that material, we determined that the CAU obtained after-the-fact legal process for only approximately 25 percent of the requests that were pending from January 2005 to September 2005, and for approximately 30 percent of the requests for process that were pending from September 2005 through April 2006. The Company B employee's spreadsheets also showed that the number of telephone numbers that had been [redacted] and that required after-the-fact legal process declined considerably between September 2005 and April 2006.

The spreadsheets prepared by the on-site Company C employee also showed that the CAU had similar rates of obtaining after-the-fact legal process for requests previously made to Company C, and also illustrated a decrease over time in the number of telephone record requests requiring after-the-fact legal process.

---

[200] Company A did not provide similar information to the CAU, and we were therefore unable to determine how many telephone numbers Company A had [redacted] without legal process or how often CAU personnel were able to obtain after-the-fact legal process for its previous record requests to Company A from 2003 to mid-2006.

We also determined that ITOS-I management learned sometime in 2006 that the CAU needed NSLs to cover the information previously given to the FBI by the on-site providers. Michael Heimbach, an Assistant Section Chief for ITOS-I from February 2003 to March 2004 and a Section Chief for ITOS-I from March 2005 to January 2007, told us that he first became aware of a backlog of NSLs in the latter part of 2006. He said he learned at that time that the CAU needed ITOS to issue NSLs for over 100 telephone numbers. Heimbach told us that he assigned personnel in ITOS "to figure this out . . . we got to get it right. We have to fix whatever is wrong."

We found that between February and May 2006, a CAU SSA informed an ITOS-I Assistant Section Chief that there was a backlog of NSLs which ITOS-I "owed" for records acquired in exigent circumstances. When the Assistant Section Chief briefed Heimbach, Heimbach assigned her to oversee the response of ITOS-I to the issue of the CAU's backlog. She told us that she convened two meetings with her Unit Chiefs and a CAU SSA who had the list of telephone numbers that required NSLs, and she instructed the Unit Chiefs to work with the pertinent field divisions to ensure that NSLs were issued. However, as described below, the backlog was addressed in another manner beginning in May 2006 when the CAU SSA drafted and CTD Deputy Assistant Director (DAD) Billy signed a blanket NSL to cover the outstanding Company B record requests.

J. OIG Analysis of FBI Attempts at Corrective Actions From 2003 through October 2006

In sum, as described above and further discussed in Chapter Five of this report, we found that the FBI repeatedly failed to take steps to ensure that the CAU complied with the ECPA when obtaining subscriber and toll billing records information from the on-site communications service providers.

When Glenn Rogers became CAU Unit Chief in 2003, he learned about and used an exigent letter provided by the Company A analyst. He said he relied on the Company A analyst's representation that the letter had been approved by FBI and Company A attorneys. However, Rogers did not seek any guidance about the use of these letters or confirm with FBI OGC attorneys that they were appropriate. Also, we believe Rogers failed to take appropriate steps to ensure that timely legal process was obtained as promised after exigent letter requests were made. This failure resulted in the development of a significant backlog of records requests for which there was no legal process. From the beginning of his tenure as CAU Unit Chief in 2003 until just prior to his promotion to CTD Assistant Section Chief in November 2004, Rogers also failed to develop or implement any system for tracking FBI requests for records or other information from the on-site providers.

We concluded that after Bassem Youssef became the CAU Unit Chief in November 2004, he took some steps to address the backlog of requests for legal process from the on-site providers relating to exigent letters. However, Youssef terminated the CAU's Tracker Database in February 2005 after complaints from CAU staff that the system was "cumbersome." Youssef said that at the time he terminated use of the database, he did not know that the CAU was obtaining records prior to service of legal process. However, even after the time he acknowledged learning about the Company B backlog he did not implement a process to maintain an accurate record at the time they were made of the nature, number, and origin of the requests to the on-site providers whether communicated by exigent letter, by telephone, by e-mail, on pieces of paper, or through sneak peeks. The failure to maintain such records was an internal control problem that greatly complicated the FBI's later efforts to determine whether it had a basis to retain the records.

In addition, contrary to his suggestion, Youssef was not the first FBI official to raise the issue of exigent letters to NSLB attorneys. We found that NSLB attorneys, including Thomas, learned about the exigent letters practice in December 2004. Further, we found that when Youssef first spoke with the Assistant General Counsel on March 11, 2005, about streamlining the NSL process, the Assistant General Counsel already was aware that the CAU was obtaining records pursuant to exigent letters prior to service of legal process. In fact, Youssef told us that he did not learn that exigent letters were used by the CAU to obtain records from the on-site providers, or that there was a significant backlog of promised legal process, until some time after this meeting.[201]

We concluded that several factors contributed to the FBI's failure to timely and effectively address the use of exigent letters. First, CAU Unit Chief Rogers and his CTD supervisors approved the use of exigent letters without first consulting FBI attorneys.

---

[201] After reviewing a draft of this report, Youssef's attorney stated that at the March 11, 2005, meeting, Youssef was the first to tell the Assistant General Counsel that the CAU's receipt of records without legal process was wrong but that the Assistant General Counsel did not provide him with any guidance or instruction to address the problem. As we describe in this chapter, however, the Assistant General Counsel was already aware of and concerned about the exigent letter problem before she met with Youssef, had already made suggestions to her supervisors about the need for opening preliminary investigations to support issuance of NSLs, and after the March 11 meeting provided guidance and instruction to Youssef as she learned more about the exigent letter practice and attempted to address it.

Second, the CAU failed to maintain an accurate record at the time they were made of the nature, number, and origin of the requests to the on-site providers whether communicated by exigent letter, by telephone, by e-mail, on pieces of paper, or through sneak peeks.

Third, the CAU received a steady stream of requests, often in major threat situations, from senior headquarters officials and field personnel, who expected – and came to rely upon – prompt responses. As a result, using exigent letters and other informal requests, the CAU quickly developed a backlog of record requests for which it had obtained records but not provided the promised legal process.

Fourth, all three on-site providers accepted exigent letters and other informal requests as a basis for providing subscriber and toll billing records information, and other calling activity information covered by the ECPA.

Fifth, we found that senior CTD managers assumed that its operational units were acquiring information from the on-site communications service providers through the CAU by lawful means. It was not until early 2006 that a CTD ITOS Assistant Section Chief learned about the backlog of promised legal process from the CAU and directed her Unit Chiefs to address the problem by obtaining the approval ECs and after-the-fact NSLs from the pertinent field divisions.

Sixth, we determined that when NSLB attorneys learned about the CAU's acquisition of records without legal process, including the use of exigent letters, they did not stop the practice or at a minimum ensure that CAU personnel were trained on the methods by which the FBI is authorized to obtain telephone toll billing records and subscriber information in various types of investigations. Instead, the attorneys themselves became involved in issuing after-the-fact NSLs to cover records previously obtained through the use of exigent letters. Further, while the NSLB made resources available to the CAU regarding the use of NSLs, NSLB attorneys did not believe that they could assist the CAU until umbrella files (preliminary investigations from which the NSLs could be issued) were implemented. However, the initiative to create umbrella files languished for nearly 9 months and ultimately was rejected, and the designated NSLB attorneys did not receive requests for assistance from the CAU.

Although NSLB attorneys were aware that the CAU was still obtaining records without legal process, they failed to terminate the exigent letters practice. Rather, the NSLB allowed the CAU's use of exigent letters in what they believed were emergency situations, and focused on the umbrella file proposal as a way to link telephone numbers listed in exigent letters and after-the-fact legal processes to open national security investigations.

Seventh, the NSLB provided advice to the CAU about the use of the exigent letters that was inconsistent with the ECPA NSL statute. In April 2005, the Assistant General Counsel sent an e-mail to Youssef in which she advised that exigent letters should be used by the CAU "only if it is clear . . . that the requester cannot await an NSL." This advice was inaccurate because the ECPA does not authorize the FBI to obtain toll billing records from communications service providers unless it first serves compulsory legal process such as an NSL or the provider makes a voluntary production pursuant to Section 2702's emergency disclosure provision. Even if the letter were interpreted as seeking voluntary production, the advice that the letter could be used "when there really are exigent circumstances . . . only if it is clear. . . that the requester cannot await an NSL" would allow use in circumstances that did not meet Section 2702's standard. The NSLB's erroneous advice was forwarded by Youssef to all CAU personnel. Neither the Assistant General Counsel's immediate supervisor nor NSLB Deputy General Counsel Thomas – who were both informed that Youssef was circulating the e-mail containing her advice to the entire unit – corrected this inaccurate advice.

K. FBI Issues 11 Improper Blanket NSLs in May to October 2006

This section of our report describes the FBI's ineffective attempts at corrective action from May through October 2006, regarding the exigent letter practice and the backlog of record requests for which the FBI had not yet served legal process. During this period, the NSLB reaffirmed its flawed approval of the use exigent letters with the promise of future legal process. In addition, the FBI issued 11 improper blanket NSLs prepared by CAU personnel and signed by senior CTD officials to "cover" the records it had previously received through exigent letters and other informal requests.

1. Youssef Proposes Policy and Procedures for Service of NSLs

On May 10, 2006, Youssef e-mailed the CAU's draft of a guidance EC containing proposed procedures for the CAU's use in obtaining records from the on-site communications service providers to an FBI OGC attorney for review. The draft guidance stated that in exigent circumstances the CAU could obtain records from the on-site providers using exigent letters and then issue after-the-fact NSLs. The draft stated specifically that the CAU would issue exigent letters "in crisis situations where there is a specific

threat to the United States or its allies, both domestically or overseas, and loss of life and property are imminent."[202]

On May 18, 2006, Youssef forwarded the draft EC to NSLB Deputy General Counsel Thomas. On May 19, 2006, the Assistant General Counsel reviewed the draft EC and recommended minor changes. These changes were incorporated into a draft EC dated May 19, 2006, but this draft was never finalized or distributed. However, in May 2006 this OIG review became known within the FBI, and the number of exigent letters issued dropped significantly thereafter.

2. NSLB Revises Model for Exigent Letters but Approves Their Continued Use

On May 19, 2006, in connection with her review of the draft EC, the Assistant General Counsel asked a CAU SSA to send her copies of the exigent letters that were being issued by the CAU. The SSA sent copies of exigent letters, one for each provider, to the Assistant General Counsel that day by e-mail.[203] This was the first time she or any attorneys in the FBI OGC had reviewed the text of an exigent letter.

On May 26, 2006, the Assistant General Counsel responded to the CAU SSA by sending him revised model exigent letters, stating the new letters should be used "[p]ronto." She revised the exigent letters to state that NSLs, rather than grand jury subpoenas, would be forthcoming. The SSA e-mailed the revised exigent letters to all CAU personnel. The Assistant

---

[202] After reviewing a draft of this report, Youssef's attorney stated that this draft guidance set forth the "proper definition of 'exigent circumstances'" and, if adopted, would have brought the exigent letter practice into compliance with the law. We found that the draft guidance's reference to imminent loss of life was much closer to the standard set forth in Section 2702(c)(4)'s emergency voluntary disclosure provision than the Assistant General Counsel's earlier guidance and we believe it likely would have resulted in a further decrease in the use of exigent letters if adopted. However, the draft also described procedures that would have continued the flawed practice of promising compulsory legal process to obtain the records through exigent letters.

[203] In the May 19, 2006, e-mail from the Assistant General Counsel to the SSA, which copied Youssef, the Assistant General Counsel stated that she was not sure that she had ever seen an exigent letter and asked to see one. Later that day the SSA forwarded to her copies of exigent letters, one for each of the three on-site providers, again copying Youssef. The SSA who sent the letters to the Assistant General Counsel told us that he could not recall whether he e-mailed the letters in response to her request or at Youssef's direction. Youssef asserted to us that he had asked a CAU SSA to send an exigent letter to the Assistant General Counsel for review in April or May 2006. The e-mail from the CAU SSA to the Assistant General Counsel did not indicate that Youssef or anyone else in the CAU was concerned about its contents.

General Counsel told us that her intent was to make sure that if the CAU was "going to use exigent letters at all, this [the revised letter] is the document [they] need to use."[204]

On June 15, 2006, the Assistant General Counsel forwarded a copy of the revised exigent letter to Thomas, her immediate supervisor and other FBI OGC attorneys, and she informed them that she had drafted similar exigent letters for each of the on-site providers. The e-mail stated that she had changed the letter that the CAU had been using, which referred to a grand jury subpoena and not an NSL.

Thomas did not object to the revised exigent letter. She told us that she did not recall receiving the e-mail and that she had no recollection of the e-mail.

3. Three Blanket NSLs (May, July, and September 2006)

On May 17, 2006, the OIG interviewed the Assistant General Counsel in connection with our first NSL review. During the interview, she told us about the CAU's use of exigent letters. This was the first time we questioned her, or anyone else in the FBI, about exigent letters.

Following the interview that same day, the Assistant General Counsel sent an e-mail to Youssef with copies to other CTD and NSLB personnel. The e-mail stated that the Assistant General Counsel had discussed with the OIG the difficulty that the CAU had experienced in obtaining prompt issuance of NSLs to the on-site communications service providers after receipt of records. She wrote that she had represented to the OIG, "as you have represented to me, that the problem appears to be resolved" and that the operational units were issuing the NSLs.

Youssef acknowledged receipt of the e-mail the following day, May 18, writing, "thank you for volunteering our names." He added in the e-mail that he was only kidding and that "an [OIG] interview would be welcome at any time."

---

[204] Like the original exigent letter, the revised model exigent letter promised future legal process, which we concluded circumvented the ECPA's requirements that either (1) the FBI issue legal process in advance of obtaining records, or (2) the provider produce records voluntarily in circumstances satisfying Section 2702's emergency voluntary disclosure provision.

On May 18, shortly after Youssef sent his response to the Assistant General Counsel's e-mail regarding her interview with the OIG, a CAU SSA asked the on-site Company B and Company C employees to send him lists of records requests for which legal process had not been provided. Both providers responded that day with lists of records requests for which they had not received legal process. Youssef told us that because the Assistant General Counsel had informed him about the OIG investigation, he may have asked about the efforts to address the backlog and that may have prompted the May 18, 2006, e-mails from the Company B and Company C on-site employees attaching the lists of telephone numbers.

As described below, the telephone numbers the providers identified were subsequently incorporated into blanket NSLs the FBI issued to Company B and Company C to "cover" or "validate" [redacted] or records provided to the CAU for which the providers had not received NSLs or other legal process. Additionally, in July and September 2006, Company A provided to the CAU lists of record requests that still required legal process, and in September 2006 the FBI issued another blanket NSL to Company A to cover its outstanding requests for legal process.

However, as summarized in Table 4.1 and detailed more fully in the following sections, these three blanket NSLs issued to the on-site communications service providers were deficient. The ECPA does not authorize the FBI to issue retroactive legal process for ECPA-protected records. Moreover, using blanket NSLs to "cover" the previously obtained records would not cure any prior violations of the ECPA that occurred when the FBI sought and received records without prior legal process and in the absence of a qualifying emergency. In addition, all three of these blanket NSLs were used to cover many telephone numbers not relevant to national security investigations (which include counterterrorism and espionage investigations), did not contain the required certifications regarding non-disclosure, and did not state that they related to records that had already been provided to the FBI.

TABLE 4.1

Three Blanket NSLs Issued by the CTD in 2006

	NSL Date	Recipient	Signer	Number of Telephone Numbers	Used to Cover Records on Telephone Numbers Not Relevant to National Security Investigations	No approval EC	No reference to records already [redacted]/obtained	No certification re: non-disclosure
1	05/12/06	Company B	DAD Billy	192	48	√	√	√
2	07/05/06	Company C	A/DAD Heimbach	35	7	√	√	√
3	09/21/06	Company A	A/DAD Love	700	120 (approx.)	√	√	√

a. Company B May 12 NSL

The first blanket NSL that addressed the backlog of records requests, dated May 12, 2006, was issued to Company B around May 23, 2006.[205] It was signed by Joseph Billy, Jr., then a CTD Deputy Assistant Director (DAD).[206] The blanket NSL contained as an attachment the list supplied by the on-site Company B employee on May 18, 2006, of 192 telephone numbers. The on-site Company B employee told us that those were all the telephone numbers for which Company B needed legal process at that time. The list included numbers that CAU personnel had asked Company B to [redacted] during the period September 2004 to April 2006 pursuant to exigent letters (some of which had been provided after the [redacted]).

The CAU SSA who drafted the Company B May 12 NSL said that it was his idea to create the blanket NSL. He said the on-site communications service providers' employees were complaining to him and others on his team that they were owed NSLs for a lot of numbers they had previously [redacted] at the FBI's request. The SSA told us that his idea was to draft

---

[205] We refer to this NSL as the Company B May 12 NSL which was the date on the NSL, even though it was not signed until after May 23, 2006.

[206] Billy became the Assistant Director of the CTD on October 15, 2006, and remained in that position until his retirement from the FBI in March 2008.

one NSL for then-DAD Billy's signature. The SSA told us that he discussed his idea with Youssef and that Youssef agreed with the proposal. The SSA also stated that when Youssef agreed with the concept, he appeared "quite giddy about getting the books cleared up."

Youssef also said to us that this SSA proposed to him the idea of the Company B May 12 NSL. Youssef stated that the SSA told him he had discussed the issue of obtaining individual after-the-fact NSLs with the CTD operational unit and had been told that it would "take forever" to get the NSLs. Youssef added that the SSA told him that if all the telephone numbers were put in one NSL, Billy would sign it. Youssef said to us that at first he resisted the idea because he did not want to create a precedent of having the CAU draft NSLs, since that was the operational unit's job. However, he said that the SSA suggested that they draft the NSL "to be cooperative," and therefore Youssef agreed. Youssef also stated that within a few weeks or maybe a month or two from that conversation the SSA informed Youssef that the NSL had been signed.

The SSA told us that he used as a model for the blanket NSL, a copy of an NSL provided by a CAU Intelligence Analyst on his team. He said the process of drafting the NSL and getting it signed took about 2 weeks. The SSA later learned that the NSL that he used as a model was outdated and did not contain the certification required by the *USA PATRIOT Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act) concerning imposition of non-disclosure and confidentiality requirements on NSL recipients.[207]

The Company B May 12 NSL also was not accompanied by any approval EC. An approval EC is the document routinely generated by FBI agents seeking approval to issue NSLs. FBI policy requires approval ECs to describe the underlying national security investigation to which the NSL relates and, in the case of NSLs seeking telephone records, the relevance of the telephone number to that investigation. The SSA told us that he did not prepare or ask others to prepare an approval EC for the Company B May 12 NSL because he did not think it was necessary. Youssef also told us that

---

[207] Section 116 of the *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109-177, 120 Stat. 192 (2006) states that if the FBI seeks to impose non-disclosure and confidentiality obligations on NSL recipients, the FBI Director or his designee must 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.

when the NSL was drafted he was unaware that an approval EC was necessary.

The CAU SSA who drafted the Company B May 12 NSL told us he did not discuss it with any FBI OGC attorney. He said he also did not know there was an NSLB attorney who would draft an NSL for him. Neither Youssef, who was aware of the NSLB's outstanding offer of assistance, nor anyone else in the CAU or CTD notified the FBI OGC about the blanket NSL.

Billy acknowledged to us that his signature appeared on the Company B May 12 NSL. However, he said he did not recall signing the NSL, did not know the SSA who prepared the document, and did not recall ever meeting him. Billy stated that over the course of his FBI career he had signed hundreds of NSLs. He also said that his normal practice was to rely on an approval EC to adequately describe the predication for the requested records. In response to our questioning, Billy said he did not rule out the possibility that over the course of his FBI career he had signed an NSL without an approval EC, but he stated that such a case would be an exception and that he believed he would have received sufficient facts to ensure that the NSL was properly predicated. Billy also said that he knew that NSLs were authorized only in instances in which there was an open preliminary or full national security investigation and that the requested records had to relate to that open investigation.

We found several defects with this NSL. First, this NSL was served after-the-fact. As noted previously, there is no provision in the ECPA authorizing the issuance of retroactive legal process.

Second, this NSL was defective under the ECPA because 39 of the 192 telephone numbers included in the Company B May 12 NSL were relevant to FBI domestic terrorism investigations, and 5 related to FBI criminal investigations. However, the ECPA and the Attorney General's NSI Guidelines authorize the use of NSLs only in international terrorism or espionage investigations. Therefore, the use of this NSL to cover previously obtained records for telephone numbers relevant to domestic terrorism and criminal investigations violated the ECPA NSL statute, the Attorney General's NSI Guidelines, and FBI policy.

Third, the NSL did not contain the certification required by the Patriot Reauthorization Act and the ECPA for NSLs imposing non-disclosure and confidentiality obligations on the recipient.

Fourth, this NSL also failed to comply with FBI policy requiring that it be accompanied by an approval EC establishing the predication for the request and the relevance of the telephone records sought to an authorized

national security investigation. The FBI also relies on approval ECs to generate required reports to Congress on NSL usage.

Finally, the NSL did not disclose that the FBI had previously asked Company B to [redacted] these records or that Company B had done so and had provided responsive records.

b. Company C July 5 NSL

A second blanket NSL, dated July 5, 2006, was issued by the CTD to Company C.[208] This NSL was prepared by the same CAU SSA who prepared the Company B May 12 NSL.

As described above, on May 18, 2006, the Company C employee sent to a CAU SSA a list of telephone numbers for which Company C had previously delivered records to the FBI without legal process. This list contained 70 unique telephone numbers. The SSA who drafted the Company C July 5 NSL requested that the Company C employee omit from this list telephone numbers related to any criminal investigations. In response, the Company C employee gave the SSA an amended list on July 5, 2006, that excluded telephone numbers associated with criminal and counterintelligence investigations. The amended list consisted of 35 telephone numbers for which CAU personnel had asked Company C to provide records from September 2004 to April 2006. The SSA attached the amended list to the Company C July 5 NSL.

Michael Heimbach, then a Section Chief for the ITOS-I of the CTD, signed the July 5 blanket NSL. At the time he was temporarily assigned as an Acting Deputy Assistant Director (Acting DAD) of the CTD.[209] Heimbach signed the NSL as Acting DAD. At the time Heimbach signed this NSL, the FBI had not issued guidance on whether FBI personnel serving as Acting DADs were authorized to sign NSLs. The FBI OGC later issued guidance on June 1, 2007, stating that Acting Deputy Assistant Directors are not authorized to sign NSLs.[210] However, on January 16, 2009, the Department's Office of Legal Counsel (OLC), in response to a request for a legal opinion by the FBI General Counsel Caproni, opined that Acting DADs

---

[208] We refer to this as the Company C July 5 NSL.

[209] In January 2007, Heimbach became a SAC in the FBI's Washington Field Office. Since April 2008 Heimbach has been the CTD Assistant Director.

[210] Because the FBI did not formalize this guidance until June 2007, the FBI Office of Professional Responsibility (FBI OPR) decided to take no disciplinary action against any Acting Deputy Assistant Director who signed NSLs without authorization.

(and certain other acting officials) are authorized to sign NSLs under three of the NSL statutes, including the ECPA NSL statute, 18 U.S.C. § 2709. Caproni notified the OIG in March 2009 that the FBI is revising its June 1, 2007, guidance in light of the OLC opinion.

On July 5, 2006, the SSA who prepared the NSL sent an e-mail to the Company C employee stating, "I have the signed NSL cleaning up all the past #'s requested for Company C." Youssef, who was copied on the e-mail, responded to the SSA, "this is good." On July 7, 2006, the Company C employee acknowledged receiving the NSL in an e-mail that he sent to the SSA and Youssef.

Youssef told us that he did not recall knowing at the time that the SSA drafted the July 5 Company C NSL, but that it did not surprise him. Youssef said he had discussed other blanket NSLs with the SSA for two major operations. He also stated that he could not recall what was in his mind when he wrote in his July 5, 2006, e-mail to the SSA, "[t]his is good," in response to being informed that the Company C July 5 NSL had been signed.

Heimbach told us that he signed the NSL but could not recall how the NSL came to him, who brought it to him, and to whom he returned it. Heimbach said that an NSLB attorney, whose name he could not recall, had assured him that he was authorized to sign the NSL as an Acting DAD. However, he stated that he did recall contacting any NSLB attorney prior to signing the NSL to ensure that he was authorized to sign as an Acting CTD DAD.[211] Heimbach told us that he learned sometime after he signed the Company C July 5 NSL that he was not authorized to sign NSLs as an Acting DAD.[212] The SSA also told us that sometime after Heimbach signed the NSL, Heimbach mentioned at a section meeting that he had learned that he was not authorized to sign NSLs and advised CXS personnel that NSLs should not be brought to him for signature.

The Company C July 5 NSL was not accompanied by an approval EC. Heimbach told us his practice was that he would not sign an NSL without an accompanying EC establishing and documenting the predication for the

---

[211] The SSA who prepared the NSL told us that he asked Heimbach to sign the NSL and that Heimbach immediately signed it with no discussion.

[212] An NSLB attorney told us that she believes that in early August 2006 Heimbach asked her whether another CTD Acting DAD, Arthur Cummings, II, was authorized to sign NSLs. This attorney said she told Heimbach that Acting DADs were not authorized to sign NSLs.

NSL and the relevance of the telephone numbers to an open national security investigation. Heimbach said that he assumed he was told when he signed this NSL that the approval EC was being prepared or had already been prepared.

As was the case with the Company B May 12 NSL, no CAU or CTD personnel sought legal guidance from any FBI OGC attorney regarding the content of the Company C July 5 NSL.

We found several defects with this NSL. First, as was the case with the Company B May 12 NSL, the NSL was served after-the-fact, which is not authorized by the ECPA. Second, the NSL included seven telephone numbers relevant to domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA NSL statute or the Attorney General's NSI Guidelines. Third, although the NSL imposed a non-disclosure and confidentiality obligation on Company C, the NSL did not contain the certification required by the Patriot Reauthorization Act and the ECPA for such NSLs. Fourth, the NSL was not accompanied by the required approval EC establishing the predication for the request and the relevance of the records sought to an authorized national security investigation.

Finally, the NSL did not disclose that the FBI had previously asked Company C to [redacted] these records or that Company C had already done so and had provided responsive records.

c. Company A September 21 NSL

The third blanket NSL, dated September 21, 2006, was issued to Company A.[213] It was prepared by the CAU's Primary Relief Supervisor.[214] The NSL listed 700 telephone numbers that CAU personnel had asked Company A to [redacted] between May 2003 and January 2006. Some of these numbers were provided in response to exigent letters, and some of the exigent letters had been issued after the [redacted].[215]

---

[213] We refer to this as the Company A September 21 NSL.

[214] We call this SSA the Primary Relief Supervisor because Youssef referred to him in this capacity in his annual performance evaluations.

[215] The telephone numbers listed on this NSL were relevant to various FBI investigations, including international terrorism investigations. However, others related to domestic terrorism investigations and criminal investigations such as fugitive cases, alien smuggling, securities fraud, arson, illegal narcotics, and bank robbery.

The Primary Relief Supervisor stated that Youssef had assigned him to work with Company A on the outstanding telephone numbers. He said that he worked directly with the Company A analysts to obtain a spreadsheet of numbers for which legal process was outstanding, and he also sought guidance from the SSA who had drafted the Company B May 12 NSL.

On July 28, 2006, a Company A analyst sent a preliminary list of 213 telephone numbers to the Primary Relief Supervisor. The Company A analyst took approximately 3 months to compile the final comprehensive list, which identified 700 telephone numbers. The Primary Relief Supervisor then drafted the Company A September 21 NSL and attached the list of 700 numbers. He said that in drafting the NSL he likely used a "pony" (or model NSL) given to him by the SSA who had drafted the Company B May 12 NSL.

Youssef told us that he was not aware at the time that the Company A September 21 NSL had been issued, and that he learned about it later in connection with the OIG investigation.

This NSL was not accompanied by an approval EC, which is required by FBI policy to document that the requested records are relevant to an authorized national security investigation. The Primary Relief Supervisor told us that he did not know that an approval EC was required for an NSL.

The NSL was signed by Jennifer Smith Love, who was then a CXS Section Chief, temporarily assigned to serve as an Acting CTD DAD.[216] Love told us that she recognized her signature on the Company A September 21 NSL but could not recall any details surrounding this NSL, including who gave it to her. Love told us that at the time she signed the NSL she was unaware that an approval EC was required.

Like the Company B May 12 and Company C July 5 NSLs, the Company A September 21 NSL was defective in several respects. First, the Company A September 21 NSL was served after-the-fact. Second, the NSL included 134 telephone numbers that were relevant to criminal and domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA NSL statute or the Attorney General's NSI

---

[216] In December 2006, Love was promoted to be a Special Agent in Charge in the FBI's Washington Field Office. In June 2008 Love became the SAC of the FBI's Richmond Field Division.

Guidelines. Third, although the NSL imposed a non-disclosure and confidentiality obligation on Company A, the NSL did not contain the certification required by the Patriot Reauthorization Act and the ECPA for such NSLs. Fourth, the NSL was not accompanied by the required approval EC establishing the predication for the request and the relevance of the records sought to an authorized national security investigation.

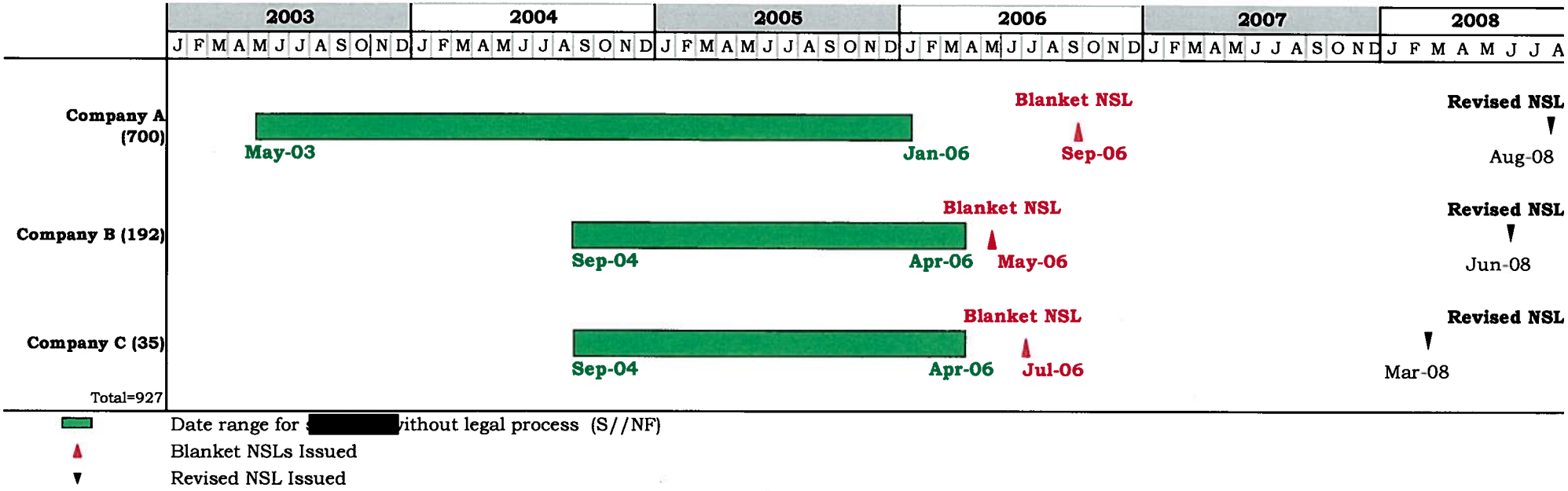
Finally, the NSL did not disclose that the FBI had previously asked Company A to [redacted] these records or that Company A had already done so and in many instances had provided responsive records.

d. Timeline Regarding Three Improper Blanket NSLs

Diagram 4.1 (next page) illustrates the timeline of the three blanket NSLs just described, including the time period in which records were initially [redacted] without legal process pursuant to exigent letters or other informal requests, the dates of the blanket NSLs issued to cover these requests, and the date of three correcting NSLs (described later in this chapter) issued by the FBI to address the records identified in the three improper blanket NSLs.

DIAGRAM 4.1

Timeline of Requests Made and [redacted] by the Three On-Site Communications Service Providers Addressed by Three Blanket NSLs, and Subsequent Corrective Actions



4. Eight Additional Blanket NSLs in 2006

We determined that CAU personnel drafted and CTD senior officials signed eight additional improper blanket NSLs between August and October 2006 related to major FBI operations. Together, these eight blanket NSLs were issued to cover the FBI's previous requests to the communications service providers without accompanying NSLs for [redacted] on calling records and other information on over 1,500 telephone numbers.

All of these eight NSLs were served after-the-fact, although the ECPA does not authorize retroactive legal process. Five of the NSLs also failed to comply with the ECPA certification requirement for NSLs imposing non-disclosure and confidentiality obligations on the recipients. The eight NSLs also were issued without approval ECs in violation of FBI policy and failed to disclose that the FBI had already acquired the records. The additional deficiencies in these eight blanket NSLs are summarized in Table 4.2 and described in more detail in this section.

TABLE 4.2

Eight Blanket NSLs Issued by the CTD in Connection with FBI Operations Y and Z

	Date	Recipient	Signer	Number of Telephone Numbers	No approval EC or legal review	No reference to records already [redacted]/obtained	No certification re: non-disclosure	Date of Revised NSL	Date of corrective approval EC
1	08/24/06	Company B	A/DAD Cummings*	72	√	√	√	5/04/07	5/04/07
2	08/24/06	Company C	A/DAD Cummings*	610	√	√	√	3/07/08	3/07/08
3	08/25/06	Company A	A/DAD Cummings*	735	√	√	√	3/07/08	3/07/08
4	09/19/06	Company A	A/DAD Cummings*	107	√	√	√	5/04/07	5/04/07
5	09/19/06	Company C	A/DAD Cummings*	73	√	√	√	5/04/07	5/04/07

	Date	Recipient	Signer	Number of Telephone Numbers	No approval EC or legal review	No reference to records already [redacted]/obtained	No certification re: non-disclosure	Date of Revised NSL	Date of corrective approval EC
6	10/20/06	Company A	Assistant Director Billy	445	√	√		None required per FBI OGC	4/13/07
7	10/20/06	Company B	Assistant Director Billy	445	√	√		None required per FBI OGC	4/13/07
8	10/20/06	Company C	Assistant Director Billy	445	√	√		None required per FBI OGC	4/13/07

*Cummings signed the NSLs as SAC.
Yellow = Operation "Y" blanket NSLs Turquoise = Operation "Z" blanket NSLs

a. Five Blanket NSLs in Connection with Operation "Y"

The CAU SSA who drafted the Company B May 12 and Company C July 5 blanket NSLs also drafted five other blanket NSLs in August and September 2006. All five of these additional blanket NSLs listed telephone numbers related to a major FBI counterterrorism operation that was initiated in [redacted] which we refer to as Operation Y.[217]

We were told that CAU employees told the three on-site communications service providers when Operation Y first began that the FBI was undertaking a significant operation that would generate many requests for [redacted] of telephone records, and that after-the-fact NSLs listing multiple telephone numbers would be prepared to cover the requests for these records. Youssef told us that he could not recall whether he or someone else from the CAU informed the providers about the anticipated requests for Operation Y. He told us that the plan was for the Headquarters operational unit to prepare after-the-fact NSLs. We determined that, with few exceptions, records requests relating to this operation were

[217] The name of this operation is classified.

communicated to the on-site communications service providers by informal means other than exigent letters, such as by e-mail.

Operation Y was an investigation of a terrorist plot [redacted] to detonate explosives [redacted] CAU personnel made requests for telephone records related to this investigation for a 6-week period. The Company B on-site employee told us that he was informed by CAU personnel that Operation Y involved "something big going on . . . and it could be another 9/11."

One Company A analyst told us that he received no briefing from the CAU concerning Operation Y, and a second Company A analyst told us he had [redacted] for the FBI for this case for several weeks without even being aware that the [redacted] he was conducting were associated to Operation Y.

Arthur A. Cummings III, then a SAC in the FBI's Washington Field Office but temporarily assigned as an Acting Deputy Assistant Director (DAD) in the CTD, signed the following five blanket NSLs relating to Operation Y, none of which had approval ECs:

- August 24, 2006, NSL to Company B listing 72 telephone numbers (Company B August 24 NSL);
- August 24, 2006, NSL to Company C listing 610 telephone numbers (Company C August 24 NSL);
- August 25, 2006, NSL to Company A listing 735 telephone numbers (Company A August 25 NSL);
- September 19, 2006, NSL to Company A listing 107 telephone numbers (Company A September 19 NSL); and
- September 19, 2006, NSL to Company C listing 73 telephone numbers (Company C September 19 NSL).

As a SAC in the Washington Field Office, Cummings was authorized to sign NSLs.[218] Cummings acknowledged that the NSLs contained his signature and said that he specifically recalled signing the Company C August 24 and Company A August 25 NSLs because they included many telephone numbers. He said that he had no specific recollection of signing

---

[218] In November 2006, Cummings became a DAD in the CTD, and in January 2008 became the Executive Assistant Director for the FBI's National Security Branch.

any of the other three blanket NSLs. Cummings said that he believed that each of the NSLs had approval ECs because it was his practice to ensure that NSLs always had approval ECs.

Cummings told us that prior to signing any NSLs while assigned as an Acting DAD he asked an NSLB attorney whether he was authorized to sign NSLs in that capacity. He stated that the NSLB attorney told him that although he was not authorized to sign NSLs as an Acting DAD, since he was "formally" a SAC at the time he was authorized to sign NSLs in his capacity as a SAC.[219] Cummings stated that other than signing NSLs, he performed no other duties as a SAC while temporarily assigned as an Acting DAD for the CTD.

The NSLB attorney with whom Cummings consulted confirmed that based on direction from her NSLB Unit Chief, she had advised Cummings that he was authorized to sign NSLs as a SAC.[220]

We determined that all five Operation Y NSLs were defective. First, the NSLs were served after-the-fact. Second, although the NSLs imposed non-disclosure and confidentiality obligations on Company A, the NSLs did not contain the certifications required by the Patriot Reauthorization Act and the ECPA for such NSLs. Third, the NSLs were not accompanied by approval ECs establishing the predication for the requests and the relevance of the records sought to authorized national security investigations.

Finally, the NSLs also did not disclose that the FBI had previously asked the providers to [redacted] these records or that the providers had already done so and in many instances had provided responsive records.

---

[219] As noted above, at the time the FBI had no written guidance on the authority of acting FBI officials to sign NSLs.

[220] NSLB Deputy General Counsel Thomas told us she was not sure whether this advice was correct. She stated, "the issue would be if you are an Acting DAD, then you have left the current [SAC] position." She added that her advice would have been to have the NSLs sent to her instead of having Cummings sign them because, "we do not need to go down that legal road." As noted previously, the FBI OGC issued guidance on June 1, 2007, stating that Acting Deputy Assistant Directors are not authorized to sign NSLs. However, on January 16, 2009, the Department's Office of Legal Counsel opined that Acting DADs are authorized to sign NSLs under three of the NSL statutes, including the ECPA NSL statute.

b. Three Blanket NSLs in Connection With Operation "Z"

The FBI issued three more blanket NSLs in October 2006, one to each of the three on-site communications service providers, in connection with a different major FBI counterterrorism investigation, which we refer to as Operation Z.[221]

In connection with Operation Z, the CAU was provided telephone numbers recovered [redacted]. Youssef advised CAU personnel of the investigation by e-mail on [redacted] stating that "[w]e anticipate numerous requests for telephone exploitation and I want us to be ready." He also asked for a CAU "volunteer to head this project." Four days later, on [redacted] the CAU began asking the on-site providers to provide records for groups of telephone numbers related to this operation.

The CAU Primary Relief Supervisor told us that at Youssef's direction he issued three exigent letters dated [redacted] one to each of the three on-site providers. These exigent letters listed telephone numbers relating to Operation Z. The exigent letters, which were sent to the three on-site providers by e-mail, each contained an attachment listing the same 48 telephone numbers. From [redacted] through October 20, 2006, the CAU asked for, and in many instances received, toll billing and other records on 397 additional telephone numbers relating to this operation. Almost all of these [redacted] were requested without exigent letters.

Youssef stated that he did not recall directing the Primary Relief Supervisor to issue exigent letters at the start of Operation Z, but that he would not be surprised if exigent letters had been issued because that was how the CAU regularly operated. Youssef said that he was not aware that only one exigent letter was issued to each provider, with [redacted] on additional telephone numbers later requested without even exigent letters.

A CAU Intelligence Analyst who worked on Operation Z told us that she volunteered to be the coordinator of telephone analysis requests that the CAU would receive in connection with this operation. She maintained a contemporaneous log of the telephone numbers that the CAU gave to the

---

[221] The name of this operation is classified.

three on-site providers to [redacted] in connection with this operation. She said that in late October 2006, the Primary Relief Supervisor directed her to compile a list of all telephone numbers that had been [redacted] Using her log, the Intelligence Analyst prepared a list of 445 telephone numbers and gave it to the Primary Relief Supervisor.

The Primary Relief Supervisor then prepared a blanket NSL for each of the three on-site providers, attaching the list of 445 telephone numbers to each NSL. He said that he gave the NSLs to Youssef or Youssef's immediate supervisor for Billy to sign, and that the NSLs were signed on or around October 20, 2006.

Billy confirmed his signature was on all three NSLs, although he said he could not recall signing them. He said he recalled the case and that NSLs were issued. He also told us that signing NSLs without approval ECs was "completely outside" his practice.

Youssef told us that he was not involved with the Operation Z NSLs. He said that the Primary Relief Supervisor was the CAU point of contact with the CTD operational unit for Operation Z. Youssef also said that he did not recall that the Primary Relief Supervisor had drafted the three blanket NSLs for Operation Z and said he also did not recall whether he had provided the NSLs to Billy for signature. Youssef told us that he recalled one instance in which he had provided NSLs to Billy for signature but did not think it related to Operation Z. Youssef said that Billy asked him what case the NSLs were associated with but did not ask for any approval ECs.

The Primary Relief Supervisor stated that he did not draft approval ECs to accompany the NSLs because he believed they were being prepared by the CTD operational unit involved with Operation Z. He also told us that when he drafted the Company A September 21 NSL, he did not know that approval ECs were required, but he knew that a CTD operational unit was responsible for preparing ECs for the Operation Z NSLs.

We determined that all three Operation Z NSLs were defective. First, the NSLs were served after-the-fact. Second, the NSLs were not accompanied by approval ECs establishing the predication for the requests and the relevance of the records sought to authorized national security investigations. Finally, the NSLs did not disclose that the FBI had previously asked the providers to [redacted] these records or that the providers

had already done so and in many instances had provided responsive records.[222]

As described in the next section, the FBI later drafted an approval EC dated April 13, 2007, documenting the predication for these three blanket NSLs. We found a draft version of this EC stating that the records were obtained in exigent circumstances. However, the final signed EC did not contain that statement. In an e-mail dated April 30, 2007, from the Assistant General Counsel to NSLB Deputy General Counsel Thomas relating to the issuance of the EC, she told Thomas that the Unit Chief of the operational unit responsible for Operation Z "was not willing to put in [the approval EC] that it was an exigency, and he was not even willing to say that CAU thought it was an exigent circumstance because he didn't think CAU could believe that." The Unit Chief and an SSA of the operational unit responsible for Operation Z told us that they believed the telephone records requested by the CAU for this operation were not [redacted] under exigent circumstances. In addition, Youssef said that the telephone records that the CAU obtained from the on-site providers in Operation Z were of "very high intelligence value as opposed to a known threat."

5. OIG Analysis of 11 Improper Blanket NSLs

In sum, we concluded that the FBI's attempt to address the backlog of records requests awaiting legal process by issuing blanket NSLs was ill-conceived, legally deficient, contrary to FBI policy, and poorly executed, and these blanket NSLs created more problems than they solved.

First, as described at the beginning of this Chapter, the ECPA does not authorize the FBI to issue retroactive legal process to cover previously acquired records or information. Moreover, issuance of retroactive legal process did not cure any prior violations of the ECPA that occurred when the FBI sought and received records without prior legal process and in the absence of a qualifying emergency.

---

[222] In addition to the Operation Y and Z blanket NSLs discussed in this section, the CAU used the same practices in support of other counterterrorism investigations. For example, 4 after-the-fact NSLs and 3 after-the-fact grand jury subpoenas were used to cover [redacted] and the acquisition of records for more than 950 telephone numbers that were relevant to 2 other counterterrorism operations in 2005 and 2006. The FBI served legal process between 2 weeks and 6 months after receipt of the records. In many instances, records were provided in response to requests communicated by e-mail and other informal means. We found only a few exigent letters associated with these requests.

Beyond this threshold legal problem, we found that the three blanket NSLs to the three on-site communications service providers in 2006 to cover the backlog of records requests listed telephone numbers that were relevant to many different FBI investigations, including criminal and domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA and the Attorney General's NSI Guidelines. Accordingly, the signers of the NSLs could not certify, as required by the ECPA, that the records sought were relevant to "an authorized investigation to protect against international terrorism or clandestine intelligence activities" and that any investigation of a U.S. person was "not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States."[223] Also, these NSLs were issued without the required approval ECs, in violation of FBI policy. Without approval ECs to capture the records identified in these NSLs, the FBI did not collect data necessary to include in required periodic reports to Congress on NSL usage.

The eight blanket NSLs issued in connection with Operations Y and Z also failed to comply with FBI internal policy because they were issued without accompanying approval ECs. Additionally, the three blanket NSLs to Company A, Company B, and Company C to cover the backlog of records requests and the five Operation Y NSLs did not contain the required ECPA certification for NSLs imposing confidentiality and non-disclosure obligations on the recipients.

Finally, none of the 11 blanket NSLs stated that the FBI had already acquired the records, in some instances more than 3 years earlier. While we developed no evidence suggesting that the communications service providers who received these NSLs were misled, we nonetheless believe that the NSLs should have stated that the FBI had already acquired the records. The FBI later made this disclaimer in various corrective NSLs issued in 2008 and 2009. We believe it should have done so in these 11 blanket NSLs as well so that the NSLs would be fully accurate and would not mislead anyone who subsequently reviewed these NSLs.

II. The FBI's Corrective Action Since November 2006

We describe in this section the FBI's attempts at corrective action beginning in November 2006, after the FBI OGC learned that the CTD had

---

[223] See 18 U.S.C. § 2709(b). As discussed below, the FBI did not complete until March 2009 its review of all the telephone numbers listed in these three NSLs and issue revised NSLs for the telephone numbers that were relevant to national security investigations.

issued blanket NSLs without approval ECs. These efforts included the CTD's preparation of draft memoranda reporting possible intelligence violations to the FBI OGC; the FBI OGC's notification to the President's Intelligence Oversight Board (IOB) of an intelligence violation; the issuance of new guidance in March 2007 clarifying the FBI's authority to request telephone subscriber and toll billing records information; mandatory NSL training for FBI employees; relocation of the communications service providers' employees; and the FBI's analysis of whether it will retain records acquired in response to exigent letters and the blanket NSLs.

A. FBI OGC Learns of Blanket NSLs

As described above in connection with the Company B May 12 NSL, the Assistant General Counsel sent an e-mail to Youssef and other CTD and NSLB personnel regarding what she had told the OIG during her May 17, 2006, interview concerning problems the CAU had experienced in issuing NSLs. The Assistant General Counsel sent Youssef a follow-up e-mail on August 2, 2006, in which she asked Youssef whether there was any backlog of requests for which the FBI had received information but not yet issued an NSL. In his e-mail response dated August 3, 2006, Youssef stated that Billy had signed a "blanket NSL" for the "backlogged requests."[224]

On August 3 and on August 8, 2006, the Assistant General Counsel sent e-mails to Youssef requesting a copy of the NSL and approval EC that Youssef said Billy had signed in his August 3 e-mail but she received no reply from Youssef. NSLB attorneys took no further action regarding the Company B May 12 NSL until November 2006. On November 7, 2006, in connection with a meeting FBI General Counsel Caproni had scheduled that day with the OIG concerning a draft of our first NSL report, the Assistant General Counsel forwarded Youssef's August 3, 2006, e-mail about the Company B May 12 NSL to Caproni. The Assistant General Counsel wrote to Caproni, "I presume that Bassem [Youssef] told OIG about it so I thought you ought to know about it."

Caproni forwarded the e-mail to Billy and asked him whether he recalled signing a blanket NSL. Billy responded that he did not recall "signing anything blanket." On November 8, 2006, Caproni forwarded Billy's response to the Assistant General Counsel and asked her whether she could "unravel this." Also on November 8, the Assistant General

---

[224] Although Youssef's e-mail did not further describe this NSL, Youssef told us that he was referring to the Company B May 12 NSL.

Counsel forwarded Caproni's e-mail to Youssef and asked again for a copy of the NSL.

On November 14, 2006, in response to the Assistant General Counsel's inquiries about the blanket NSL that Billy had signed, a CAU SSA informed the Assistant General Counsel in an e-mail that Cummings had signed similar NSLs. The SSA then gave the Assistant General Counsel copies of the Company B May 12 NSL and three of the five Operation Y blanket NSLs that Cummings had signed.

After reviewing these four blanket NSLs, the Assistant General Counsel expressed concern to Youssef and the CAU SSA that these NSLs lacked required approval ECs, which were needed to document the predication for the NSLs and the investigations to which they related. The Assistant General Counsel also reported her concerns to her supervisors.

B. The CAU's Draft Memorandum to the FBI OGC Reporting Possible Intelligence Oversight Board Violation

On February 22, 2007, the Assistant General Counsel learned from an NSLB colleague (not from CAU personnel) about the three blanket Operation Z NSLs, which also lacked approval ECs. She then directed Youssef to draft a memorandum to the FBI OGC reporting the seven after-the-fact blanket NSLs she knew about at that time as possible Intelligence Oversight Board violations (PIOB): the Company B May 12 NSL, three of the five Operation Y NSLs, and the three Operation Z NSLs.

FBI personnel are required by internal FBI policy to report PIOBs to the FBI OGC within 14 days of discovery in an Electronic Communication (EC). Executive Order 12863, which has since been modified, required the Department to report intelligence violations to the IOB. According to Executive Order 12863, possible intelligence violations include any activities that "may be unlawful or contrary to Executive Order or Presidential Directive."

The Assistant General Counsel informed Youssef that the PIOB memorandum should address that the NSLs were issued without approval ECs and that the NSLs did not include the appropriate non-disclosure certification, but should not address "the exigent letter situation itself since we approved that as a legal principle."

The efforts to draft the PIOB memorandum resulted in new disclosures to the FBI OGC, as well as significant confusion and errors. For example, the first draft contained a description of the seven blanket NSLs that the Assistant General Counsel knew about and had asked to be included in the draft. In addition, it described two blanket NSLs that

neither Youssef nor others in the CTD or the CAU had previously disclosed to the FBI OGC: the Company C July 5 blanket NSL and the Company A August 25 Operation Y blanket NSL.

The CAU Supervisory Intelligence Analyst who drafted the PIOB memorandum told us he had never drafted a PIOB memorandum before and "this was just very confusing for me." He said that he pulled information for the draft from a file left behind by the CAU SSA who had drafted some of the blanket NSLs. He said that he drafted the "bare bones" of what he knew about the NSLs and sent the draft to Youssef. Youssef told us that he viewed the PIOB as "a first rough draft" and the CAU's "best effort," and that he believed that the FBI OGC was going to finalize the PIOB memorandum.

After reviewing the first draft, the Assistant General Counsel asked CAU personnel to explain why the draft referred to NSLs which she had not been previously told about.[225] In response, the Acting CXS Section Chief, Youssef, and the CAU's Primary Relief Supervisor re-drafted the PIOB memorandum on March 3, 2007. The second draft included the seven NSLs that the Assistant General Counsel had originally asked to be addressed but omitted any reference to the two additional NSLs included in the first draft that she had questioned.[226]

The Acting CXS Section Chief characterized his role in the second draft as trying to explain "massive confusion." He told us that the second draft was an attempt "to recreate a record that didn't exist." He said that he directed that the two blanket NSLs which the Assistant General Counsel had questioned be omitted from the second draft because the Supervisory Intelligence Analyst who had prepared the first draft could not explain them to him.

---

[225] The Assistant General Counsel referred in her e-mail to:

> one [NSL] to [Company C] on 7/5/2006 (WHICH I'VE NEVER HEARD OF), one [NSL] to [Company A] on 8/25/06 (WHICH I'VE NEVER HEARD OF) . . . The 8/25/06 NSL lists 750 numbers, not a paltry sum. The 7/5/06 NSL lists almost 50.

[226] Neither draft of the possible Intelligence Oversight Board violations (PIOB) memorandum listed the other two blanket NSLs that the CAU had drafted and the CTD had signed: the Company C August 24 Operation Y blanket NSL, which covered 612 telephone numbers, and the Company A September 21 blanket NSL, which covered 700 telephone numbers. Neither of these NSLs had been disclosed to the Assistant General Counsel or other FBI OGC attorneys at the time. The OIG brought these two blanket NSLs to the FBI OGC's attention in July 2007 during this investigation.

The Primary Relief Supervisor told us that he wrote the second draft memorandum but in doing so mostly relied on information from the Acting Section Chief and Youssef. He said that he provided input on the Operation Z NSLs included in the memorandum "because that's the case that I knew."[227]

Youssef told us that the CAU was told to draft the PIOBs but was "not given very clear instructions as to what the [P]IOB was about." He also said, "we did not know where to go, we did not know where to start and we put together what we knew."

We found that for several days after the second draft was completed, FBI OGC attorneys, including Caproni, exchanged e-mails with the Acting Section Chief and Youssef concerning the two blanket NSLs that were included in the first draft but omitted from the second draft. On March 6, 2007, NSLB Deputy General Counsel Thomas and the Assistant General Counsel met with the Acting CXS Section Chief and Youssef to discuss those NSLs. According to the Assistant General Counsel, the Acting Section Chief and Youssef stated at the meeting that the Senior Intelligence Analyst who prepared the first draft had mistakenly included those two NSLs, and that those NSLs had been properly issued. The Assistant General Counsel also said that the Acting Section Chief and Youssef told her that they could not locate the NSLs in the file.

The Assistant General Counsel reported to her supervisors after the meeting that Youssef had convinced her of the "incompetence of the people who were drafting the EC" and that she now believed the two blanket NSLs were erroneously listed in the first draft and properly omitted from the second draft.

Ultimately, the FBI OGC decided not to formally notify the IOB of details concerning the blanket NSLs.[228] Thomas told us that she decided,

---

[227] As described previously, the Primary Relief Supervisor had drafted the Operation Z NSLs. He also had drafted the Company A September 21 blanket NSL (which was not included in the draft PIOB memoranda), but told us he did not recall that NSL when he worked on the PIOB draft memoranda.

[228] Rather, on October 31, 2007, Thomas sent a letter to the IOB chairman to supplement information the FBI OGC had provided in earlier briefings to IOB staff on the FBI's analysis of exigent letters and blanket NSLs. The letter stated that the FBI would be reporting to the IOB the blanket NSLs that were issued without required approval ECs, as well as the blanket NSLs that improperly requested records relevant to criminal investigations. The letter also stated that the FBI will purge from FBI databases records for which the FBI "has no legal authority" under the ECPA NSL statute or the emergency voluntary disclosure statute. Julie F. Thomas, Deputy General Counsel, National Security (Cont'd.)

and Caproni agreed, that it would not be prudent to send piecemeal information to the IOB. She said that after the FBI fully resolves the issues relating to the CAU's improper receipt of records, the FBI will finalize a report to the IOB. Caproni and Thomas said that the FBI has periodically briefed the IOB about the manner in which the CAU has improperly obtained records from the on-site providers without process, including through exigent letters and blanket NSLs.[229]

In sum, the draft PIOB memoranda were flawed and failed to identify all 11 blanket NSLs that the CAU had prepared and CTD officials had signed between May and September 2006. We concluded that these failures occurred because CAU personnel did not maintain copies of the 11 blanket NSLs, and because the FBI's attempts in February and March 2007 to account for the blanket NSLs in the draft PIOB memoranda were confused, inaccurate, and ineffective.

C. FBI Legal Guidance Clarifying Legal Authorities

On March 1, 2007, shortly before the OIG publicly issued its first NSL report, the FBI OGC issued a guidance memorandum for FBI personnel stating that, after reviewing information provided to the FBI in the OIG's first NSL report, the FBI OGC was providing a "clarification of the legal avenues available to investigators who seek to obtain subscriber information and toll billing information from telephone companies."

The memorandum described the legal basis for employing the ECPA NSL authority and the ECPA emergency voluntary disclosure statute, and it directed that FBI investigators cease the practice of using exigent letters to obtain subscriber or other information from communications service providers "in advance of and upon the promise of the issuance of legal process."

Law Branch, Federal Bureau of Investigation, letter to Intelligence Oversight Board, October 31, 2007.

[229] In the October 31, 2007, letter to the IOB, Thomas stated that the failure to issue approval ECs for these NSLs violated FBI policy, "impacts Congressional [NSL] reporting, and hinders oversight." The letter stated that when the FBI's review is complete, the FBI would report to the IOB the absence of ECs documenting the issuance of these blanket NSLs. Julie F. Thomas, Deputy General Counsel, National Security Law Branch, Federal Bureau of Investigation, letter to Stephen Friedman, Chairman, Intelligence Oversight Board, October 31, 2007. After reviewing a draft of this report, the FBI stated that on March 31, 2009, the FBI OGC formally briefed the IOB regarding the CAU's use of exigent letters, the 11 blanket NSLs, and the FBI's subsequent corrective actions.

The EC stated that regardless of whether investigators seek the information through an NSL, grand jury subpoena, or emergency voluntary disclosure, "it is incumbent upon the employee to develop or obtain a sufficient factual predicate to allow for the lawful acquisition of this information." The EC also stated that the ECPA NSL statute requires that the FBI determine that a telephone number is related to an existing national security investigation and that the information sought is relevant to that investigation. It further stated that investigators requesting emergency voluntary disclosure can seek the same information – even in the absence of an open national security or criminal investigation – if they give the provider sufficient facts for the provider "to believe, in good faith, that disclosure of the information sought is required without delay by an emergency situation involving the danger of death or serious physical injury to any person." The EC stated that the provider's "good faith belief may be based solely on a statement from the FBI or other entity that an emergency exists," and that while a "request to the service provider may be oral, it is preferable to make the request in writing."

The EC also stated that requests for emergency voluntary disclosure must be approved by officials at a level not lower than an Assistant Special Agent in Charge for field divisions and not lower than Section Chief for a headquarters unit.[230] It stated that regardless of whether the request is made in writing or orally, the investigative file and a control file should contain written documentation of the approval of the emergency voluntary disclosure request by the appropriate FBI official, the emergency, and the approval of the service provider.[231]

D. Relocation of Communications Service Providers' Employees From the FBI

After the OIG issued the first NSL report, employees of the three on-site communications service providers moved out of the FBI's offices in December 2007 and January 2008. The FBI General Counsel told us that in the aftermath of the OIG's first NSL report in March 2007, the FBI and the three on-site providers concluded that while the co-location was legal and operationally beneficial, it blurred the distinction between the providers and the FBI. According to the FBI General Counsel, the FBI and the providers also concluded that both sets of employees had become "too

---

[230] The EC stated that the better practice is that the approval be in writing "in the form of a signature [by the approving official] on the letter to the service provider."

[231] A control file is an administrative file that is used to store various types of FBI information unrelated to particular investigations.

comfortable," had started thinking they were part of "the same team," and had failed to adhere to the internal controls established by the FBI, on the one hand, and the providers on the other.

These moves were also accompanied by changes in the FBI's protocols for obtaining telephone records under the contracts with the three providers. According to the CXS Section Chief, a new protocol for requesting records from the providers was established in December 2007 and documented in an EC dated January 11, 2008. Under the new protocol, [redacted]

FBI officials told us that, notwithstanding the move to off-site locations and implementation of the new protocols, the providers remain capable of quickly responding to the CAU's requests for telephone records in high-threat or emergency circumstances.

E. FBI Analysis of Whether it Will Retain or Purge Records

Beginning in late 2006 and concluding in April 2009, the FBI analyzed whether it would retain telephone records it acquired in response to exigent letters or records for any additional telephone numbers that were listed in the 11 improper after-the-fact blanket NSLs described in this report.

1. FBI Analysis

As described above, the FBI OGC was first told about a blanket NSL issued to address the backlog of records requests for Company B in August 2006, when Youssef informed the Assistant General Counsel that Acting Assistant Director Billy had signed "a blanket NSL request on all backlogged requests." Although Youssef's e-mail did not further describe the blanket NSL, Youssef told us that he was referring to the Company B May 12 blanket NSL. Eventually, the FBI OGC learned that the CAU drafted and CTD officials signed 11 blanket NSLs between May and October 2006.

In an elaborate and time consuming process, the FBI analyzed the 4,379 unique telephone numbers listed in exigent letters and the 11 blanket NSLs. We summarize below how the FBI organized and assigned the work of analyzing which numbers will be retained, its legal analysis of this issue, and the FBI's conclusion as to which telephone records it will retain and which it will purge from its databases.

a. FBI Review Team

To determine which records to retain, under the overall direction of NSLB Deputy General Counsel Thomas, the FBI assigned teams of attorneys, Supervisory Special Agents, Special Agents, and Intelligence Analysts to review the 2,222 unique telephone numbers listed in the exigent letters and the 2,157 additional unique telephone numbers listed in the 11 blanket NSLs.

The CTD selected an Acting Assistant Section Chief from one of its operational units to lead the FBI's analytical efforts, under the guidance of three NSLB attorneys. The Assistant Section Chief had extensive experience in both counterterrorism investigations and in the use of NSLs. CTD Intelligence Analysts who were also experienced in counterterrorism investigations assisted in this effort. During its peak, the Assistant Section Chief's team utilized 19 Intelligence Analysts and 7 support personnel. The team's effort was also supported in September and October 2007 by Intelligence Analysts based at an FBI facility in Idaho, who searched the FBI's databases for information relevant to the analysis.

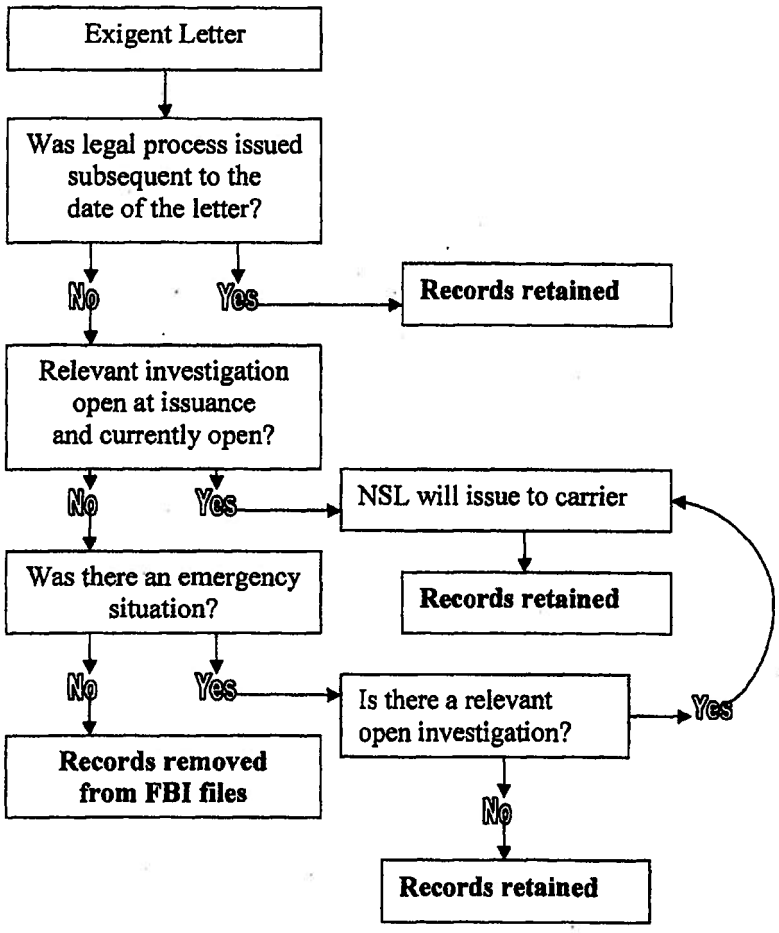
The review team gave the NSLB attorneys summaries of information collected on each telephone number, along with the team's recommendation as to whether the records should be retained by the FBI or purged. NSLB attorneys evaluated the data collected on each telephone number and made a determination as to whether they concurred with the team's recommendation.

b. FBI "Decision Tree"

In making its determinations on record retention, the FBI developed a 5-step analytical process, referred to by FBI OGC attorneys as the "decision tree," to assess whether the FBI would retain records obtained in response to exigent letters or after-the-fact blanket NSLs. The FBI OGC created Diagram 4.2 to illustrate the steps in its analysis:

DIAGRAM 4.2

FBI Summary Chart of Plan to Rectify the Exigent Letter Situation



First, the FBI determined whether legal process – an NSL or grand jury subpoena – was issued to the on-site communications provider before or after the records listed in exigent letters and the blanket NSLs had been requested.[232] In instances in which a valid NSL or subpoena was issued, the FBI concluded that it will retain the records. As described below, the FBI further reviewed the records for which legal process was located to

---

[232] Although the FBI's decision tree states that the FBI would determine if "legal process [was] issued subsequent to the date of the letter," in practice, the review team relied upon any valid legal process in determining whether to retain records, including legal process dated before the date of the exigent letter.

ensure that it only retained records for the time period specifically documented in the legal process.

Second, if the FBI was unable to identify valid legal process issued before or after the records were requested, the FBI examined both whether there was an investigation open *at the time of the request* and whether an investigation to which the records are relevant is *currently open.* If both requirements were satisfied, the FBI concluded that it would issue an NSL from the open investigation and retain the records. The approval ECs accompanying any such NSLs and the NSLs themselves state that the NSLs are not seeking new telephone records but instead are issued to account for previously acquired telephone records. If there was no investigation open at the time of the initial request and no investigation to which the records are relevant currently open, the FBI determined whether it had, in fact, acquired and uploaded any records associated with the telephone number.

Third, in instances in which legal process was not served, and there was no open investigation at the time of the initial request or there was no currently open investigation to which the telephone number was relevant, the FBI assessed whether there was an emergency situation at the time of the request. The FBI decided that if a reasonable person could conclude that an emergency situation, as defined by 18 U.S.C. § 2702(c)(4), existed at the time of the request, the FBI would retain the records.[233]

When analyzing whether a Section 2702(c)(4) "emergency circumstance" could support retention of records, the FBI review team told us that its attorneys, agents, and analysts attempted to engage in "time travel" and consider the facts known at the time of the request. NSLB Deputy General Counsel Thomas said that the team considered whether a reasonable person "looking from the [perspective of the]provider," could have concluded, based upon the facts that were present at the time of the request, that there was an "emergency circumstance" as defined in Section

---

[233] To make this determination, the review team analyzed the investigative information in FBI case files and used the "emergency" standard in 18 U.S.C. § 2702(c)(4), which authorizes communications service providers to voluntarily provide non-content telephone records to the FBI if the providers believe in good faith that "an emergency involving danger or death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."

The Assistant Section Chief, the Intelligence Analysts, and the NSLB attorneys described the ECPA emergency voluntary disclosure standard as the benchmark for their analysis, but they did not assess, or conclude, that the records in fact had been requested or received under the emergency voluntary disclosure statute in effect at the time.

2702(c)(4).[234] If the review team deemed that emergency circumstances existed that could have satisfied the statutory standard, the FBI would retain the records.

Fourth, if the FBI determined that legal process was not issued and that there was no relevant open investigation at the time of the request or no currently open relevant investigation, and that there were no emergency circumstances within the meaning of Section 2702(c)(4), the FBI would purge or remove the records from all FBI databases and FBI case files.

2. FBI Analysis of Records Obtained From Exigent Letters and 11 Improper Blanket NSLs

The FBI identified a universe of 4,379 unique telephone numbers from the exigent letters and blanket NSLs that it determined must be analyzed to establish whether records related to each number should be retained or purged. As Table 4.3 illustrates, the FBI decided it would retain the records related to a total of 3,352 telephone numbers (76 percent) because they fell into one of the three categories that justified retention under the decision tree described above. The FBI determined that records for a total of 739 telephone numbers (17 percent) would be purged from FBI databases because the records did not fall into one of the three categories for retention. The FBI could not locate any telephone records in FBI databases for the remaining 288 telephone numbers (7 percent) and, accordingly, no purging was necessary.

As Table 4.3 illustrates, the FBI located "standard process" for 1,405 of the 4,379 telephone numbers (32 percent). The FBI defined "standard process" as an NSL, a grand jury subpoena, or an administrative subpoena that it determined was issued in connection with the record [redacted] of these numbers. The FBI informed us that in most cases the legal process issued after-the-fact to cover exigent letters were NSLs, not grand jury subpoenas. We asked the FBI to determine how many of the telephone numbers were covered by each type of standard process and in how many instances the standard process was issued after-the-fact. Although as of October 2009 the FBI had not provided complete data. The FBI's partial data indicates that 1,104 of the 1,405 telephone numbers were covered by NSLs, which were issued after-the-fact for 946 of the telephone numbers.

---

[234] An e-mail dated August 22, 2007, summarizing a meeting that day with the review team and NSLB attorneys assigned to assist the team stated that the review "[r]equires time travel. Put yourself in the position of what was occurring when events were occurring. What did people believe at the time. BACK UP WITH DOCUMENTS..."

The FBI data also shows that 244 telephone numbers were covered by grand jury subpoenas, which were issued after-the-fact for 201 of the numbers.

In Table 4.3 we summarize the review team's final determinations on the retention of records for the 4,379 unique telephone numbers, and in the sections that follow we describe these determinations in more detail.

TABLE 4.3

FBI's Analysis of Basis for Retaining Records Listed in Exigent Letters and 11 Blanket NSLs

Blanket NSL or Exigent Letter	Providers			Unique Telephone Numbers					
					Retained			Not Retained	
	Company A	Company C	Company B	Total	Standard Process	New	2702(c)(4)	Purged	No Records
5/12/2006 Blanket NSL (1)			■	**105**	4	34	15	47	5
7/5/2006 Blanket NSL (1)		■		**33**	1	9	16	6	1
9/21/2006 Blanket NSL (1)	■			**693**	94	172	59	235	133
8/24/2006 Operation Y (2)		■	■	**544**	0	523	0	12	9
8/25/2006 Operation Y (1)	■			**184**	0	140	0	35	9
9/19/2006 Operation Y (2)	■	■		**157**	0	157	0	0	0
10/20/2006 Operation Z (3)	■	■	■	**441**	441	0	0	0	0
Subtotals of 11 Blanket NSLs				**2,157**	**540**	**1,035**	**90**	**335**	**157**
Exigent Letters	■	■	■	**2,222**	**865**	**765**	**57**	**404**	**131**
Totals				4,379	1,405	1,800	147	739	288

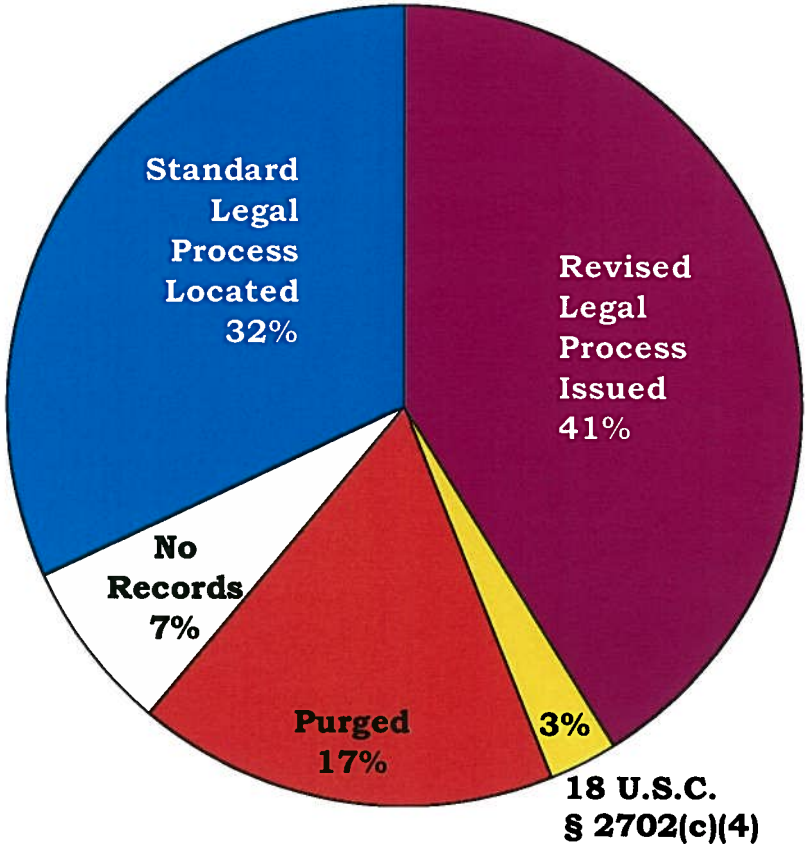
- **Standard Process** - Telephone records for which the FBI located an NSL, grand jury subpoena, or FBI administrative subpoena.
- **New Legal Process Issued** - Telephone records related to a currently open investigation from which an NSL was issued with an approval EC.
- **2702(c)(4) records** - Telephone records related to investigations that are now closed but for which circumstances existed that would have satisfied the legal standard for the ECPA emergency voluntary disclosure statute, 18 U.S.C. § 2702(c)(4).
- **Purged** - Telephone records that the FBI determined it will purge records from Telephone Applications, another telephonic database, and the investigative files.
- **No Records** - Telephone numbers that were listed in exigent letters or 11 blanket NSLs, but for which the FBI could not locate records in FBI databases. This category required no action.

In Charts 4.1 and 4.2 we summarize the review team's final determinations on retention of records for the same 4,379 unique telephone numbers, breaking down the data into the following sub-categories:

- Exigent Letters and Blanket NSLs (combined)
- Exigent Letters
- Company B May 12, Company C July 5, and Company A September 21 Blanket NSLs
- Operation Y and Z Blanket NSLs

CHART 4.1

Analysis of the FBI's Basis for Retaining Records from Exigent Letters and 11 Blanket NSLs



Exigent Letters and 11 Blanket NSLs

Exigent Letters

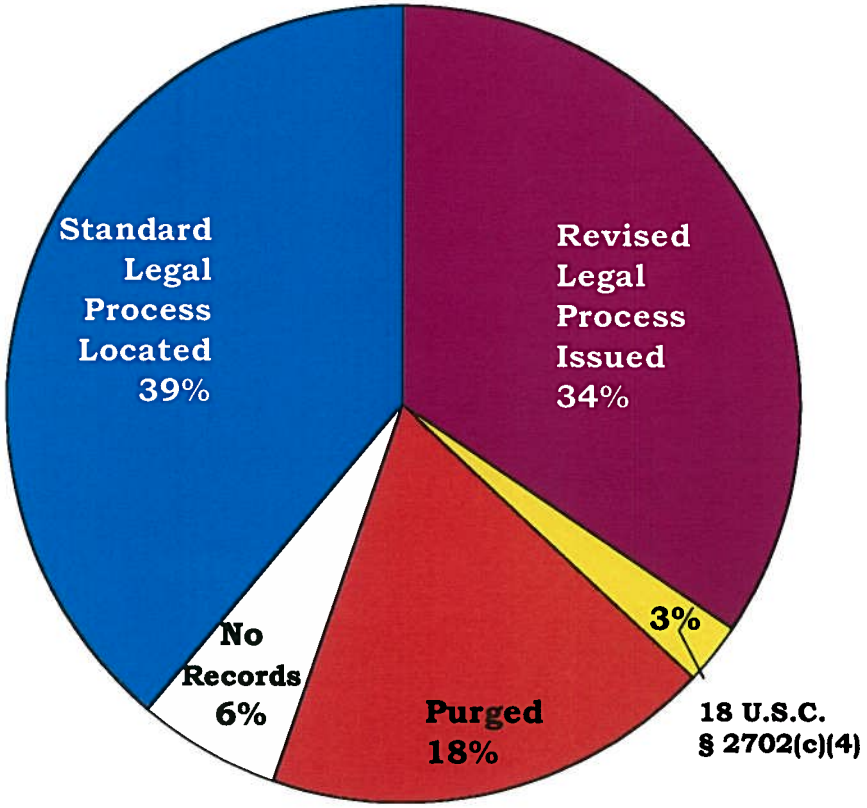
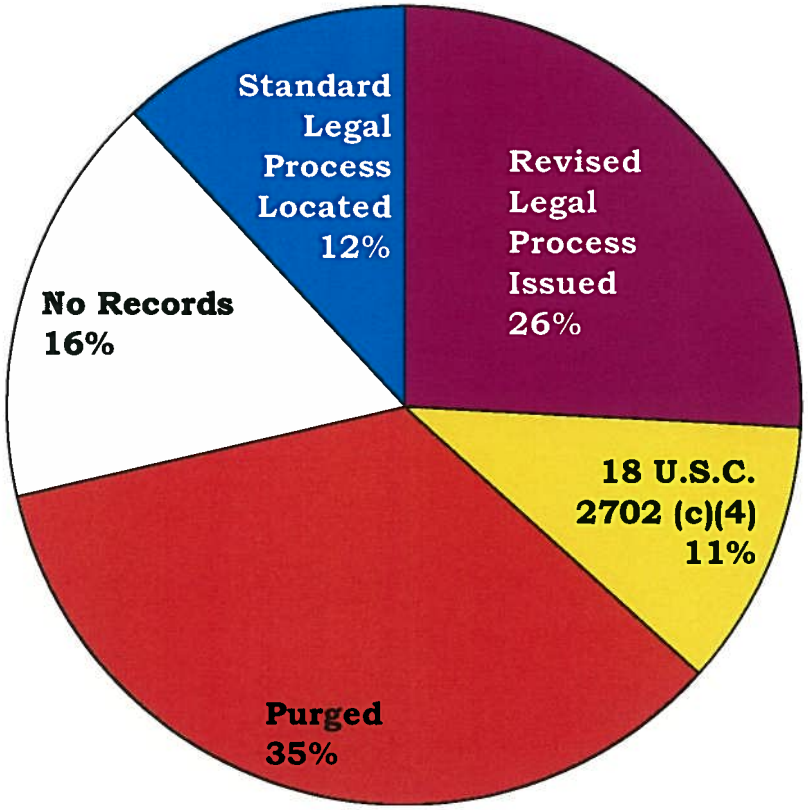


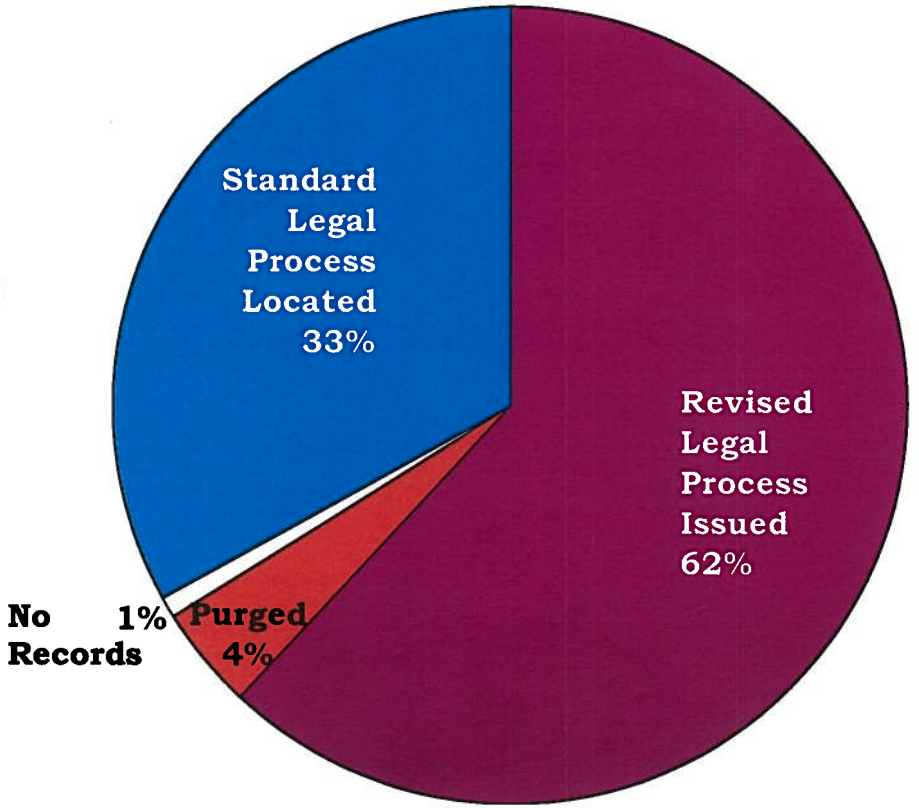
CHART 4.2

Analysis of the FBI's Basis for Retaining Records from Exigent Letters and 11 Blanket NSLs



Company B May 12, Company C July 5, and Company A September 21 Blanket NSLs

Operations Y and Z NSLs



a. Records Obtained in Response to Exigent Letters

The FBI told us it identified 2,222 unique telephone numbers listed in the 798 exigent letters which the OIG identified during our investigation and which the OIG gave to the FBI.[235] The FBI told us it has made the following determinations about these records:

- The FBI has located legal process (NSLs, grand jury subpoenas, or other legal process) issued either before or after the telephone number was given to the on-site communications service providers for 865 (39 percent) of the 2,222 unique telephone numbers identified in exigent letters. The FBI decided that it will retain these records because they are covered by legal process.[236]
- The FBI identified 765 telephone numbers (34 percent) for which it determined there were open national security investigations to which the telephone numbers were relevant at the time of the exigent letters and there is a currently open national security investigation to which the numbers are relevant. The FBI told us it issued NSLs and retained these records.
- The FBI determined that it obtained records on 57 telephone numbers (3 percent) in response to exigent letters that were issued in circumstances that would have satisfied the ECPA emergency voluntary disclosure statute (18 U.S.C. § 2702(c)(4)).[237] Accordingly, the FBI decided that it will retain the records for these numbers.

---

[235] The FBI did not retain copies of exigent letters. The OIG obtained copies of 798 exigent letters, which included a total of 3,764 telephone numbers, by serving OIG administrative subpoenas on the three on-site communications service providers. The FBI told us that after eliminating duplicate telephone numbers and telephone numbers listed in any of the 11 blanket NSLs, 2,222 unique telephone numbers remained.

[236] We address below the FBI's further analysis of these records to determine whether any of the records obtained by the FBI exceeded the date range specified in the corresponding legal process. The FBI determined that it will purge any such records.

[237] After reviewing a draft of this report, the FBI asserted that the low percentage of records it retained in its reconciliation project based on the emergency voluntary disclosure provision was a consequence of the sequence of the FBI's decision tree, and that the FBI often never reached the emergency provision as a basis for retention. The FBI also stated that "because CAU did not have adequate documentation," the FBI chose not to rely (Cont'd.)

- The FBI determined that records for 404 telephone numbers (18 percent) would be purged from FBI databases because the records did not qualify for retention under the categories described in the decision tree.
- The FBI determined that there were no records in FBI databases for 131 telephone numbers (6 percent), and therefore no further action was required as to these records.

Thus, with respect to the exigent letters, the FBI determined that it would retain records for 1,687 telephone numbers, that it had no information in its databases for 131 telephone numbers, and that it would purge records relating to 404 telephone numbers.

b. Actions Regarding the 11 Blanket NSLs

The FBI determined that the 11 blanket NSLs together listed an additional 2,157 unique telephone numbers. As with the telephone numbers listed in the exigent letters, the FBI used the decision tree described above to decide whether it will retain records for these additional telephone numbers.

Regarding the 11 blanket NSLs, the FBI has taken the following actions to date:

Company B May 12, Company C July 5, and Company A September 21 blanket NSLs (831 unique telephone numbers):

- The FBI determined that legal process existed for 99 telephone numbers (12 percent), and the FBI decided that it will retain these records.
- The FBI determined that there were open national security investigations to which records for 215 telephone numbers (26 percent) were relevant at the time of the requests, and there are currently open national security investigations to which the

---

primarily on the emergency disclosure provision in its reconciliation project. Nevertheless, the FBI asserted that "a substantial number" of the records were produced in qualifying emergencies. We agree with the FBI that the lack of documentation of the requests and the circumstances under which they were made makes reliance on Section 2702 problematic. As described in Chapter Six, the lack of documentation and other factors made it difficult for the OIG or the FBI to determine reliably whether and which requests without legal process were made in qualifying emergencies.

numbers are relevant. The FBI has issued NSLs for these 215 telephone numbers and will retain these records.

- The FBI determined that there were no open national security investigations to which records for 90 telephone numbers (11 percent) were relevant at the time of the requests and the time of the analysis but in circumstances that the FBI concluded would have satisfied the ECPA emergency voluntary disclosure statute (18 U.S.C. § 2702(c)(4)). The FBI decided that it will retain these records.
- The FBI determined that records for 288 telephone numbers (35 percent) would be purged from FBI databases because the records did not qualify for retention under the categories described in the decision tree.
- The FBI determined that there were no records in FBI databases for 139 telephone numbers (16 percent), and therefore no further action was required.

Five Operation Y NSLs (885 unique telephone numbers):

- The FBI determined that there were open national security investigations to which records for 820 telephone numbers (93 percent) were relevant at the time of the requests, and there are currently open national security investigations to which the numbers are relevant. The FBI has issued NSLs for these 820 telephone numbers and will retain these records.[238]
- The FBI determined that records for 47 telephone numbers (5 percent) would be purged from FBI databases because the records did not qualify for retention under the categories described in the decision tree.
- The FBI determined that there were no records in FBI databases for 18 telephone numbers (2 percent), and therefore no further action was required.

Three Operation Z NSLs (441 unique telephone numbers):

- The FBI determined that revised NSLs were not necessary because these three NSLs were signed by authorized FBI officials and contained the required certifications for NSLs

---

[238] Sixteen telephone numbers (2 percent) were relevant to open national security investigations other than Operation Y.

imposing non-disclosure and confidentiality obligations on the recipients.[239]

- On April 13, 2007, the CTD issued an EC documenting the predication for the three NSLs. Consequently, the FBI decided that it would retain these records.

c. Overcollections

The FBI review team also analyzed the records obtained for the telephone numbers listed in exigent letters and the blanket NSLs to determine if the FBI had acquired any records beyond the records specified in the legal process that formed the basis for the decision to retain the records. Specifically, the review team examined whether any records obtained and uploaded into FBI databases in response to exigent letters or listed in the blanket NSLs included records outside the date range of the dates specified in the corresponding legal process.[240] Based on its review, the FBI identified records related to 302 unique telephone numbers that it decided to purge due to overcollections.[241]

Of these 302 telephone numbers, the FBI identified 73 telephone numbers for which the FBI uploaded overcollections of more [redacted] In that universe, the FBI uploaded records on 1 telephone number more [redacted] outside the date range in the legal process, and records on 14 telephone numbers that were [redacted] outside the date range of the legal process.

The FBI decided to purge these overcollected records because they exceeded the scope of the legal authority used to obtain them. For example,

---

[239] The NSLs each included the same 445 telephone numbers, but 4 numbers were duplicates.

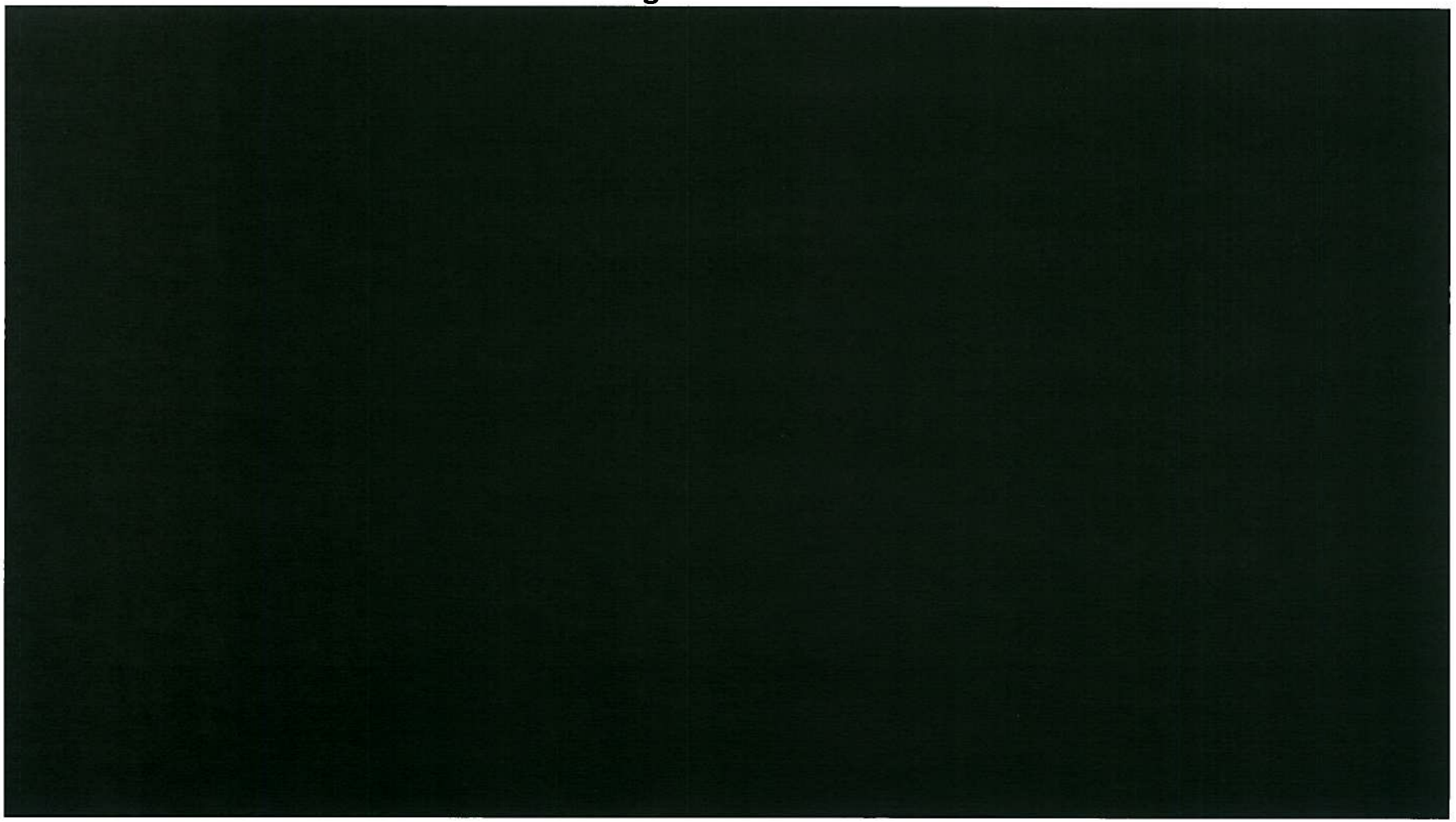
[240] In an August 26, 2008, EC the FBI stated that it had established a 14-day "grace period" before and after the date range specified in the after-the-fact legal process. Overcollections that fell within the grace period were not purged from FBI databases.

[241] As discussed in Chapter Two of this report, the CTD did not require until June 1, 2007, that case agents immediately ensure that responsive records accurately match the NSL request. The guidance issued in June 2007 required that any identified overcollections must be sequestered with an FBI attorney before the records are uploaded into any FBI database and must be returned to the provider, destroyed by the FBI, or addressed in another NSL. Similarly, the FBI did not require until October 17, 2007, that CAU requesters review responsive telephone records received from the communications service providers to ensure proper collection and then certify to the CAU's database manager by e-mail that the responsive records had been verified as accurately encompassing both the target telephone numbers and date ranges contained in the NSL.

the ECPA NSL statute requires certification that the records sought in NSLs are relevant to an international terrorism investigation. If the NSLs used to obtain the records certified, as required by the ECPA, that records sought within a specified time period were relevant to authorized national security investigations, but the FBI acquired records outside that date range, the overcollected records were not covered by the NSL certification. Chart 4.3 illustrates the variance between the date range of the after-the-fact legal process and the date range of uploaded records for 10 telephone numbers with the longest periods of overcollection:

CHART 4.3

Records for 10 Telephone Numbers Uploaded into FBI Databases with the Longest Periods of Overcollections



3. Steps Taken to Purge Records

The FBI has purged records from centralized FBI databases, field division-based databases, and hard copy files maintained by field division personnel. Based upon the FBI review team's findings, the CTD directed that records be purged either by the CAU, the Field Investigative Software Development Unit, or various field offices.[242]

4. Records Improperly Acquired Relating to Criminal Investigations

The FBI OGC determined that 266 telephone numbers listed in exigent letters and in 3 of the 11 blanket NSLs were related to criminal investigations or domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA NSL statute, the Attorney General's NSI Guidelines, or FBI policy.

According to the FBI OGC, it located appropriate legal process (either grand jury subpoenas or FBI administrative subpoenas) issued to the on-site providers before or after the FBI obtained records for 16 of these 266 telephone numbers, and the FBI determined that it will retain these records. The FBI OGC determined that it would retain records requested in grand jury subpoenas if a grand jury had been empanelled at the time the legal process was issued and the subpoena was served either before or after the records were obtained.[243] Of the remaining 250 telephone numbers, the FBI could not locate legal process for 167 telephone numbers. The FBI therefore directed the CAU to purge the records in FBI databases on these telephone numbers. The FBI review team informed us that there were no responsive records in FBI databases for the remaining 83 telephone numbers.

The FBI OGC informed us that a court-ordered wiretap had been instituted that targeted 1 of the 266 telephone numbers. The wiretap was

---

[242] As described above and in Chapter Two of this report, the CAU is responsible for uploading telephone transactional records into a [redacted] database. The Field Investigative Software Development Unit administers an unclassified FBI database called Telephone Applications, which is used to analyze the calling patterns of telephone records. Telephone Applications stores raw data derived from telephone records, known as "metadata," including the call duration. It does not store the contents of telephone conversations.

[243] Data on the FBI's retention decisions show that four grand jury subpoenas were dated after the date when the corresponding records were uploaded into an FBI database, while five were issued prior to uploading.

instituted 11 days after the date of an exigent letter seeking records on that telephone number. The FBI OGC directed the field division "to determine whether any information from the . . . exigent letter was utilized to establish probable cause for the [wiretap]." The FBI OGC advised us in March 2009 that the field office stated that probable cause for the wiretap was established by independent means.

As a result of the FBI's analysis, the FBI has decided to retain records for 16 of the 266 telephone numbers related to criminal or domestic terrorism investigations and to purge records for 167 telephone numbers.

5. Other NSLs Referred by the OIG to the FBI

In the course of this investigation, the OIG identified 32 NSLs that we believed warranted further review because they appeared to be signed by individuals who did not have authority to sign NSLs or the NSLs had other possible irregularities. We provided copies of these NSLs to the FBI in September 2007. In addition to the 32 NSLs identified by the OIG, the FBI identified 39 other NSLs with possible irregularities.

Of the 71 irregular NSLs, the FBI reported to us that it had issued letters of censure to 6 FBI employees who together signed 14 NSLs because they lacked the authority to sign NSLs.[244] The FBI took no action against 3 other FBI employees who together signed a total of 14 NSLs while they were serving as Acting Deputy Assistant Directors (Acting DAD), and the FBI noted that it did not have a written policy in place expressly prohibiting Acting DADs from signing NSLs until June 1, 2007 (after these NSLs were signed). Moreover, in January 2009 the Department's Office of Legal Counsel (OLC) determined that Acting DADs are authorized to sign NSLs.

Thirty-five of the 71 irregular NSLs were unsigned. The FBI said it was able to locate properly signed NSLs in its files for 23 of the NSLs in this group. The FBI said it was unable to determine who was responsible for the other 12 unsigned NSLs, and no action was taken with regard to these NSLs.

Of the remaining eight NSLs, the FBI said that one of the signatures on an NSL was illegible and no action was taken, four NSLs were referred by

---

[244] These individuals held the positions of SSA (1), Unit Chief (1), Acting Special Agent in Charge (3), and Section Chief (1).

the Inspection Division to the FBI OGC for possible IOB violations, and the FBI has not completed its research into the remaining three NSLs as of October 2009.[245]

6. OIG Analysis of FBI Retention Decisions

In evaluating the FBI's process and decisions regarding whether to retain or purge telephone records obtained through exigent letters and listed in the blanket NSLs, we recognize the competing interests faced by the FBI. On the one hand, the FBI wanted to retain records it believed were relevant national security investigations. FBI General Counsel Caproni stated that the FBI was concerned with losing information that could be critical to a counterterrorism investigation. In describing the FBI's various corrective measures, Caproni stated that the FBI cannot "put the nation at risk. So we chose a path that we think is reasonable."

On the other hand, FBI officials stated to Congress and publicly following the release of the OIG's first NSL report that it would "ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation."[246] The FBI Director and General Counsel Caproni stated that any records that were not associated with authorized investigations would "be removed from our databases and destroyed."[247]

In evaluating the FBI's review efforts, we recognize that the ECPA has no exclusionary rule for records acquired in violation of the statute.[248] Moreover, we recognize that the only duty specifically imposed on the FBI on discovery of the ECPA violations is to report the violations to the IOB, and that the FBI has provided periodic briefings to the IOB staff about exigent

---

[245] After reviewing a draft of this report, the FBI stated that the NSLB reported its findings to the Inspection Division regarding the four possible IOB violations in April 2009. One was then reported to the IOB, and the FBI concluded that the other three NSLs were proper.

[246] Valerie E. Caproni, General Counsel, FBI, before the House Committee on the Judiciary, U.S. House of Representatives, concerning "The Inspector General's Independent Report on the FBI's Use of National Security Letters," (March 20, 2007), http://www.fbi.gov/congress/congress07/caproni032007.htm (accessed March 26, 2009); Robert S. Mueller, III, Director, FBI, before the Senate Committee on the Judiciary, U.S. Senate, concerning "Oversight of the Federal Bureau of Investigation" (March 27, 2007), http://www.fbi.gov/congress/congress07/muelleri032707.htm (accessed March 26, 2009).

[247] Id.

[248] See 18 U.S.C. § 2708.

letters, blanket NSLs, and the FBI's ongoing analysis of the records obtained in response to these informal means. Thus, while the FBI is not legally required to purge records it obtained improperly, it decided to do so under certain circumstances.

In light of these competing issues, we believe that the FBI's decision tree and its analysis of which records to purge were reasonable responses to our identification of the improper collection of these telephone records. The FBI's analysis attempted to incorporate the legal standards of the ECPA NSL statute and the ECPA emergency voluntary disclosure statute, albeit after-the-fact. We also agree that it is reasonable to purge only those records whose retention cannot be justified under an application of the ECPA standards, even though the standards were applied after the collection had already occurred.

In applying these standards, the FBI has devoted significant resources in manpower and time to review the improperly obtained records and to consider whether there is a basis for retaining these records. However, it is also important to recognize, as we detailed in Chapter Two of this report, that the FBI's inexcusable failure to document its requests for thousands of telephone records severely hampered its ability to determine which records should be purged.

Finally, we believe the FBI should notify the IOB of the full details of its final record retention decisions, purging decisions, the 11 blanket NSLs, and all other actions to address the FBI's improper acquisition of ECPA-protected records.[249]

III. OIG Conclusions Regarding FBI Attempts at Corrective Action for Exigent Letters

As discussed in this chapter, prior to the issuance of the OIG's first NSL report in March 2007, from late 2003 through March 2007, the FBI made various attempts to address issues arising from the CAU's use of exigent letters and other informal means to obtain telephone records. However, during this time period, the FBI's actions were seriously deficient and ill-conceived, and the FBI repeatedly failed to ensure that it complied with the law and FBI policy when obtaining telephone records from the on-site communications service providers. Also during this time, the FBI

---

[249] After reviewing a draft of this report, the FBI stated that it has formally briefed the IOB on all these issues.

regularly issued after-the-fact NSLs, which were an inappropriate tool for remedying the FBI's improper practices. The FBI also issued 11 improper blanket NSLs to try to "cover" or validate the improperly obtained records. These attempts were inconsistent with the ECPA NSL statute, the Attorney General's NSI Guidelines, and internal FBI policy.

By contrast, after the OIG issued its first NSL report in March 2007, the FBI took additional actions to address the problems created by exigent letters, which we believe were appropriate. The FBI ended the use of exigent letters; issued clear guidance on the proper use of NSLs; directed that FBI personnel be trained on NSL authorities; agreed to the move of the communications service providers' employees off the FBI's premises; and expended significant effort to determine whether improperly obtained records should be retained or purged from FBI databases.

CHAPTER FIVE
OIG FINDINGS ON FBI MANAGEMENT FAILURES AND INDIVIDUAL ACCOUNTABILITY

In this chapter, we assess the accountability of FBI employees, their supervisors, and the FBI's senior leadership for the use of exigent letters and other improper practices we described in this report. In Part I of this chapter, we discuss the significant management failures that we concluded contributed to these improper practices and to the FBI's failure to address the improper practices in a timely manner. In Part II, we assess the accountability of individual FBI employees for these improper practices.

I. Management Failures

We found that numerous, repeated, and significant management failures led to the FBI's use of exigent letters and other informal requests for telephone transactional records over an extended period of time. The FBI failed to follow the *Electronic Communications Privacy Act* (ECPA) statute, the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), and FBI policies when obtaining thousands of telephone records from the on-site communications service providers. While these on-site providers provided the FBI with an important resource in support of its counterterrorism, counterintelligence, and criminal programs, the FBI failed to provide adequate training, guidance, and oversight to ensure that FBI personnel used this resource in accordance with applicable statutes, guidelines, regulations, and FBI policies. These failures began shortly after the Communications Analysis Unit (CAU) was established within the Counterterrorism Division (CTD) in 2002, and continued until March 2007 when the OIG issued its first NSL report describing the use of exigent letters. We believe that every level of the FBI, from the FBI's most senior officials, to the FBI's Office of the General Counsel (FBI OGC), to managers in the CTD, to the supervisors in the CAU, to the CAU agents and analysts who repeatedly signed the letters, was responsible in some part for these failures.

As discussed in Chapter Two of this report, the concept of using exigent letters originated as a time-saving technique in the FBI's New York Field Division during its criminal investigations of the September 11 terrorist attacks. However, their use was transferred to the CAU at FBI Headquarters in early 2003 and over time became one of the means by which the FBI routinely obtained telephone records from the on-site communications service providers. The embedding of the communications service providers' employees in FBI work space alongside CAU employees, coupled with the FBI's increasing reliance on telephone subscriber and toll

billing records information in its counterterrorism investigations, led to a culture in which exigent letters and other even less formal and equally inappropriate requests for information became the CAU's accepted and customary method of conducting business. We found that a distinct lack of oversight and scrutiny by CAU managers, CTD officials, and FBI OGC attorneys enabled the improper practice of obtaining ECPA-protected telephone records with the promise of future legal process to expand and proceed virtually unchecked for over 4 years.

In reaching our conclusions, we recognize the CAU's and the FBI's important mission to detect and prevent terrorist attacks and the challenges the FBI faced after the September 11 attacks. After the September 11 attacks, the FBI reorganized its mission, structure, and procedures to emphasize counterterrorism. As part of this reorganization, the FBI created the CAU with the important mission of facilitating prompt retrieval and analysis of telephone records from the communications service providers for high-priority investigations. The CAU typically requested the telephone records to pursue its critical counterterrorism mission, not with the intention to obtain records that CAU personnel knew they were not legally entitled to obtain. Moreover, it is important to recognize that when we uncovered the improper exigent letter practices and reported them to the FBI in our first NSL report, the FBI terminated these improper practices and issued guidance to all FBI personnel about the proper means to request and obtain telephone records under the ECPA.

However, in our view that does not excuse the extended, widespread, and improper use of exigent letters and other informal means to obtain telephone records that the FBI used for many years, or the FBI's ill-conceived and ineffective attempts to cover those record requests with after-the-fact NSLs and improper blanket NSLs. As discussed in the next section, we believe the responsibility for these practices was widespread, from the top of the FBI, to the supervisors who oversaw these practices, to the FBI attorneys who failed to correct these practices in a timely way, to the line employees who signed these letters that were inaccurate on their face.

A. Failure to Plan for Proper Use of the On-Site Communications Service Providers

We found that FBI officials at all levels failed to develop a plan and implement procedures to ensure that telephone records were properly obtained from the on-site communications service providers. Such planning was needed from the outset of the CAU's establishment in 2003, particularly when employees of the communications service providers were co-located in the CAU's work space. We also believe that the need for such planning was obvious before the CAU began operations, not just in hindsight.

When the CAU began operations in 2002, a combination of factors created clear risks for potential misuse of NSL authorities and other authorities to obtain records in support of FBI national security investigations. These factors included the FBI's expanded NSL authorities in the USA PATRIOT Act[250]; the CAU's status as an operational support unit; the establishment of contracts with the communications service providers for on-site support at the FBI; the close proximity of the providers' employees to CAU personnel in a common work area[251]; the assignment of Supervisory Special Agents (SSA) and Intelligence Analysts to the CAU who had little or no background in national security investigations or in using NSLs; and continual and insistent demands for telephone transactional records from FBI field and Headquarters operating units. However, FBI managers failed to recognize these risks and take steps to avoid them.

For example, from the inception of the FBI's contractual relationships with the three providers in 2003, senior FBI leaders knew that the CAU would be handling telephone transactional records which the FBI could lawfully obtain pursuant to the ECPA. However, FBI leaders and managers failed to ensure that responsible officials in the CTD and the FBI OGC's National Security Law Branch (NSLB) reviewed the proposed and final contracts with the on-site providers to ensure that the agreements conformed to the requirements of the ECPA, the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), and other relevant laws and policies governing the FBI's authority to obtain telephone transactional records. FBI leaders and managers also should have recognized early on the need to train CAU personnel on the authorized methods and procedures for requesting records from the on-site providers, the need to clearly communicate those procedures to the on-site providers' employees and their respective supervisors, and the necessity of establishing oversight mechanisms to ensure those procedures were followed.

The first CAU Unit Chief, Glenn Rogers, and most SSAs initially assigned to the CAU had no prior experience in national security

---

[250] As described in our first NSL report, the Patriot Act significantly broadened the FBI's authority to obtain information through NSLs by lowering the evidentiary threshold for seeking NSLs and by extending the authority to sign NSLs to Special Agents in Charge of the FBI's 56 field offices.

[251] We found that the close proximity of the providers' employees and CAU personnel led to a casual, informal atmosphere in the CAU, as well as friendships and social contacts outside the office that blurred the lines between the responsibilities of FBI personnel and the providers. We believe that atmosphere contributed to the informal and improper use of exigent letters and other requests for telephone records.

investigations. The FBI's failure to provide adequate guidance on the proper way to obtain telephone records in national security investigations had serious consequences. We found that from the outset of the CAU's operations, the CAU SSAs used impermissible procedures such as exigent letters and sneak peeks to obtain ECPA-protected information and records. These practices – some of which were copied from procedures used by FBI personnel in the New York Field Division in connection with criminal investigations relating to the September 11 hijackers – became standard operating procedures for the CAU and continued throughout the 3-year period while Rogers was the CAU Unit Chief and then the Assistant Section Chief of the CTD's Communications Exploitation Section (CXS).

Only years later, in retrospect, a senior CTD official acknowledged the FBI's failure to plan in advance for having the communications service providers on-site, observing, "it [was] like having the ATM in your living room. You know you can go to it all the time and take the overdrafts because that was what was happening."

B. Failure to Provide Training and Guidance to CAU Personnel

The FBI compounded its planning failures when it did not ensure that all CAU personnel were trained on the legal requirements for obtaining ECPA-protected records. In particular, FBI managers from the CAU Unit Chiefs, to the FBI OGC, to the senior leaders of the FBI failed to ensure that CAU personnel were properly trained to request telephone subscriber and toll billing records information from the on-site communications service providers in national security investigations only in response to legal process or under limited emergency situations defined in 18 U.S.C § 2702(c)(4). They also failed to ensure that CAU personnel were trained to comply with the Attorney General's NSI Guidelines and internal FBI policies governing the acquisition of these records. This training was needed not only for existing CAU personnel but also, in light of personnel turnover in the unit over the 4-year period of our review, for all incoming CAU employees.

At the most basic level, the FBI failed to instruct CAU personnel that FBI requesters must provide NSLs or other legal process before CAU personnel requested records from the on-site providers relevant to FBI investigations, except in certain specified emergency situations. Additionally, the FBI failed to train field and Headquarters requesters on when and how true emergency requests should be handled. The FBI also failed to advise CAU personnel of the statutes or regulations in addition to the ECPA that limit the FBI's authority to obtain certain types of telephone records, such as news reporters' toll billing records; the FBI's authority to issue administrative subpoenas in certain investigations; and the FBI's

authority to obtain pen register/trap and trace orders for ECPA-protected information covered by the Pen Register Act.

Even Joseph Billy, Jr., who was CTD Deputy Assistant Director (DAD) and the CTD Assistant Director from April 2005 to March 2008, told us that he was unaware of the ECPA emergency voluntary disclosure statute when he was a Special Agent in Charge, a CTD DAD, or the CTD Assistant Director. In fact, Billy said he did not know that communications service providers did not need NSLs for records they provided to the FBI pursuant to the ECPA emergency voluntary disclosure statute. He told us that when he learned about the statute prior to his August 2007 OIG interview, "that was a revelation to me."

The FBI's failures also involved senior attorneys in the FBI OGC. NSLB attorneys failed to recognize the seriousness of the information they learned in late 2004 and early 2005 about the "form letter" – an exigent letter – that was being used in the CAU to obtain records from the on-site providers that was followed by after-the-fact NSLs. From then until March 2007, when the OIG's first NSL report was issued, the FBI OGC failed to take sufficient action to address the FBI's improper use of these exigent letters and after-the-fact legal process.

Aggravating this failure, FBI OGC attorneys also provided flawed guidance to CAU personnel about obtaining records from the on-site providers. For example, in April 2005 the Assistant General Counsel who was the NSLB point of contact for NSL-related policies and issues wrote that exigent letters could be used in emergencies "only if it is clear to you that the requestor cannot await an NSL." This guidance did not accurately state the requirements of either the ECPA NSL statute (18 U.S.C. § 2709), or the emergency voluntary disclosure statute (18 U.S.C. § 2702(c)(4)).[252] However, this flawed guidance was circulated to all CAU employees, and the CAU continued to request information from the on-site providers first, and addressed the need for legal process later (if at all).

---

[252] To conform to the ECPA, proper guidance would have stated that the FBI could either compel the production of records by first serving legal process or could request voluntary disclosure of records in the types of emergencies defined in the emergency voluntary disclosure statute. In April 2005, the statute authorized communications service providers to voluntarily disclose records or information "if the provider reasonably believe[d] that an emergency involving immediate danger or death or serious physical injury to any person justifie[d] disclosure of the information. 18 U.S.C. § 2702(c)(4) (Supp. 2002). In March 2006, the provision was amended to allow a communications service provider to disclose records "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." See 18 U.S.C. § 2702(c)(4).

A second instance of a flawed legal response occurred in May 2006 when the NSLB again perpetuated the use of exigent letters promising future legal process. Although NSLB attorneys were aware of the CAU's use of exigent letters at least by December 2004, no NSLB attorney asked to see a copy of any exigent letter until May 2006. As described in Chapter Four of this report, we found that the Assistant General Counsel, who was involved in advising the CAU on the use of exigent letters, first asked to see the exigent letter on May 19, 2006, 2 days after the OIG interviewed her in connection with our first NSL report and asked her questions about the CAU's acquisition of records prior to issuing legal process. After reviewing the exigent letter, the Assistant General Counsel modified the letter by substituting the word "NSL" for the word "subpoena" and deleting the reference to the U.S. Attorney's Office. This corrected the inaccurate reference to grand jury subpoenas in many of the letters, but the advice given by the NSLB was still flawed because the revised letter continued to seek to obtain records with the promise of future legal process. We find it troubling that neither the Assistant General Counsel, her immediate supervisor, nor NSLB Deputy General Counsel Thomas reviewed an exigent letter for more than 1½ years after they learned of their use.

In addition, the FBI OGC and the CTD failed to use the FBI's alternate authority under the ECPA (18 U.S.C. § 2702(c)(4)) to request voluntary disclosure of telephone records from the on-site providers in qualifying emergencies. Even though FBI OGC attorneys developed the first general guidance for all FBI divisions during the spring and summer of 2005 regarding the emergency voluntary disclosure statute, they failed to coordinate with CTD management and direct that the FBI (1) stop using exigent letters; or (2) advise CAU personnel that the emergency voluntary disclosure statute should be used to address record requests in appropriate circumstances. These corrective actions did not happen until 2007, shortly before the OIG's first NSL report was issued.

The FBI OGC's failure to ensure that CAU personnel were aware of the ECPA emergency voluntary disclosure statute had significant consequences. Between August 25, 2005, (the date of the FBI OGC guidance on the ECPA emergency voluntary disclosure statute), and November 13, 2006. (the date of the last exigent letter we located), CAU personnel issued an additional 86 exigent letters seeking records for 553 telephone numbers. None of these letters was subjected to the scrutiny or approval procedures that FBI personnel were directed to employ when requesting emergency voluntary disclosures under the ECPA. Moreover, as described in Chapter Two of this report, during this same time period the FBI acquired records or calling activity information on thousands of other telephone numbers through other informal means, such as sneak peeks, e-mail, and telephonic requests.

C. Failure to Oversee the CAU Activities

In addition to the FBI's failures in planning, training, and legal advice, we also found that every level of FBI supervision – from the FBI's most senior leadership to the Unit Chiefs in the CAU – failed to recognize the need for, and assure adequate oversight of, the practices employed by the CAU to obtain subscriber information, toll billing records, and other calling activity information from the on-site providers.

In our review , with the exception of CXS Assistant Section Chief John Chaddic, and Rogers (who became an Assistant Section Chief in the CXS after serving as Unit Chief of the CAU), no one in the CTD's supervisory chain above the CAU Unit Chiefs said they were aware of the FBI's use of exigent letters. As described in Chapter Two, John Pistole and Willie Hulon, the Executive Assistant Directors of the FBI National Security Branch during the period covered by our review; CTD Assistant Director Joseph Billy, Jr.; and CTD Deputy Assistant Director John Lewis all said they were unaware that the CAU was using exigent letters rather than NSLs to obtain records from the on-site communications service providers.[253] Similarly, Laurie Bennett, who was the CXS Section Chief, said she did not know about the use of exigent letters. CXS Section Chief Jennifer Smith Love also told us that she was unaware of exigent letters until after she left her position as the Section Chief. However, Love also told us she knew the FBI was getting records without legal process, yet she did not ensure that the CAU's activities were legal or fully reviewed.

The one CTD manager who said he was aware of the use of exigent letters, CXS Section Chief Chaddic, told us that he learned from Rogers that the CAU was using exigent letters as a "placeholder" to obtain telephone records from the on-site providers prior to the service of the appropriate legal process. Yet, he did not ensure that Rogers sought legal guidance from the FBI OGC about the use of the letters or implement other measures to ensure the appropriateness of the CAU's use of these letters.

We believe that each of these CTD officials was responsible for knowing what their subordinates were doing, ensuring that agents and others under their command complied with applicable law and FBI policy governing the acquisition of telephone transactional records, and ensuring that FBI attorneys had sufficient information about the CAU's practices to provide appropriate legal guidance and advice concerning what the CAU was

---

[253] Pistole, Billy, and Hulon also served as Deputy Assistant Directors of the CTD during the period covered by our review.

doing and planning to do. As CTD Assistant Director Billy stated to us, "there was never a timeout period to any of this to say, okay, let's do a check, a compliance."

The failure of FBI officials to understand the practices employed within the CAU to obtain records from the on-site providers extended not only to exigent letters, but also to other improper methods described in Chapter Three this report. For example, CTD Assistant Director Billy did not know as late as April 2007 about the FBI's improper use of hot number [redacted] – a service provided by Company A's and Company C's on-site providers [redacted] without any legal process. The FBI General Counsel and the Deputy General Counsel for the NSLB also told us they did not know that the FBI had used hot number [redacted] Similarly, until this OIG investigation, we found no evidence that any responsible FBI officials or any FBI attorneys were aware that FBI agents had used inaccurate language in FISA declarations that attributed the FBI's acquisition of telephone records to NSLs when in fact the records were acquired through other means, such as exigent letters and other informal requests.

As a result of these actions, the FBI violated the statutory and Attorney General Guidelines' requirements for senior-level approval of requests for telephone subscriber and toll billing records information and other ECPA-protected information and the 4-step NSL approval process established by the FBI's own policy to ensure these requests were based on appropriate predication. As Diagram 2.2 from Chapter Two illustrates, the FBI substituted a 1-step process by which the CAU SSAs and Intelligence Analysts signed requests for telephone records without supervisory review by those officials authorized to approve and certify the FBI's basis for requesting these types of records.

In sum, we believe that FBI senior leadership, senior attorneys, and CTD supervisors failed to take adequate measures to ensure that the FBI was obtaining telephone records from the on-site communications service providers properly, that sufficient training was provided to the FBI employees who obtained these records, that the new NSL powers granted to the FBI in the Patriot Act were sufficiently monitored, and that the FBI provided sufficient oversight on these new and intrusive authorities. The need for these actions should have been particularly clear when FBI attorneys learned in late 2004 and early 2005 that the FBI was acquiring telephone records without legal process. Moreover, no one in the CAU raised concerns about these exigent letters to higher level CTD officials or other senior FBI managers, even when Unit Chief Rogers and some of the agents signing exigent letters should have realized that the letters were inaccurate on their face.

II. Individual Performance

While the management failures described above explain in part how the FBI came to use exigent letters and other informal methods for requesting records from the on-site providers, these management failures do not explain all the deficiencies we found in this review.

Rather, in this review we also concluded that FBI supervisors and attorneys did not take sufficient action to oversee or prevent the use of exigent letters and other improper requests for telephone records. We also believe that the performance of some FBI employees who signed the letters that were inaccurate on their face was not in accord with the high standards expected of FBI and other law enforcement personnel. We discuss the actions of these individuals in the sections below.

A. CAU Unit Chief Glenn Rogers

While Rogers served as the CAU's first Unit Chief and later as CXS Assistant Section Chief, he made several decisions that resulted in widespread use of exigent letters without adequate legal review by the NSLB, and also without an adequate system to track their use or document the many less formal requests for telephone records from the on-site providers.

First, we found that in November 2003 Rogers approved an EC which instructed CAU personnel on how to handle responsive toll billing records obtained "[u]nder the authority of an Exigent Circumstances Letter." Yet, Rogers made no effort to confirm, either then or later, whether these so-called exigent letters were appropriate for use by the CAU in connection with national security investigations. As the CAU Unit Chief, Rogers was responsible for ensuring that the processes used by his unit were lawful and appropriate. Rogers said that a Company A analyst told him in May 2003 that exigent letters had been used by the FBI's New York Division and that the "lawyers" had approved the letter. His decision to rely only on a Company A analyst's vague representations as to the propriety of using such letters, and a reference to unnamed "lawyers," was imprudent and improper.

Second, we found that Rogers failed to properly discharge his duties as CAU Unit Chief and CXS Assistant Section Chief when he signed, and permitted his subordinates to sign, exigent letters that inaccurately stated that subpoenas requesting the telephone records listed in the letters had "been submitted to the U.S. Attorney's Office who will process and serve them formally . . . as expeditiously as possible." When we asked Rogers why he signed his name to exigent letters containing these inaccurate statements, he said:

> The only thing I really regret is the wording in that letter. The letter was just a placeholder and it was a bad move on my part . . . It's my fault . . . I relied on a flawed piece of paper to do that and I am sick by it. I am sickened. But I do not think the letter is the issue. To me the issue is the exigent circumstances and there were.

Rogers's explanation is unpersuasive. He knew the letters contained statements that were inaccurate, yet he signed 12 exigent letters and allowed his subordinates to sign 678 additional exigent letters during his tenure as a supervisor in the CTD. Even if there were exigent circumstances – and we found evidence indicating that there was not exigent circumstances in all cases, let alone a qualifying emergency under Section 2702 – that does not excuse an FBI employee signing his name to a letter that contains inaccurate statements of fact.

Moreover, after at least three CAU SSAs complained to Rogers about using exigent letters that contained inaccurate references to grand jury subpoenas having been requested from the U.S. Attorney's Office, Rogers told them to continue using the letters. He told one of them not to change "a single word." Rogers should have recognized and taken immediate action then to address the inaccurate statements in the letters. He should have acknowledged the SSAs' concerns and, at minimum, changed the wording of the exigent letters to make them accurate. He also should have consulted with NSLB attorneys and asked them to review the exigent letters to determine if they could lawfully be used to support FBI investigations. He did none of these things.

Third, Rogers failed to ensure that the personnel assigned to his unit – many of whom had no prior experience in the FBI's national security programs – received training on the authorized methods to request and obtain telephone subscriber and toll billing records information in national security investigations. None of the CAU SSAs we interviewed who signed exigent letters said they had received training on the FBI's authorities under the ECPA to obtain records pursuant to NSLs or the emergency voluntary disclosure statute.

Fourth, Rogers did not ensure that guidance was issued which, at a minimum, described in which situations exigent letters could be used. As a result, CAU personnel used exigent letters and then provided after-the-fact legal process in a wide variety of inappropriate circumstances. As described in Chapters Two, Three, and Four of this report, these included instances in which NSLs were not authorized under the ECPA, the Attorney General's NSI Guidelines, or FBI policy and also when the standards set forth in the ECPA emergency voluntary disclosure statute were not satisfied. Rogers's authorization of the CAU's use of exigent letters to obtain thousands of

ECPA-protected records rather than using legal process such as NSLs or emergency voluntary disclosure requests led to a serious abuse of the FBI's expanded authority to issue NSLs following enactment of the Patriot Act.

Fifth, Rogers failed to ensure that Bassem Youssef, his successor as CAU Unit Chief, was briefed on the unit's methods and procedures, including the specific methods the CAU used for obtaining records from the on-site providers. Rogers told us he had objected to Youssef's selection as Unit Chief and that he had little substantive contact with Youssef after his appointment. Notwithstanding Rogers's objections to Youssef's selection, Rogers should have fully briefed Youssef upon his entry on duty as Unit Chief and should have remained engaged with Youssef's management of the unit, including Rogers's plan to implement the Tracker Database to track requests to the on-site providers and the need to issue follow-up legal process.

Rogers attempted to justify his actions by stating that he regularly reminded CAU personnel to stay current on securing the after-the-fact legal process for the providers. He also said he sometimes spoke with personnel assigned to CTD operational units and at least one field division about the importance of issuing after-the-fact legal process for telephone records. However, his efforts were not sufficient to ensure that after-the-fact legal process was issued, and he never raised concerns about the practice to other managers or attorneys in the FBI.

In addition, we found that Rogers's failure to clearly explain to CAU personnel what was appropriate under the law and FBI policy led to other lax and sloppy practices in the CAU, including sneak peeks and informal requests for records conveyed by e-mail, telephone calls, and face-to-face conversations.

Sixth, when Rogers was the CAU Unit Chief and also when he was the CXS Assistant Section Chief, the CAU did not implement any system for tracking requests to the on-site providers, or keeping copies of the exigent letters, or ensuring that legal process was issued promptly after the records were provided to the FBI. The CAU relied on the on-site providers rather than its own internal controls to document requests for records and the need for legal process. As a result, the growing backlog of [redacted] or records for which the providers needed legal process went largely unnoticed and unaddressed by FBI managers for over 3 years, until mid-2006. In addition, once FBI managers focused on the improper actions, the lack of documentation of these requests greatly complicated the FBI's efforts to determine whether it had a basis for retaining these records.

Seventh, Rogers also did not consult with NSLB attorneys about the use of sneak peeks and other informal requests to obtain information from the on-site providers, or about the FBI's acquisition of calling activity information on [redacted] hot numbers without legal process. As Unit Chief of the CAU, he should have consulted with NSLB attorneys about these practices to ensure that CAU personnel followed the ECPA, the Attorney General's NSI Guidelines, and other relevant laws, regulations, and FBI policies governing the acquisition of telephone records.

When we questioned Rogers about these actions, he acknowledged that after a Company A analyst first told him about exigent letters in May 2003, he allowed the use of exigent letters by CAU personnel without issuing clear guidance regarding how they were to be issued. However, Rogers stated that nothing was done "to hide the fact that we were getting stuff in advance of NSLs."

Rogers also stated that from the time NSLB attorneys became fully aware of the exigent letter practice in late 2004, the NSLB attorneys never sought to bring their use to a halt. When we asked Rogers about a December 2004 e-mail from the Assistant General Counsel to a CAU SSA in which the Assistant General Counsel discussed the SSA's request for an after-the-fact NSL, Rogers noted the Assistant General Counsel's statement in the e-mail, "I am realistic enough to recognize that there are emergency situations wherein we get the information on the promise of an NSL." Rogers also told us that during the time he was the CAU Unit Chief and later the CXS Assistant Section Chief he was never told by FBI attorneys or CTD management that the exigent letter practice was unacceptable.

We agree that NSLB attorneys share some of the responsibility for the improper use of exigent letters when they did not end their use after learning about them. However, for the reasons stated above, we believe Rogers bears a large portion of the responsibility for the CAU's improper use of exigent letters.[254]

B. CAU Unit Chief Bassem Youssef

In evaluating Youssef's actions, we believe it is important to recognize that when he was assigned as CAU Unit Chief in November 2004 and Rogers became the Assistant Section Chief of the CXS (which oversaw the CAU), Youssef inherited the improper practices initiated during Rogers's tenure, including the use of exigent letters and other informal methods such

---

[254] Rogers retired from the FBI in 2006.

as sneak peeks for requesting records from the on-site communications service providers. Moreover, as described in Chapter Two, the CAU's use of exigent letters was expressly approved by Rogers in an EC to CAU personnel dated November 18, 2003.[255]

We also found that when Youssef first came to the CAU in November 2004 and continuing thereafter, Rogers did not adequately brief Youssef about the CAU practices. Youssef stated that Rogers "bypass[ed]" him on e-mails, meetings, and other information relating to the CAU operations. Youssef also said that Rogers kept him "out of the loop" and that since Rogers was his immediate supervisor until February 2006, Youssef was not able to raise concerns he had about how the CAU was being run to Rogers because Rogers was not willing to listen to his suggestions. Youssef stated that he had a conversation with Rogers, shortly after learning about the use of exigent letters, in which Youssef raised concerns about the practice. Youssef stated that Rogers told him to continue using the letters, and Youssef said he concluded that he would be insubordinate if he failed to do so.

Youssef also asserted that he was subjected to an "incredibly hostile work environment" from his chain of command above Rogers. As noted in Chapter Four, Youssef asserted that both CXS Section Chief Laurie Bennett and CTD DAD John Lewis were hostile to him and that he could not raise any concerns to them about exigent letters.[256]

---

[255] As also described in Chapter Two, the previous CAU Acting Unit Chief had approved an EC dated January 6, 2003, distributed to FBI divisions which stated that the CAU could obtain telephone records in "exigent circumstances" and that legal process must follow such requests. This EC did not explicitly refer to exigent letters.

[256] After reviewing a draft of this report, Youssef's attorney reiterated that Youssef felt he was subjected to a hostile working environment. Youssef's attorney also stated that because of a Title VII lawsuit Youssef filed against the FBI, he was involuntarily transferred to the position of CAU Unit Chief and that many of the CAU supervisors and staff shunned him and preferred to deal directly with Rogers. As noted here and in Chapter Four, the OIG took into account Youssef's work environment in assessing his performance.

Youssef's attorney made many other comments after reviewing a draft of this report. We do not address all of his comments, but respond to some of the most significant ones in this report.

We confirmed that Youssef was not included on some e-mails between Rogers and the Assistant General Counsel between November 2004 and February 2005.[257]

With regard to Youssef's claim that Rogers bypassed him, Rogers acknowledged to us that he had very little interaction with Youssef when Youssef became the CAU Unit Chief, and that Rogers never provided Youssef with any guidance on matters involving the CAU, including exigent letters. Rogers said:

> I didn't give him any briefings. He didn't ask for any . . . . He never came to me for advice . . . . The most contact I had with him was he was constantly e-mailing me to get his admin leave approved for his lawsuit. And that was the majority of my interaction with him.

Rogers also said that he had recommended to the CXS Section Chief that Youssef should not be selected for the CAU Unit Chief position because Rogers did not think that he "had enough experience or understanding of what [the CAU] did."

It is clear from the evidence that Rogers did not interact with Youssef or value Youssef's input into the CAU operations. We believe Rogers should have risen above his disagreement about Youssef's selection and ensured that, working together, they managed the unit appropriately.

It is important to recognize that soon after Youssef became the CAU Unit Chief he learned about exigent letters, that NSLB attorneys were aware of the CAU's practice of using exigent letters, and that the NSLB attorneys were working with CAU personnel on a process for issuing after-the-fact NSLs more expeditiously. In addition, Youssef took steps to address the backlogged requests for legal process. For example, in approximately April 2005, after learning from a Company B employee about the backlog of legal process owed to that provider, he instructed CAU personnel to obtain the

---

[257] We found that Youssef did not attend two important meetings with Rogers and NSLB attorneys that were held on January 6, 2005, and January 26, 2005. After reviewing a draft of this report, Youssef's attorney stated that Youssef was "excluded" from or "not invited" to these meetings. However, Youssef told us that he knew about the meetings before they were held. Youssef's attorney stated that Youssef could not attend them because he was on sick leave in one case and at a deposition in his Title VII case in the other. FBI e-mails and documents also reflect that Youssef was invited to these meetings but did not attend. Youssef acknowledged that he made no effort afterwards to learn what had occurred at these meetings.

necessary process for Company B. In October 2005 he instructed CAU personnel to ensure that all outstanding requests for records from all three providers were covered by legal process. Also in the fall of 2005, he worked with the FBI OGC and representatives of the CTD operational units to reduce the number of future records requests made prior to service of legal process.[258]

Yet, although Youssef inherited the CAU's exigent letters practice, and NSLB attorneys condoned the use of exigent letters and after-the-fact legal process, we nonetheless found that, in several respects, Youssef's actions contributed to the CAU's continued use of exigent letters and other informal requests for telephone records.

First, Youssef failed to understand fully or adequately assess (in coordination with CTD management and the NSLB) all of the methods by which FBI personnel were obtaining records from the on-site providers. Even though he was in charge of the CAU, Youssef did not understand the scope of the exigent letter practice in his unit, including the routine use of after-the-fact legal process and the other improper practices within the CAU for obtaining telephone records. For instance, Youssef told us that apart from two large counterterrorism operations in 2006, he was unaware that during his tenure CAU employees had obtained records or calling activity information for over 1,000 telephone numbers prior to service of either legal process or exigent letters. In addition, Youssef told us he could not approximate how many exigent letters were issued by CAU personnel over

---

[258] In response to a draft of this report, Youssef's attorney stated that Youssef also requested guidance from the FBI OGC regarding what constituted exigent circumstances, and that this request prompted the Assistant General Counsel's April 26, 2005, e-mail (in which she advised Youssef that exigent letters should be used "only if it is clear to you that the requestor cannot await an NSL"). Yet, we determined through contemporaneous e-mails that the Assistant General Counsel's e-mail was prompted by information she had received from another Headquarters Unit, not from any request for guidance from Youssef.

Youssef's attorney also asserted that Youssef's actions in circulating this e-mail to CAU personnel "were the first actions taken by any FBI manager, Unit Chief and/or employee of the [FBI] OGC to provide the CAU employees instruction" as to when an exigent letter could be used. We note that the Assistant General Counsel wrote in her e-mail to Youssef, "please make sure the people in your unit are instructed to ask for an NSL, and only if it is clear to you that the requestor cannot await an NSL . . . should they be done as emergencies based on your exigent letter." Thus, while we agree that Youssef acted appropriately in following the Assistant General Counsel's advice to instruct CAU personnel, it appears that the first action prompting the instruction was taken by the Assistant General Counsel, not by Youssef.

his own name as Unit Chief (we found that the number was 367). Youssef also told us that he was unaware of the details of the CAU requests for community of interest [redacted] sneak peek requests, hot number [redacted] and the unauthorized use of administrative subpoenas.

Second, like his predecessor Rogers, Youssef failed to establish an adequate tracking system for exigent letters and other means by which FBI personnel requested records from the on-site providers. Although Youssef took steps in April and October 2005 to determine the scope of the backlogged requests for legal process, he did not seek to maintain an accurate record at the time they were made of the nature, number, and origin of the requests to the on-site providers whether communicated by exigent letter, by telephone, by e-mail, on pieces of paper, or through sneak peeks. The failure to maintain such records was an internal control problem that greatly complicated the FBI's later efforts to determine whether it had a basis to retain the records.

Third, Youssef himself signed one exigent letter issued to Company A on November 21, 2005, that contained an inaccurate statement. Like virtually all other exigent letters signed by CAU personnel, this letter stated that a grand jury subpoena had been requested from the U.S. Attorney's Office. This was not true. When we showed Youssef this letter, he said that when a CAU Intelligence Analyst presented the letter to him for signature he did not recall noticing that the letter referred to a subpoena rather than an NSL. Youssef acknowledged that the follow-up legal process subsequently issued to cover the numbers in the exigent letter was an NSL. He added that he had not "closely" read the exigent letter before he signed it. Youssef told us that he should have read the exigent letter more closely, adding that he "signed this without really looking at it . . . because at that time I was aware that that is the procedure in the unit." We concluded that even if Youssef believed that exigent letters were "the procedure in the unit," his failure to review any exigent letter between March 2005 (when he first learned they were used) until November 2005 was troubling.[259]

---

[259] After reviewing a draft of this report, Youssef's attorney asserted that Youssef had to sign this exigent letter because the circumstance was a true emergency, the statement about a grand jury subpoena to follow was simply a "placeholder" meaning that some legal process would follow, and that it would have harmed the national security for Youssef to take the time to determine whether the letter accurately stated that a grand jury subpoena would follow. However, Youssef could have easily and quickly ensured the letter's accuracy by revising it to state that legal process would follow. In addition, he could have ensured that the letter was accurate, either before or after he signed it. Rather his testimony was that he did not carefully review the letter and did not notice it referred to a grand jury subpoena before signing it. Finally, we note that 367 exigent letters were signed (Cont'd.)

Fourth, we found that Youssef did not adequately inform the Assistant General Counsel that CAU personnel were having difficulty obtaining legal process to address the backlog of record requests about which he was aware. As described in Chapter Four of this report, Youssef told us that he emphasized at the September 26, 2005, meeting with NSLB attorneys and managers of a CTD operational unit that the CAU was attempting to address the "significant backlog" of NSLs owed to the providers. However, in late 2005 and early 2006 when the Assistant General Counsel asked Youssef what the NSLB could do to assist the CAU to ensure the NSLs were issued in a timely manner, Youssef replied that the CAU was "making some reasonable headway in getting NSLs" and that the on-site providers were "happy with the results." These comments did not address the problem of the significant backlog of several hundred telephone numbers for which promised legal process had not been issued. Youssef did not at this time, or later, advise the Assistant General Counsel of the scope of this backlog or that the CAU was having difficulty obtaining after-the-fact legal process to address the backlog.

By not making clear to the NSLB that the CAU was having significant difficulty in obtaining after-the-fact NSLs, Youssef contributed to an inaccurate perception that the CAU had the exigent letter matter under control. Because the NSLB was not informed of the full scope of the problems, it did not provide additional resources or issue more urgent directives in coordination with CTD officials to establish clear timetables and oversight mechanisms to address the problem. While we believe that NSLB attorneys were very slow in recognizing and correcting the core legal problem with exigent letters, we also believe Youssef's understatement of the problem contributed to the NSLB's lack of urgency in addressing the exigent letters situation.[260]

---

by the CAU staff under his name, and he did not attempt to verify that the representations in the letter were accurate.

[260] In response to reviewing a draft of this report, Youssef's attorney stated that Youssef had requested help from the FBI OGC to force the operational units to open preliminary investigations prior to the CAU requesting records from the on-site providers, but that the FBI OGC refused his request. Youssef's attorney cited two e-mails, dated April 5 and 12, 2005, written by the Assistant General Counsel. According to Youssef's attorney, Youssef's request to the FBI OGC to force the operational units to open preliminary investigations, if accepted, would have "struck at the root cause of the exigent letter[s] problem."

However, the April 5 and April 12 e-mails related to the umbrella preliminary investigative file plan that the NSLB had proposed in January 2005. In his OIG interviews, Youssef also portrayed the preliminary investigation suggestion as the FBI OGC's idea, not (Cont'd.)

As discussed above, Youssef also asserted that he was subjected to a hostile working environment from his chain of command above Rogers. However, we believe that if Youssef concluded that it would be futile to raise concerns about exigent letters with Rogers or others in the CTD chain of command, Youssef could have, and should have, raised these concerns with other FBI managers. He also could have taken the concerns he said he had in 2005 about the use of exigent letters to the FBI's Inspection Division, the FBI's Office of Professional Responsibility, the OIG, or the Department of Justice.

In sum, we recognize that Youssef was placed in a difficult position when he became the Unit Chief of the CAU because the use of exigent letters and other informal means for obtaining telephone records and other ECPA-protected information from the on-site providers had been ongoing for several years. In addition, Rogers, who was the CAU's former Unit Chief and who became Youssef's first-line supervisor, did not adequately brief Youssef about the CAU practices and did not in other ways interact appropriately with Youssef. We found that Youssef took some steps to attempt to address the use of exigent letters. However, we concluded that Youssef did not do all he could have, and should have, to address the improper use of exigent letters and other informal requests for telephone records.

C. NSLB Deputy General Counsel Julie Thomas

As summarized in Chapter Two of this report, we found that many of the improper practices described in this report pre-dated Julie Thomas's appointment in October 2004 as Deputy General Counsel of the FBI OGC's National Security Law Branch (NSLB). Before Thomas's appointment, CAU personnel had been regularly issuing exigent letters, and CAU Unit Chief Rogers had formally recognized exigent letters as an approved method for getting records from the on-site providers without first serving legal process.

---

his. Moreover, as described in Chapter Four, the umbrella plan was dropped because Youssef informed the FBI OGC months later at a meeting on September 26, 2005, that umbrella files were not needed because emergency requests for records in cases where there was no case already open 'were few and far between." Therefore, Youssef's testimony does not support the assertion that forcing the operational units to open preliminary investigations would have solved the "root cause" of the exigent letters problem, or that the FBI OGC refused his request to get the operational units to open preliminary investigations.

However, we found that after Thomas became the NSLB Deputy General Counsel and became aware of exigent letters, she did not adequately review and assess the legality of their use in a timely fashion, halt their use, ensure in coordination with CTD officials that CAU personnel understood the lawful methods for obtaining records from the on-site communications service providers, or ensure that the NSLs that she personally signed complied with the ECPA NSL statute.

As NSLB Deputy General Counsel, Thomas served as the principal legal adviser to the FBI General Counsel on FBI national security issues. After the September 11 attacks, the NSLB grew from a small unit of approximately 10 employees to a full branch within the FBI OGC consisting of 6 units staffed by over 70 attorneys, Special Agents, and support personnel. The NSLB's mission was to provide legal support throughout the FBI, including to the Counterterrorism, Counterintelligence, and Cyber Divisions, by advising on legal issues related to national security matters, ensuring an efficient and timely process for seeking FISA warrants, developing and maintaining liaison relationships within the Intelligence Community, and providing legal training on national security issues to FBI employees.

Yet, beginning in December 2004 when the Assistant General Counsel first informed Thomas about a "form letter" the CAU was using to obtain records in advance of legal process, Thomas failed to directly address the fact that these letters violated the ECPA. Even though she recognized that there were only two authorities by which the FBI could obtain ECPA records in national security investigations (pursuant to legal process or the emergency voluntary disclosure statute), Thomas did not take prompt, decisive action in December 2004 when she learned that (1) the CAU was regularly obtaining records from the on-site providers by using a form letter that promised future legal process, and (2) the CAU was having difficulty obtaining after-the-fact legal process from Headquarters' operating units and FBI field divisions regarding the records it already had received from the on-site providers.

In particular, Thomas did not ask to review the exigent letter; did not direct the Assistant General Counsel or anyone else to review the exigent letter; did not ensure that CAU personnel were trained on the lawful methods for obtaining telephone records; did not review the FBI's contracts with the three on-site communications service providers (or the underlying contract proposals and other documents) until after the FBI received a draft of the OIG's first NSL report; and did not determine if the CAU had issued any guidance to its employees about the appropriate and legal way for FBI personnel to request records from the on-site providers. Instead, Thomas approved a recommendation from the Assistant General Counsel in January 2005 that NSLB personnel be made available to the CAU to help get NSLs

signed quickly after the FBI acquired records from the on-site providers in emergency situations.

We concluded that after Thomas was given notice in December 2004 that exigent letters with the promise of future legal process were being used to obtain ECPA-protected records, at a minimum she should have asked an NSLB attorney to fully and promptly review with CTD's senior managers the methods and practices used by CAU personnel to request and obtain records from the on-site providers so that NSLB could determine if they were legal. A careful review would also have revealed the additional improper practices arising from the FBI's interactions with the on-site providers, such as requesting records without legal process or even exigent letters, sneak peeks, hot number [redacted] and the use of administrative subpoenas signed by a CAU SSA.

In evaluating Thomas's performance, we recognize that CAU personnel also failed to provide information to the NSLB that they should have known was relevant to the NSLB's legal oversight. In particular, as discussed above, CAU Unit Chief Youssef did not adequately advise the NSLB on the extent of the backlog and the ongoing difficulties CAU personnel were encountering in getting after-the-fact NSLs issued by field and Headquarters divisions. These omissions affected Thomas's ability to fully appreciate the scope of the CAU's various problems resulting from its use of exigent letters and other improper methods to obtain telephone records.

Similarly, CAU personnel did not inform Thomas or other FBI attorneys that the CAU routinely obtained ECPA-protected information from the on-site providers by using sneak peeks. Moreover, even after FBI OGC attorneys first were told by the CAU Primary Relief Supervisor about sneak peeks in February 2007, they were not informed of the extent of the information given to CAU personnel in response to such requests. As late as 2007, when the Assistant General Counsel asked CAU personnel to prepare a memorandum reporting as possible intelligence violations the improper blanket NSLs she then knew about, the CAU personnel involved in the drafting effort failed to provide accurate and complete information to the NSLB about the 11 blanket NSLs that had been drafted by CAU personnel and signed by senior CTD officials.

Yet, we believe that these deficiencies in reporting these issues to the NSLB do not excuse Thomas's failure to take adequate action with the information she did have. At critical junctures throughout 2005 and 2006, when Thomas learned more about the CAU's various practices for obtaining records from the on-site providers, she did not take timely, decisive, and effective actions to ensure that the CAU obtained records from the on-site

providers only in accordance with the ECPA and ensure that the use of exigent letters and after-the-fact NSLs was halted.

For example, after the Assistant General Counsel informed Thomas in an e-mail in April 2005 that the CAU may be handling requests from the on-site providers for records as if they were emergencies when some of the requests "were not necessarily emergencies," Thomas did not correct inaccurate guidance that the Assistant General Counsel had given to the CAU: that the CAU could continue to use exigent letters "only if it is clear to you that the requestor cannot await an NSL." As described in Chapters Four and Six of this report, this advice was inaccurate because even if the exigent letter was construed as seeking voluntary production pursuant to Section 2702, the advice would allow use of the letter in circumstances that did not meet Section 2702's definition of emergency circumstances.

Thomas told us that she did not recall receiving the Assistant General Counsel's April 2005 e-mail, but after reviewing the e-mail in August 2008 she said it was consistent with her understanding of the advice that the NSLB was providing the CAU in 2005. Thomas said she understood that the Assistant General Counsel's advice was "shorthand" for the "true emergency" standard in the emergency voluntary disclosure statute (18 U.S.C. § 2702(c)(4)). However, as described above we do not believe it is reasonable to equate the words "the requestor cannot await an NSL" with the "danger of death or serious physical injury" standard in Section 2702. More significantly, FBI General Counsel Valerie Caproni and the Assistant General Counsel stated unequivocally that the FBI did not rely on that statutory authority in approving the use of exigent letters. We concluded that Thomas's recollection was mistaken and that 18 U.S.C. § 2702(c)(4) was not relied upon by the NSLB during the period that the CAU issued exigent letters.

In August 2005, Thomas missed another opportunity to correct some of the CAU's improper practices when she failed to recognize that the emergency voluntary disclosure statute could be used to address some of the emergency requests coming to the CAU. At that time Thomas approved FBI-wide guidance issued by the FBI General Counsel for obtaining the content of communications pursuant to the ECPA emergency voluntary disclosure provision. The new guidance reiterated the requirements of the provision and specifically highlighted that since the disclosure was voluntary it "should not be followed with a subpoena or other compulsory process." Yet, even as she reviewed and approved new FBI policy for using this emergency authority under 18 U.S.C. § 2702(b)(8) for obtaining communications covered by the ECPA, Thomas failed to recognize a connection between a similar emergency disclosure provision under 18 U.S.C § 2702(c)(4) relating to toll billing records under the ECPA and how that authority related to the exigent letters practice. She again failed to halt

the use of exigent letters – which improperly combined a request for voluntary production with a promise of future compulsory process – and she also failed to identify the emergency voluntary disclosure statute as an appropriate alternative to exigent letters in qualifying emergencies.

In June 2006, when Thomas received an e-mail informing her that the Assistant General Counsel had sent a new version of a model exigent letter to the CAU in May 2006, Thomas again allowed the practice of using exigent letters to continue. The new version of the exigent letter promised that NSLs (rather than grand jury subpoenas) would be issued in the future. While the revised model exigent letter corrected an inaccurate statement in the exigent letter about grand jury subpoenas, the revised letter still did not ensure compliance with the ECPA's requirements that either (1) the FBI issue legal process in advance of obtaining records; or (2) the provider produce records voluntarily in circumstances satisfying Section 2702's emergency voluntary disclosure provision. Consequently, the revised exigent letter did not resolve the fundamental legal problem with the letters under the ECPA.

In addition, we found that Thomas herself signed seven after-the-fact NSLs in 2005. The ECPA does not authorize the issuance of retroactive legal process, and such process would not validate an improper disclosure of records under the ECPA. The NSLs and approval ECs also did not state that the FBI had already acquired the records.

In evaluating Thomas's overall performance we recognized that she was also assigned to provide legal counsel to support many high-profile threats that the FBI addressed during the period covered by our review. Thomas told us that she regularly was involved with "the most emergent issues that face the intelligence community." She said she routinely dealt with "life and death situations" that required immediate attention. Thomas also said that soon after she was appointed NSLB Deputy General Counsel in the fall of 2004, she "came to believe that the span of control of this branch was beyond the capabilities of any human being." She said that starting in December 2004 she had requested that Section Chief positions be established in the NSLB to assist her, but that this did not occur until January or February 2008.

Yet, taking all these circumstances into account, we believe Thomas inappropriately approved the use of the exigent letters practice and after-the-fact NSLs, did not promptly review an exigent letter or direct another attorney to review one, did not review the providers' contracts and

associated documents, repeatedly missed opportunities to halt the use of exigent letters, did not work with CTD managers to ensure CAU personnel were properly instructed on the FBI's authorities to obtain telephone records from the on-site providers, and signed improper after-the-fact NSLs.[261]

D. NSLB Assistant General Counsel

As described in this report, the NSLB Assistant General Counsel had the most frequent contact with CAU personnel regarding exigent letters. She was an FBI senior line attorney who was the NSLB point-of-contact for NSL-related policies and issues. In that position, she was consulted when field and Headquarters personnel, including Chief Division Counsels, had questions about NSLs. She also was responsible for drafting NSL guidance, preparing or overseeing the preparation of NSL training materials, preparing congressionally mandated reports to Congress on NSL usage, and evaluating the need for legislative amendments to the FBI's NSL authorities.

We determined that in December 2004, in connection with a request for an after-the-fact NSL from a CAU SSA, the Assistant General Counsel first learned that the CAU regularly used exigent letters to obtain telephone records, that these exigent letters promised after-the-fact legal process, that the CAU relied on field divisions to supply the after-the-fact legal process, and that the field divisions often did not respond to the CAU's requests for after-the-fact legal process. In response, the Assistant General Counsel promptly and appropriately notified her immediate supervisor and NSLB Deputy General Counsel Thomas about this information. We also found that she consistently kept both her immediate supervisor and Thomas informed about her interactions with the CAU concerning exigent letters and the problems the CAU was encountering in obtaining legal process after the exigent letters were issued. She also periodically advised CAU Unit Chief Youssef that she and the NSLB were available to assist the CAU in working through exigent letters problems by making NSLB resources available to assist with promptly drafting after-the-fact NSLs.

Yet, while the Assistant General Counsel generally kept her supervisors informed of what she learned on a timely basis, she provided inaccurate guidance to Youssef that "we are willing to allow these requests when there really are exigent circumstances . . . only if it is clear . . . that the requestor cannot await an NSL." She also recommended to NSLB Deputy General Counsel Thomas that the NSLB designate attorneys to

---

[261] Thomas resigned from the FBI in December 2008.

assist the CAU in preparing after-the-fact NSLs more expeditiously and over a period of nearly 9 months worked on a proposal to create "umbrella files" – generic national security investigations of recurring threats – that could be used to document in NSL approval ECs the predication for NSLs (until she was informed that the umbrella files were not needed). When we asked her how she justified the use of exigent letters that promised future legal process, the Assistant General Counsel told us that the FBI had "created an exception [to the ECPA statute] in national security circumstances where we think it's absolutely necessary." However, the ECPA does not provide for such an exception.

We were also troubled the Assistant General Counsel did not seek to review a copy of any exigent letter until May 2006, more than 18 months after first learning of their use in the CAU. We believe she should have asked to see an exigent letter upon hearing of its use.

Even after reviewing an exigent letter, she did not recognize that the CAU was obtaining records in violation of the ECPA. Instead of recommending that their use be halted, in May 2006 she merely revised the exigent letter to substitute the term "NSL" for the inaccurate reference to after-the-fact issuance of grand jury subpoenas, and she advised the CAU that it could continue to use the revised exigent letter. By these actions, she allowed the FBI's improper use of exigent letters and after-the-fact NSLs to continue. However, it is also important to note that she forwarded the revised exigent letter to both her supervisor and Thomas, and that neither of these supervisors objected to the Assistant General Counsel's changes or otherwise questioned the CAU's continued use of exigent letters.

Finally, we believe the Assistant General Counsel should have recognized that many of the exigent requests that came to the CAU qualified for emergency voluntary disclosure requests under the ECPA. Yet, like her immediate supervisor and NSLB Deputy General Counsel Thomas, the Assistant General Counsel did not ensure that CAU personnel were briefed about the circumstances in which the FBI could lawfully request voluntary disclosure without legal process.

In sum, we concluded that based on the Assistant General Counsel's experience in national security investigations and the position she held in the NSLB, she should have directly confronted the legal deficiencies in use of exigent letters and, through her supervisors in the NSLB and in conjunction with CTD managers, ensured that the use of exigent letters ended, which she did not do.

E. General Counsel Valerie Caproni

We examined the involvement of FBI General Counsel Valerie Caproni in the handling of exigent letters and determined that she first learned about the CAU's use of exigent letters or other improper requests for telephone records in late 2006, during the OIG's first NSL investigation.

The only evidence that Caproni was told anything prior to this time that related to the CAU obtaining records before service of legal process was a conversation that Thomas said she had with Caproni in April 2005 when Thomas was preparing for the FBI Inspection Division's triennial inspection of the FBI OGC. Thomas said she discussed with Caproni at the time that the NSLB "had a problem delivering legal services" and that "[CAU personnel] were requesting NSLs for records they had already received." Thomas said she raised the question to Caproni whether these after-the-fact NSLs should be reported as possible intelligence violations to the President's Intelligence Oversight Board. Thomas said that Caproni agreed with Thomas's assessment that "these were likely all emergency circumstances anyway and a follow-on NSL would not be required."[262]

We concluded that the information Thomas recalled sharing with Caproni was not of sufficient detail to put Caproni on notice that the CAU was obtaining records from the on-site providers with a promise of future legal process. We found no evidence that Thomas informed Caproni that the CAU was obtaining records using a letter that promised future service of legal process.

Rather, Caproni first learned about the use of exigent letters in 2006 in response to the FBI Director's request that she assess whether the FBI anticipated any problems with the OIG's first NSL investigation that was ongoing at the time. Caproni asked the Assistant General Counsel in an e-mail whether, in light of the Assistant General Counsel's recent OIG interview, she anticipated "any problems/issues/concerns." In a reply on June 1, 2006, the Assistant General Counsel wrote:

> in emergency situations . . . we have allowed CAU to get NSL information from the [e]mbedded telephone companies based upon a letter promising a legally compelling process to be forthcoming, and then the NSL is supposed to be issued . . . .

---

[262] However, as we discuss in Chapter Four of this report, Caproni told us in earlier interviews when we asked her if the FBI had been relying on the emergency voluntary disclosure statute in approving the use of exigent letters, "no, we had no discussions that these [exigent letter requests] – would qualify under that provision of the ECPA."

> There had been some problems with the promptness or lack thereof of those NSLs, as well as figuring out a [preliminary investigation] to which to attach the NSL request. I think the problem is resolved now but we still allow the receipt of info without an actual NSL prior to the receipt. It is analogous to the 2702(d) emergency but we have never premised it on that.

On July 20, 2006, NSLB Deputy General Counsel Thomas forwarded to Caproni another e-mail from the Assistant General Counsel in which the Assistant General Counsel reported that she had been asked in a recent OIG interview about the CAU's practice of issuing exigent letters "in emergency situations to get NSL information." Thomas stated in her forwarding e-mail, "[w]e have done better with this [issuing NSLs prior to requests for records] but when we are sitting right next to the rep. its tough to wait the 2-3 days it takes to get" the NSL. Caproni responded to Thomas, "I think we've always done some 'paperwork to follow' requests."[263]

However, Caproni said she did not see an exigent letter and was unaware of the extent to which the FBI was using exigent letters before the OIG showed her an exigent letter and informed her of the details of the practice in late 2006 in connection with the OIG's interview of her in our first NSL investigation.

We concluded that the two e-mails described above did not alert Caproni of the extent of the problem and in fact suggested that the problem had been "resolved." Moreover, by the time Caproni received these e-mails the OIG investigation was ongoing within the FBI and the issuance of exigent letters had all but stopped. Under these circumstances, we do not believe she was on sufficient notice of the problem, in advance of the OIG investigation, to remedy it.

---

[263] When the OIG asked Caproni about her reference to the FBI always doing "paperwork to follow" requests, Caproni stated that when she was an Assistant United States Attorney there were instances in which records were obtained prior to the service of legal process. Caproni told us, "in my experience it is not a particularly unusual circumstance to do a paperwork-to-follow request," as long as the process comes within "a day, or . . . maybe you are going to get the records on Saturday and you are going to give them the process on Monday." Caproni added that when she was told about the CAU obtaining records prior to process, "[i]t did not surprise me or shock me," noting, however, that she believed at the time that legal process was served within a day or two. Caproni distinguished her prior experience from the sort of delays that she learned were occurring in the CAU.

F. Signers of the 11 Blanket NSLs: Joseph Billy, Jr., Arthur Cummings III, Michael Heimbach, and Jennifer Smith Love

As described in Chapter Four of this report, we found that 4 senior CTD officials signed a total of 11 improper blanket NSLs in 2006. Each of these NSLs had multiple deficiencies.

We analyze below the actions of the four CTD senior officials who signed these improper blanket NSLs.

1. Joseph Billy, Jr.

Joseph Billy, Jr., joined the FBI in 1978. By mid-2006, Billy had been assigned to FBI national security investigations for about 20 years.

Billy signed 4 of the 11 improper blanket NSLs: the Company B May 12 NSL and 3 Operation Z NSLs. He signed the Company B May 12 NSL when he was a CTD Deputy Assistant Director and the three Operation Z NSLs as an Assistant Director. In both of these positions, Billy was authorized to sign NSLs by virtue of the FBI Director's delegation of NSL signature authority to Deputy Assistant Directors and Assistant Directors of the Counterterrorism Division.

However, all four NSLs were deficient. The Company B NSL violated the ECPA because (1) it included telephone numbers relevant to closed investigations and records that were relevant to domestic terrorism and criminal investigations for which NSLs are not an authorized technique under the Attorney General's NSI Guidelines; and (2) did not contain the certifications required for NSLs imposing non-disclosure and confidentiality requirements on NSL recipients.

The Company B May 12 NSL and the three Operation Z NSLs also violated FBI policy because they were not accompanied by approval ECs. Approval ECs are required in order to document that the records sought are relevant to an authorized national security investigation.

Finally, all four NSLs were issued after-the-fact, and none of the NSLs disclosed that they were issued for records that had been previously obtained through exigent letters.

Billy told us that he did not recall signing the Company B May 12 blanket NSL or the three Operation Z NSLs, but he did not contest that his signature was on all four NSLs. Further, although he told us that he knew that NSLs were only authorized in instances in which there was an open preliminary or full national security investigation, the Company B May 12 NSL included telephone numbers related to closed cases and domestic

terrorism and criminal investigations for which NSLs are not authorized. Additionally, Billy told us that signing NSLs that were not accompanied by approval ECs was "completely outside" his practice. However, we confirmed with the CAU SSAs who drafted the four blanket NSLs that Billy signed that none of these four NSLs were accompanied by approval ECs. While we developed no evidence contradicting Billy's assertion that his normal practice was to sign NSLs only if they were accompanied by approval ECs, these four NSLs were not issued with the required approval ECs.

We concluded that in signing these four NSLs, Billy failed to take appropriate steps to ensure that NSLs he signed complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. When Billy signed these NSLs he had nearly 20 years of experience with FBI national security investigations, and he knew the legal and policy requirements for using this intelligence tool. Yet, he signed these NSLs either without the required certifications or without ensuring that the requests were adequately predicated under the ECPA by examining the approval ECs.[264]

2. Arthur A. Cummings III

Arthur A. Cummings III joined the FBI in 1987. By mid-2006, Cummings had worked on FBI national security investigations for about 14 years.

Cummings signed 5 of the 11 improper blanket NSLs, all of which related to Operation Y. He signed these NSLs as a Special Agent in Charge (SAC) for the Washington Field Office while he was temporarily assigned to the CTD as an Acting DAD. As a SAC, Cummings was authorized to sign NSLs by the FBI Director's delegation pursuant to 18 U.S.C. § 2704(b).

All of the Operation Y NSLs were deficient. These NSLs were issued after-the-fact, although the ECPA does not authorize after-the-fact process. In addition, they did not contain the certifications required for NSLs imposing non-disclosure and confidentiality requirements on NSL recipients. These NSLs also violated FBI policy because they were not accompanied by approval ECs. Finally, all five NSLs were issued after-the-fact but none of the NSLs disclosed that they were issued for records that had been previously obtained through exigent letters and other informal requests.

---

[264] Billy retired from the FBI in March 2008.

Cummings said that prior to signing any of the NSLs, he had spoken with an NSLB attorney to determine if he was authorized to sign NSLs while serving as an Acting DAD in the CTD on temporary assignment. An NSLB attorney confirmed to us that she advised Cummings that he could sign NSLs in his position as a SAC.

Cummings also told us that he recalled signing the Company C August 24 and Company A August 25 Operation Y blanket NSLs, which included many telephone numbers, but he did not recall signing the other three Operation Y blanket NSLs. Cummings said he believed that each of the NSLs he signed had approval ECs because it was his practice to ensure that NSLs always had approval ECs. However, we confirmed with the CAU SSA who drafted the NSLs that approval ECs were not prepared for any of the five Operation Y blanket NSLs. Accordingly, we determined that Cummings was mistaken in his belief that all the NSLs he signed were accompanied by approval ECs.

We concluded that by signing these NSLs Cummings failed to take appropriate steps to ensure that the NSLs complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. When Cummings signed these NSLs, he had about 14 years experience in conducting FBI national security investigations, yet he failed to ensure that the requests were adequately predicated under the ECPA by examining the approval ECs.

3. Michael Heimbach

Michael Heimbach joined the FBI in 1988. By mid-2006, Heimbach had been assigned to FBI national security investigations for more than 3 years.

Heimbach signed the Company C July 5 blanket NSL. Heimbach signed this NSL when he was a Section Chief of the International Terrorism Operations Section 1 of the CTD, but while temporarily assigned as an Acting DAD for the CTD. Similar to the Company B May 12 NSL signed by Billy, this NSL violated the ECPA because it (1) included telephone numbers relevant to closed investigations and records that were relevant to domestic terrorism and criminal investigations for which NSLs are not an authorized technique under the Attorney General's NSI Guidelines; and (2) did not contain the certifications required for NSLs imposing non-disclosure and confidentiality requirements on NSL recipients. Additionally, this NSL violated FBI policy because it was not accompanied by an approval EC. As mentioned previously, approval ECs are required in order to document that the records sought are relevant to an authorized national security investigation.

Finally, this NSL was issued after-the-fact, although the ECPA does not authorize retroactive legal process, and did not disclose that it was issued for records that the FBI had been previously obtained through exigent letters.

Heimbach told us that prior to signing the NSL, an NSLB attorney told him that he was authorized to sign the NSL as an Acting DAD. Heimbach also told us that his practice was to require approval ECs to establish and document the predication for the NSL and the relevance of the telephone numbers to an open national security investigation. He stated that he assumed he was told when he signed the Company C July 5 NSL that the approval EC was being prepared or had already been prepared. However, we confirmed with the CAU SSA who prepared the NSL and brought it to Heimbach for signature that an approval EC was never drafted. We therefore concluded that Heimbach was mistaken in his belief that an approval EC was being prepared or had already been prepared.

We concluded that by signing this NSL Heimbach failed to take appropriate steps to ensure that he complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. When Heimbach signed this NSL, he had over 3 years experience in conducting FBI national security investigations, yet he failed to ensure that the requests were adequately predicated under the ECPA by examining the approval EC.[265]

4. Jennifer Smith Love

Jennifer Smith Love joined the FBI in 1987. By mid-2006, Love had been assigned to FBI national security investigations for about 20 months.

Love signed the Company A September 21 blanket NSL when she was a Section Chief of the Communications Exploitation Section of the CTD but temporarily assigned as an Acting DAD for the CTD. Similar to the Company B May 12 NSL signed by Billy and the Company C July 5 NSL signed by Heimbach, this NSL violated the ECPA because it (1) included telephone numbers relevant to closed investigations and records that were relevant to domestic terrorism and criminal investigations for which NSLs are not an authorized technique under the Attorney General's NSI Guidelines; and (2) did not contain the certifications required for NSLs

---

[265] As noted above in connection with the NSL signed by Heimbach, the FBI did not issue guidance stating that Acting DADs are not authorized to sign NSLs until June 1, 2007. We agree that in the absence of clear written policy on signature authority, Heimbach should not be faulted for signing the NSL while serving as an Acting DAD.

imposing non-disclosure and confidentiality requirements on NSL recipients. Additionally, this NSL violated FBI policy because it was not accompanied by an approval EC.

Finally, this NSL was issued after-the-fact, although the ECPA does not authorize retroactive legal process, and did not disclose that it was issued for records that the FBI had been previously obtained through exigent letters and other informal requests.

Love told us that she recognized her signature on the Company A September 21 NSL, but said she could not recall any details surrounding this NSL, including who gave it to her. She also told us that she did not know that NSLs required approval ECs.

We concluded that by signing this NSL Love failed to take appropriate steps to ensure that she complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. When she signed this NSL Love had about 20 months experience conducting FBI national security investigations. If Love did not know FBI policies regarding the issuance of NSLs – including the requirement that they contain approval ECs – she should not have signed any NSLs and should instead have sought appropriate legal guidance.

5. OIG Conclusion on CTD officials who signed improper blanket NSLs

When Congress amended the Patriot Act in 2001, it significantly expanded the FBI's preexisting authority to issue NSLs. Section 505 of the Patriot Act broadened the FBI's NSL authority by eliminating the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power. This section of the Patriot Act substituted the lower threshold that the information sought must be relevant to an authorized investigation to protect against international terrorism or espionage, provided that any investigation of a U.S. person is not conducted "solely on the basis of activities protected by the first amendment of the Constitution of the United States." As a consequence of this lower threshold, the FBI can obtain information about persons who are not subjects of FBI investigations so long as the requested information is relevant to an authorized national security investigation.

As we described in this chapter, we believe serious, repeated management failures by the FBI's senior leadership, the CTD, and the FBI OGC caused the breakdown in responsibility and accountability for exigent letters, other improper requests, and the attempts at corrective action – such as blanket NSLs. However, we also believe that the CTD senior

individuals who signed these blanket NSLs contributed to misuses of these authorities.

As senior CTD officials, Billy, Cummings, Heimbach, and Love were responsible for ensuring that the NSLs they signed complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. While we recognize that each of these four officials had other significant responsibilities in the FBI and that they each worked in a high-pressure environment in furtherance of the FBI's counterterrorism mission, we believe they should have taken more care to ensure that the NSLs they signed complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy.

G. CAU Personnel Who Signed Exigent Letters

As described in Chapter Two of this report, we determined that many CAU employees – 2 Unit Chiefs, 15 SSAs, and 3 Intelligence Analysts – signed 722 exigent letters issued by the CAU between March 2003 and November 2006. The vast majority of these exigent letters stated:

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

As discussed above, this language came from the New York Field Division where grand jury subpoenas signed by the U.S. Attorney's Office were used to obtain telephone records related to the counterterrorism investigations in response to the September 11 attacks. This practice and the use of exigent letters were adopted by the CAU beginning in 2003.

In evaluating the accountability of the CAU employees who signed these exigent letters, we asked the CAU employees who signed two or more exigent letters whether they knew when they signed the letters that the factual statements were accurate. We asked specifically whether they knew that there were exigent circumstances associated with the requests and whether they knew that requests for grand jury subpoenas had been submitted to the U.S. Attorney's Office, as specifically stated in the letters.

With few exceptions the CAU SSAs who signed the letters said they believed exigent circumstances were present in every instance in which they signed an exigent letter. The only exceptions to these general statements were (1) an SSA who told us that he signed several letters when he was new to the CAU under circumstances he was "pretty sure . . . could be questionable"; (2) another SSA who told us that he sometimes signed

exigent letters presented to him by the CAU Intelligence Analysts without requiring an explanation of the details if he was busy on other projects; and (3) CAU Unit Chief Bassem Youssef and at least two SSAs who told us they did not read the exigent letters closely or in detail, signed it "without looking at it," or "just glanced over it." Nearly all of the SSAs also told us that their primary concern each time they signed an exigent letter was to be responsive to the demand for telephone toll billing records as quickly as possible in order to support critical FBI investigations.

The exigent letters also stated that requests for a specific form of legal process – "subpoenas" – had already been submitted to the U.S. Attorney's Office. In most cases, this was not true. As described in Chapter Four of this report, in most cases the legal process issued after-the-fact to cover exigent letters were NSLs issued by the FBI, not grand jury subpoenas. However, most of the CAU SSAs we interviewed told us they did not know whether grand jury subpoenas had been requested, although some recognized that the letters inaccurately described the process for obtaining grand jury subpoenas.

We sought to determine whether the signers of exigent letters knew whether the statement that requests for grand jury subpoenas had been submitted to the U.S. Attorney's Office was false when they signed the letters. One SSA who signed 139 exigent letters told us that although he recognized that the exigent letters inaccurately stated that grand jury subpoenas had been submitted, he signed the letters nonetheless because he "thought it was all part of the program coming from the phone companies themselves," and he assumed the letters were approved by the communications service providers' attorneys.

Another SSA who signed 115 exigent letters said that he knew that subpoenas had not been issued but signed the exigent letters anyway, because he saw the letter used by other CAU personnel as a standard practice and he received assurances from CAU Unit Chief Glenn Rogers that the exigent letter was okay to use.

A third SSA who signed 98 exigent letters said he was not concerned with the reference to subpoenas having been submitted to the U.S. Attorney's Office, although the language "did not make sense" because it did not correctly reflect the procedure to obtain subpoenas. This SSA said he "didn't really have any reason to question" the letters because the letters were accepted by the providers and were an established practice in the CAU.

When we questioned other SSAs about their signing exigent letters which inaccurately stated that grand jury subpoenas had already been requested from the U.S. Attorney's Office, they said that they did not pay

much attention to and were not concerned about the reference to a grand jury subpoena. Other SSAs told us that when they signed the letters they did not know for sure what type of after-the-fact legal process would be used by the field division or Headquarters unit that initiated the request. Others told us that they considered the reference to grand jury subpoenas to broadly include all categories of legal process, such as NSLs. As noted above, a few SSAs told us that they never read the exigent letters closely enough to notice any of the statements they contained.

As noted above, when we asked CAU Unit Chief and CXS Assistant Section Chief Glenn Rogers why he signed, and permitted his subordinates to sign, exigent letters containing inaccurate statements, he said he regretted the wording of the letter, but that the letters were just a "placeholder." In response to a similar question, Youssef told us he should have read the letter more closely and did not realize that the exigent letters referred to subpoenas rather than NSLs until April or May 2006.[266]

In evaluating the performance of the individual signers of the inaccurate exigent letters, it is also important to consider several mitigating circumstances.

First, CAU Unit Chief Rogers approved the use of exigent letters by the CAU, and in November 2003 Rogers issued an EC to the CAU that referred to the exigent letters as a tool for obtaining telephone toll billing records from Company A, which was the only on-site provider at the time. As described in Chapter Two, three SSAs who signed exigent letters told us that they raised concerns about the wording of exigent letters to their Unit Chief at the time, Glenn Rogers. In each instance, the SSAs said that Rogers assured them that the letter was "standard operating procedure" and had been approved by "lawyers." Rogers also told one SSA that he should not change "a single word" in the letter. Although Rogers told us that he did not recall these SSAs or anyone else coming to him with complaints about the exigent letters, we concluded, based on the consistent testimony of the SSAs, that this had occurred.

Second, CAU personnel were not trained on national security investigations or NSLs when they arrived in the unit until after the OIG's first NSL report was released in March 2007. Rather, newly assigned personnel – most of whom had no prior experience in national security

---

[266] However, after this time period 28 additional exigent letters were signed by other CAU personnel with Youssef's name listed as the CAU Unit Chief, including 15 that continued to refer to grand jury subpoenas having been requested.

investigations – learned the procedures for requesting and obtaining records from the on-site providers' employees and from other CAU personnel.

Third, by late December 2004 NSLB attorneys, including NSLB Deputy General Counsel Thomas, knew that the CAU was obtaining records prior to service of legal process based on a form letter but did not probe the details or terminate the practice. Rather, in January 2005 NSLB attorneys met with Rogers and a CAU SSA to discuss how the NSLB could assist in quickly preparing NSLs after the CAU had obtained records. Thus, CAU personnel believed that the exigent letters had been approved not only by the CAU Unit Chiefs but by the NSLB.

Fourth, the use of exigent letters was widespread and the accepted way of doing business in the CAU. Many CAU SSAs told us that the letters were part of the standard practice used by the CAU. Some SSAs also identified a particular Company A employee as having assured them that the exigent letter practice had been approved by "attorneys," which the SSAs said they interpreted to mean attorneys from both the FBI and Company A.

Fifth, because the CAU was an operational support unit, none of its personnel had authority to sign NSLs. As a result, when CAU personnel issued exigent letters to obtain records from the on-site providers, the CAU generally depended upon the original FBI requesters in field or Headquarters operational units to issue the after-the-fact legal process. Due to the absence of a tracking system for after-the-fact legal process in the CAU, the CAU SSA who signed the exigent letters would not necessarily know what type of legal process was eventually issued or even that the request was eventually covered by the promised legal process. Additionally, due to turnover in the CAU, the CAU employee who signed the exigent letter may have rotated out of the CAU when the after-the-fact legal process was served on the on-site providers weeks, months, or even years later.

Sixth, grand jury subpoenas in fact were subsequently issued to cover some of the exigent letter requests.

Finally, employees of the on-site providers accepted exigent letters as authority for responding to FBI requests and in many instances even drafted the exigent letters. Indeed, as described in Chapter Two of this report, CAU SSAs told us that the providers' employees were sometimes the first to brief them on the exigent letters practice. The role of the on-site providers in explaining, drafting, and accepting the exigent letters, together with the fact that these SSAs saw other personnel in the unit regularly sign and issue the letters, led these SSAs to conclude that signing exigent letters to initiate [redacted] for telephone records was an appropriate business practice within the CAU.

OIG Conclusion on CAU Personnel who Signed Exigent Letters

First, consistent with our standard practice, we referred the evidence that we developed regarding the signing of these inaccurate exigent letters to the Public Integrity Section of the Department's Criminal Division for its determination of whether criminal prosecution was warranted. Upon evaluating the evidence referred by the OIG, the Public Integrity Section declined prosecution for the exigent letters matter.

We agree that the evidence was insufficient to support a criminal prosecution. We also agree that significant mitigating circumstances, described above, must be considered in evaluating the accountability of FBI employees who signed exigent letters. However, we also believe that none of these factors, alone or in combination, excuses an FBI employee for signing an exigent letter either knowing the letter was inaccurate, not making the effort to confirm the factual accuracy of the letter, or not raising concerns about the letter's accuracy to FBI supervisors. Simply put, we do not believe employees of the FBI should sign their names to letters making a statement that is not true, even if the letters are approved by management, sanctioned by FBI attorneys, part of an established practice, or accepted by the recipients. When FBI employees signed exigent letters attesting to the fact that "subpoenas have been submitted to the U.S. Attorney's Office who will process and serve them formally" to the communications service providers, the FBI employees who signed these letters should believe that this is true.

We recognize that a few SSAs raised concerns about the exigent letters to their supervisor, CAU Unit Chief Rogers, and he instructed them to continue using the letters without changing the wording. Even in this circumstance, we believe that FBI employees confronted with this problem had other options than to simply sign the letters. They could have sought further guidance from more senior managers in the FBI, either directly or anonymously. They could have requested guidance from the FBI OGC. They could have complained to a senior CTD official or the FBI Inspection Division. They could have contacted the OIG. None of them took any of these steps. Instead, they continued to sign inaccurate exigent letters. We believe that in signing these inaccurate letters the FBI employees failed to exercise sufficient care to ensure the letters were accurate or raise concerns to others.

However, we also believe Rogers was most culpable for the FBI's improper use of exigent letters. Without consulting CTD supervisors or any FBI attorneys, Rogers took an exigent letter that had been used by the FBI's New York Field Division and authorized its use in the CAU to support a variety of FBI investigations. He signed exigent letters himself and permitted his subordinates to sign hundreds of exigent letters even though

they contained inaccurate statements of fact on their face. In clear derogation of his duties as a supervisor, Rogers also ignored complaints from at least three SSAs in the unit who complained directly to him about the inaccurate reference in the letters to grand jury subpoenas and told them not to change a word. While this does not fully excuse the CAU personnel who signed the letters, it is an important factor to consider when assessing their performance.

H. FBI Personnel Involved in Media Leak Investigations

As described in Chapter Three of this report, FBI personnel were involved with requests to [redacted] reporters' toll billing records in three different media leak investigations without first obtaining the required Attorney General approval. We believe that these matters involved some of the most serious abuses of the FBI's authority to obtain telephone records.

First, we believe that the FBI's overall management failures described in this chapter contributed to the improper [redacted] of reporters' records. The FBI's failure to plan for the co-location of the providers' employees resulted in the CAU's extensive use of exigent letters and after-the-fact legal process beginning in 2003. The failures in planning were compounded by the failure to train CAU personnel on the authorized means to obtain telephone records under the ECPA and on the express limitations on the FBI's authority to compel the production of particular subcategories of telephone records, including subpoenas for reporters' toll billing records. As a result, we found that requests for reporters' toll billing were handled by the CAU SSAs and Intelligence Analysts as routine records requests. When the CAU received these requests, no alarm bells went off and no higher-level supervisors provided any review of these requests. Instead, the CAU SSA and Intelligence Analyst involved in requesting or analyzing the reporters' records obtained by the FBI said they were unaware of any special regulation governing subpoenas for reporters' records.

As described below, however, in addition to these management failures we believe several FBI personnel bore some responsibility for these serious abuses in these media leak investigations.

1. First Matter

In the first media leak investigation described in Chapter Three (concerning classified information about the [redacted] that appeared in Washington Post and New York Times news articles), an FBI case agent exchanged e-mails with a CAU Intelligence Analyst about whether the on-site providers had the capability of retrieving records of [redacted] calling activity. Yet, in the absence of any request from the case

agent or others to actually obtain these records, a CAU SSA issued an exigent letter to an on-site Company A analyst requesting the reporters' records. The exigent letter, which also contained no date restrictions, was issued without the knowledge of the case agent, CTD managers, or any prosecutor. It also was issued without the required Attorney General approval or compliance with Department regulations governing subpoenas of the telephone toll billing records of reporters. We found that the reporters' records were produced to the FBI and uploaded into a [redacted] database, where they remained for over 3 years until the OIG identified the records in connection with this investigation and informed the FBI and the Criminal Division of this fact.

We believe that the CAU SSA's issuance of the December 17, 2004, exigent letter for the reporter's records under these circumstances was a serious performance failure. While exigent letters were routinely used in the CAU during this period, the SSA showed poor judgment in this instance by issuing an exigent letter in the absence of a request from the FBI case agent working on the investigation. The fact that the FBI requested and obtained reporters' records without any FBI supervisor or prosecutor knowing about it reveals the lax, sloppy, and unsupervised manner in which CAU personnel obtained telephone records from the on-site providers. The CAU SSA's explanation for issuing the exigent letter – that he "had never even read the content of these [exigent] letters," but was "just using the standard forms I was provided" – underscores the FBI's failure to train CAU personnel on the proper methods for requesting telephone records, the failure to establish firewalls between FBI personnel and the providers' employees, and the failure to ensure that CTD supervisors and FBI attorneys provided oversight of the CAU's interactions with the providers.[267] The resulting violations of federal regulation and Department policy were made significantly worse because the exigent letter did not even include a date range, and therefore the provider produced records for [redacted] telephone calls to and from reporters, a researcher for The Washington Post, and the 2 news bureaus, with only 3 calls that fell within the time frame the case agent believed to be relevant to the investigation.

We also determined that the CAU Intelligence Analyst who received and analyzed the reporters' records in response to this exigent letter was never instructed about the special rules applicable to subpoenas for obtaining reporters' toll billing records. However, he received at least one e-mail prior to receipt of the records that referenced the case agent's

---

[267] This SSA signed 115 exigent letters, the second highest number of exigent letters signed by CAU personnel.

expectation that a grand jury subpoena would be forthcoming. In his e-mail to the case agent forwarding the responsive records, the Intelligence Analyst even recognized that a grand jury subpoena was still needed.

We also found that the case agent failed to exercise appropriate care and attention to detail. Although a CAU Intelligence Analyst sent an e-mail to the agent on January 5, [redacted] that attached reports containing toll record information for the reporters' telephone numbers, the case agent said he did not open the attachments and did not realize that they included the reporters' toll billing records. In a subsequent e-mail on March 24, [redacted] the CAU Intelligence Analyst reminded the case agent that the January 5 e-mail contained "two products which reflected [Company A] toll records on several of the [redacted] numbers that you have targeted." We believe that if the agent had exercised greater care when he received these e-mails, he would have realized that the analyst had sent him reporters' telephone records without a subpoena and without obtaining Attorney General approval as required.

Moreover, if the case agent had realized he had received the reporters' records and promptly alerted his supervisors, they and the Criminal Division could have undertaken corrective measures in early [redacted] to address the improper collection. Because he failed to do so, the reporters' records remained in the [redacted] database until June 2008, when the OIG notified the FBI of the issue.

Finally, as detailed in Chapter Three, the FBI [redacted] telephone records the FBI had obtained in response to the exigent letter. FBI agents [redacted]

When we notified the FBI leadership in 2008 that we had discovered that the FBI had obtained reporters' telephone records improperly and without required Attorney General approval, the FBI appropriately notified the affected reporters and their newspapers, as required by federal regulation. However, in that notification the FBI did not disclose that the [redacted]

In Chapter Six of this report, we recommend that the FBI assess the information we developed in this review regarding subpoenas and other requests for reporters' telephone records to determine whether administrative or other personnel action is appropriate for the individuals involved. We recommend that the FBI's assessment include a review of the

performance of the CAU SSA who signed the exigent letter, and the case agent who received the records but failed to alert his supervisors or the Assisant United States Attorney (AUSA). In addition, we recommend that the Department re-evaluate the policies governing the [redacted] reporters because of the significant First Amendment interests implicated [redacted] We believe that the FBI cannot [redacted] such as when it is investigating national security threats or the kidnapping of a child, if it [redacted]

2. Second Matter

In the second media leak investigation discussed in Chapter Three, an AUSA (local AUSA) and a federal prosecutor approved two grand jury subpoenas. The FBI case agent had forwarded to the prosecutor for his use in drafting the subpoenas text suggested by an on-site Company A analyst, which included requests [redacted]

When the subpoenas were issued, both the case agent and the prosecutor knew that the target numbers had been in telephonic contact with a reporter during the time period specified in the subpoenas. As a result, if Company A fully responded to the subpoenas, the responsive records would include [redacted] but also the telephone records of reporters [redacted] Yet, in the absence of Attorney General approval or compliance with the federal regulation governing subpoenas for reporters' toll billing records, the subpoenas were issued, records were produced to the FBI, and the records were uploaded into a [redacted] database.

In our investigation, we identified this problem but also determined that in this instance no reporters' telephone records were actually provided to the FBI.

When we investigated how these subpoenas were issued, the case agent told us that he had merely forwarded the on-site Company A analyst's suggested language to the prosecutor for his "consideration" and was not "prescribing that the text be used." He said the prosecutors had made "unequivocal statements that . . . they were the legal advisors." We believe the case agent's explanations are insufficient and that he should have determined the meaning of [redacted] in the subpoena before providing it as suggested text for the subpoena attachments. At a minimum, he should have consulted with his supervisor, CAU personnel, or

his Chief Division Counsel about what the phrase meant in the context of seeking telephone records in a media leak investigation.

We received conflicting evidence as to whether the case agent had assured the prosecutor before the subpoenas were issued that use of the language suggested by the Company A analyst would not result in the production of [redacted] records. The case agent said both that he did not recall any discussion with the prosecutor about the meaning of the language and that he did not tell any of the prosecutors that the language in the subpoenas or the attachments would not request telephone records of reporters. However, the prosecutor said the case agent had assured him that the suggested language would not result in [redacted] telephone records and was needed only to ensure the retrieval of [redacted] incoming and outgoing calls between the target number and others. In addition, the prosecutor's notes seem to corroborate his assertion that the case agent had told him, erroneously, that the language in the subpoena referring to a [redacted] would not generate [redacted] records, which would have included the records of reporters.

The prosecutor said he realized after the subpoenas were served and responsive records were provided to the FBI that [redacted] language in the subpoenas could have resulted in the production of reporters' records. Following consultation with Criminal Division supervisors, the prosecutor sequestered a hard-copy of the records, witnessed the case agent delete the electronic records from the case agent's e-mail, and consulted with the Department's Office of Enforcement Operations about whether the reporter should be notified in accordance with federal regulations.

We believe the prosecutor and the Criminal Division acted responsibly in addressing the issue once they realized that the subpoena could have generated the reporter's records [redacted] However, to ensure that the FBI deleted all copies of the records, the Criminal Division and the CAU should have conferred to see if additional steps were necessary to address other FBI e-mails attaching the records. Additionally, we believe that prosecutors who approve grand jury subpoenas should review them carefully and ensure they understand what is being requested. In the case of these two subpoenas, the local AUSA who was facilitating issuance of grand jury subpoenas initialed the subpoenas, without attachments, even though the subpoenas said on their face, "Please see attachment." We believe that the local AUSA should not have initialed subpoenas without reviewing and understanding the attachments.

We recommend that the FBI provide periodic guidance to FBI personnel on the special regulations and policies governing subpoenas of

news reporters' toll billing records. We also recommend that the FBI, in conjunction with Department of Justice attorneys, review Department policy regarding responsibility for authorizing grand jury subpoenas when prosecutors share responsibility for investigations with U.S. Attorneys' Offices.

3. Third Matter

In the investigation of a third media leak matter discussed in Chapter Three, employees of Company A, Company B, and Company C [redacted] their databases for records of telephone calls of a cellular phone number used by a reporter. However, the government served no legal process on any of the on-site providers authorizing the [redacted] of the reporter's calling activity.

We determined that prior to [redacted] a grand jury subpoena had been issued to Company A for toll billing records [redacted] The subpoena was requested by an FBI Special Agent and was prepared by personnel in a U.S. Attorney's Office. Although the Special Agent said that his supervisor or one of the prosecutors associated with a related investigation probably had directed him to have the subpoena prepared, the FBI supervisor said he did not recall directing the Special Agent to do so, and the prosecutors said they knew nothing about the subpoena.[268]

We determined that in response to the grand jury subpoena an on-site Company A analyst [redacted] on [redacted] listed in the subpoena. In e-mail exchanges, the Special Agent informed a Company A analyst of the name and cellular phone number of a reporter, facts explaining the relevance of calling activity by the reporter to the investigation, and information indicating that the cellular phone number of the reporter was in contact with [redacted] of the subpoena during a particular period. When the Company A analyst concluded his [redacted] of [redacted] and did not see records of calling activity between [redacted] and the reporter's cellular phone number, on his own he [redacted] Company A's database for records of calling activity by the reporter's cellular phone number. The Company A analyst downloaded and reviewed the calling activity records but did not identify any calls between the reporter's cellular

---

[268] As noted in Chapter Three, we found evidence that the Special Agent's supervisor participated in the interview of the person associated with [redacted] prior to the issuance of the subpoena.

phone number and [redacted] during the specified period. The Company A analyst reported to the Special Agent that there were no records of calling activity between [redacted] and the reporter's cellular phone number, but did not advise the Special Agent that he had [redacted] the [redacted] of the reporter's cellular phone number as well as [redacted]

Thereafter, the Company A analyst provided the CAU Primary Relief Supervisor with the reporter's telephone number, [redacted], and a 3-day date range. Without receipt of any legal process, and in the absence of Attorney General approval, the Company B and Company C on-site employees [redacted] their respective databases for both the reporter's and the [redacted] calling activity during the 3-day time period identified by the Special Agent to the Company A analyst.[269] [redacted] of the calling activity by the [redacted] specified telephone numbers appear to have been sneak peeks, a practice we describe in Chapter Two of this report. As with the CAU's use of sneak peeks generally, [redacted] were conducted without any legal process. While [redacted] its database for calling activity by the reporter, Company B identified responsive records, although we found no evidence that these records were uploaded into FBI databases.

Thus, the Company A analyst [redacted] Company A's records for the reporter's calling activity without any legal process and absent a specific request from the Special Agent or anyone in the FBI or DOJ. In our view, this case again illustrates one of the hazards of having the providers' employees on-site and the total absence of supervision and oversight of the communications service providers' employees by CTD managers and FBI attorneys. Moreover, even if the Special Agent did not specifically ask the providers' employees to [redacted] the reporter's calling activity, by providing the reporter's cellular phone number and details about the calling activity of interest to the Company A analyst, the Special Agent set in motion events that led to unauthorized [redacted] for the reporter's calling activity by all three providers and to [redacted] of the reporter's toll billing records by Company A and Company B.

We are also troubled by the fact that the on-site employees of Company C and in all likelihood Company B were asked by the CAU Primary Relief Supervisor without legal process to [redacted] calling activity by the reporter's telephone number to determine whether the reporter had been

---

[269] The Company B [redacted] included 1 day before and 1 day after the 3-day period provided by the Special Agent to the Company A analyst.

in contact with the [redacted] This is yet another example of the improper processes and lax controls in the CAU.

In Chapter Six of this report, we recommend that the FBI assess the information we developed in this review regarding subpoenas and other requests for reporters' telephone records to determine whether administrative or other personnel action is appropriate for the individuals involved.

III. Conclusion

As discussed in this chapter, we found serious and repeated management failures that led to the FBI's use of exigent letters and other improper requests for telephone records from the on-site providers.

In addition to these management failures, we identified failures on the part of FBI supervisors and attorneys who did not take sufficient action to avoid, prevent, or correct the improper use of exigent letters and other informal requests for telephone records. We recommend that the FBI review the conduct and performance of these individuals, as described in this report, and determine whether discipline or other action with regard to each of them is appropriate.[270]

[270] Several of the individuals whose performance we criticize have resigned or retired from the FBI, including former CTD Assistant Director Joseph Billy, Jr., former CTD Assistant Director Michael Heimbach, former CXS Assistant Section Chief Glenn Rogers, and former NSLB Deputy General Counsel Julie Thomas.

CHAPTER SIX
CONCLUSIONS AND RECOMMENDATIONS

I. Conclusions

The OIG conducted this review of the FBI's use of exigent letters and other informal requests for telephone records to examine the circumstances under which they were used and to assess the accountability of FBI senior officials, supervisors, and employees who were responsible for these practices. This report supplements our findings on exigent letters that were described in our first NSL report issued in March 2007, and our second NSL report issued in March 2008.

A. Exigent Letters and Other Informal Requests

In this report, we found widespread use of exigent letters and other informal requests for telephone records that did not comply with legal requirements or FBI policies governing acquisition of these records. We determined that this practice began in 2003, when the FBI Counterterrorism Division's (CTD) new Communications Analysis Unit (CAU) started using exigent letters to acquire subscriber and telephone toll billing records information from three on-site communications service providers. Glenn Rogers, the CAU Unit Chief at the time, said he approved the use of exigent letters in the CAU because the letters had previously been accepted by Company A during the FBI's New York Field Division's criminal investigations of the September 11 hijackers and because a Company A analyst had assured him they were "approved by the lawyers." However, Rogers did not consult with any attorneys in the FBI Office of the General Counsel's (FBI OGC) National Security Law Branch (NSLB) or other FBI Headquarters' attorneys about whether the letters could be used in national security investigations or other FBI investigations.

In 2003 and 2004, the FBI entered into contracts with Company A, Company B, and Company C that established arrangements whereby these companies placed their employees in the CAU's office space so they could expeditiously respond to FBI requests for telephone records. For example, pursuant to its contract with the FBI, Company A made available to the CAU, in a readily retrievable format, toll billing records [redacted] Company A [redacted] Prior to this contractual arrangement, Company A could easily retrieve telephone records [redacted] During the period of our review, the FBI paid the 3 providers a total of [redacted] under these contracts.

We found that from March 2003 to November 2006, CAU personnel issued 722 exigent letters for telephone records from these 3 communications service providers. One exigent letter was signed by a CXS Assistant Section Chief, 12 were signed by CAU Unit Chiefs, 706 were signed by CAU Supervisory Special Agents (SSA), and 3 were signed by CAU Intelligence Analysts.

Most of the 722 CAU exigent letters stated:

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

However, in our investigation we determined that in some instances CAU SSAs signed exigent letters even though they believed that the factual statements in the letters were inaccurate. For example, CAU Unit Chief Rogers and several SSAs told us they signed exigent letters even though they recognized at the time that subpoenas requesting the records had not been submitted to the U.S. Attorney's Office, as the letters stated. Moreover, we found a few instances in which the signers of exigent letters did not know whether there were exigent circumstances or signed the letters even though they questioned the letter's accuracy about whether an emergency existed.

When we asked FBI supervisors and employees why they issued such letters when they knew that no subpoena had been requested, no one could satisfactorily explain their actions. Instead, they gave a variety of unpersuasive excuses, contending either that they thought someone else had reviewed or approved the letters, that they had inherited the practice and were not in a position to change it, that the communications service providers accepted the letters, or that it was not their responsibility to follow up with appropriate legal process.

In official memoranda distributed to all FBI personnel in January 2003, CTD managers referred to a practice whereby the CAU could obtain records from Company A prior to service of legal process. In November 2003, Rogers issued an electronic communication to CAU personnel that specifically mentioned exigent letters.

We determined that the FBI's use of exigent letters became so casual, routine, and unsupervised that employees of all three communications service providers told us that they – the company employees – sometimes generated the exigent letters for CAU personnel to sign and return to them.

In fact, one of the on-site Company A analysts established an icon on his computer desktop at the CAU so he could quickly generate exigent letters for CAU personnel to sign.

We also found that FBI personnel routinely uploaded telephone toll billing records obtained in response to exigent letters into a [redacted] database where the records were available for review and analysis by [redacted] employees throughout the government who were authorized to access the database.

Most of the exigent letters and other informal requests did not include date ranges for the records requested. Similarly, the CAU's other informal requests to the on-site communications service providers (such as those communicated by e-mail, in person, on pieces of paper, or by telephone) frequently did not have date parameters. As a result, the FBI often obtained substantially more telephone records, covering longer periods of time, than FBI agents typically obtain when serving NSLs with date restrictions. In addition, in cases where the date range established the relevance of the information sought to the investigation, its omission meant that records were received and uploaded into a [redacted] database in violation of the ECPA's requirement that the records sought be relevant to a national security investigation.

We also found that the FBI did not track its use of exigent letters or even keep copies of them. When the CAU first began using exigent letters in March 2003, it failed to establish procedures to track the letters or even ensure that legal process was promptly obtained and served on the providers. Instead, the CAU had to rely on the on-site providers to identify the records for which they were still owed legal process.

In addition to exigent letters, we determined that the FBI used other informal methods to request and obtain ECPA-protected records and calling activity information from the on-site providers. These informal methods included requests made by e-mail, face-to-face requests, requests on pieces of paper (including post-it notes), and telephonic requests made without first providing legal process or even exigent letters. As was the case with exigent letters, these requests were not approved or signed by FBI officials specially delegated to issue NSLs under the ECPA, were not accompanied by the certifications required for NSLs issued under the ECPA, and were not consistently documented or tracked in the CAU.

We concluded that the FBI's use of exigent letters and other informal requests for telephone toll billing records circumvented, and in many cases violated, the requirements of the ECPA statute.

As described in this report, the ECPA generally prohibits communications service providers from disclosing toll records information except in certain limited circumstances set forth in the statute. The relevant exceptions require providers to disclose such information in response to legal process such as NSLs, and permit voluntary disclosures in emergencies involving danger of death or serious physical injury.

Yet, the exigent letters and other informal requests were not valid legal process for compelling the disclosures pursuant to 18 U.S.C. § 2709. Section 2709 of the ECPA authorizes the FBI to compel the production of toll records through NSLs issued by statutorily designated high-level FBI officials who certify that the records sought are relevant to an authorized national security investigation. As we described in our report, the exigent letters and verbal, e-mail, or handwritten requests routinely used by CAU personnel to request toll billing or other calling activity information from the providers did not meet these requirements. For example, none of the individuals who signed exigent letters issued by the CAU were among those specially delegated officials authorized to sign NSLs.[271] Further, none of the exigent letters contained a certification that the records sought were relevant to an authorized national security investigation or that any investigation of a U.S. person was not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In response to our findings, the FBI asserted that its use of exigent letters and other informal requests may have been justified under the emergency voluntary disclosure provision of the ECPA, Section 2702(c)(4). During 2003 through March 2006 – the period when most of the exigent letters were issued – that section authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably

---

[271] The ECPA NSL statute authorizes only the FBI Director or his designees in positions not lower than Deputy Assistant Director (DAD) or field division-based Special Agents in Charge (SAC) to sign NSLs compelling communications service providers to produce subscriber and toll billing records information in investigations of international terrorism or espionage. See 18 U.S.C. § 2709. As Diagram 2.2 in Chapter Two illustrates, by issuing exigent letters the FBI substituted a 1-step process in which CAU personnel signed requests for telephone records without supervisory review by those officials authorized by the ECPA to approve and certify the FBI's basis for requesting these types of records, and without the documentation of the predication for the requests that FBI policy required.

believe[d] that an emergency involving immediate danger of death or serious physical injury justifie[d] disclosure of the information."[272]

We recognize that some – but not all – of the FBI's requests may have been made in circumstances that qualified as emergencies under the applicable emergency voluntary disclosure provision. For example, as we described earlier, exigent letters and other informal requests were used to obtain records in connection with Operation Y (an investigation of a terrorist plot in [redacted] to detonate explosives [redacted] At least one provider's employee told us that he was informed of the nature of the threat in that matter.[273]

However, other exigent letters and informal requests were used in circumstances that do not appear to qualify as emergencies under Section 2702. For example, as described in Chapter Four, although CAU personnel used exigent letters and other informal requests to obtain records from all 3 providers relating to over 400 telephone numbers in connection with "Operation Z," the Unit Chief and an SSA of the operational unit responsible for that high-profile counterterrorism operation told us that they did not believe the CAU requests were made in exigent circumstances.[274] In

---

[272] 18 U.S.C. § 2702(c)(4) (Supp. 2002). In March 2006, the provision was amended to allow voluntary disclosure "if the provider, in good faith, believes that an emergency involving "danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109-177, § 107(b)(1)(B), 120 Stat. 192 (2006). The legislative history of a similar amendment to Section 2702(b)'s emergency voluntary disclosure provision for content information suggests that the belief standard was relaxed because communications service providers "expressed concern to the Committee that the [reasonably believes] standard was too difficult for them to meet and that, as a result, providers may not disclose information relating to emergencies." *Cyber Security Enhancement Act of 2002*, H.R. Rep. No. 107-497, at 12-13 (2002). The Committee report that accompanied the amendments to Section 2702(b) also stated that the Section was "aimed at protecting providers who in good faith attempt to assist law enforcement with an emergency situation." Id. at 14. However, it also stated that the amendment "does not change the standard or lower the standard for law enforcement behavior." Id.

[273] Company B's representative said he was told by CAU personnel that "it could be the next 9/11." However, Company B provided the fewest records to the FBI in connection with this operation. In contrast, one of Company A's employees told us he received no briefing from the CAU regarding this operation, and the other employee stated that he worked on the matter for several weeks before becoming aware that the records he was providing were associated with Operation Y.

[274] After reviewing a draft of this report, the FBI provided the OIG with several contemporaneous e-mails beginning on June 12, 2006, which it asserted would demonstrate the emergency nature of Operations Z. However, we concluded that those e-
(Cont'd.)

addition, an FBI e-mail shows that the Unit Chief refused to state in the EC that was belatedly drafted to document the predication for the CAU's Operation Z requests that the requests were made in circumstances "judged to be exigent."[275]

Several factors make it difficult to determine whether and when the FBI's other uses of exigent letters and informal requests satisfied Section 2702's emergency disclosure exception. First, given the FBI's lack of internal controls over the process of requesting records by exigent letters and other informal requests, it is difficult for the OIG or the FBI to determine with certainty today how many of the requests were made in circumstances satisfying Section 2702(c)(4). Indeed, the FBI has conceded that the lack of documentation for the requests and their connection to particular investigations has impeded its efforts to demonstrate which requests clearly were made in Section 2702 circumstances.

Second, the FBI officials who were most familiar with the exigent letter practice at the time the letters were in use – including Glenn Rogers, Bassem Youssef, and the NSLB Assistant General Counsel – unequivocally stated to us that they did not consider the letters at the time they were made to be requests for voluntary production pursuant to Section 2702.

In addition, as described in Chapter Two, the evidence shows that CAU personnel who made the requests did not understand "exigent circumstances" to be synonymous with the definition of qualifying emergencies under 2702. Although some agents and analysts said an "exigent" matter included a life-threatening matter, others described it as an important, pressing, fast-moving, or high-priority matter, and others said it was a matter in which a high-level FBI official demanded the information.

Finally, even assuming that some of the investigations associated with the exigent letter requests were qualifying emergencies under the statute, the evidence is insufficient to determine whether the providers had the statutorily required belief that such emergencies justified voluntary disclosure. Relevant factors to this issue include that the exigent letters did

---

mails reflected the importance of the investigation, but did not convey that emergency circumstances existed and required disclosure without waiting for legal process. Indeed, with regard to the earliest request for records reflected in these e-mails, we found that the operational unit issued an NSL for the records.

[275] We found other examples of use in non-emergency circumstances, such as the exigent letters used to obtain reporters' records and records relating to a fugitive investigation described in Chapter Three.

not request voluntary disclosure, but instead stated that compulsory legal process (generally grand jury subpoenas) had already been requested and would be served "as expeditiously as possible." In addition, employees of the on-site providers told us they usually were given no information about the circumstances underlying the exigent letters or other informal requests for records, and that they "assumed" the circumstances were exigent. Further, at least one of the provider's employees told us he had doubts about whether the requests were truly exigent.[276] Under these circumstances, it is difficult to determine whether and when the providers' employees had the statutorily required "reasonable" or "good faith" belief that the requisite emergency circumstances existed.[277]

After reviewing a draft of this report, the FBI also asserted for the first time that as a matter of law the FBI is not required to serve NSLs to obtain "records associated [redacted]" in national security investigations. According to the FBI, the majority of exigent letter and other informal requests discussed in this report were for telephone records [redacted] the FBI could have obtained these records without any legal process or qualifying emergency through voluntary production by the communications service providers.[278]

[redacted]

---

[276] This provider ultimately required FBI requesters to endorse a stamped certification that tracked the statutory language in Section 2702 before the provider would provide records in response to exigent letters.

[277] After reviewing a draft of this report, the FBI asserted that the legal standard of Section 2702 could be met when an FBI employee requested telephone records in a qualifying emergency, regardless of whether the FBI employee was aware of the statute. The FBI also asserted that the providers could form a "reasonable" or "good faith" belief that an emergency existed without necessarily knowing the facts surrounding the emergency. As described above, however, with some exceptions the providers frequently received no information about the investigation for which records were requested, or even a generalized representation that an emergency situation existed.

[278] We disagree with the FBI's statement that the majority of exigent letter and other informal requests discussed in this report were for telephone records [redacted] In fact, we determined, based on the FBI's records, that the majority of its exigent letter requests were for toll billing records associated [redacted] We were unable to reach a conclusion concerning the percentage [redacted] requested through informal means other than exigent letters, because the records for these requests (some of which were oral or written on post-it notes) are incomplete and therefore unreliable.

[redacted]

The FBI did not rely on this section when it requested and obtained the records discussed in this report. However, after reviewing a draft of the OIG report the FBI asked the Office of Legal Counsel (OLC) for a legal opinion on this issue.[280] When making the request for an OLC opinion, the FBI stated that [redacted]

On January 8, 2010, the OLC issued its opinion, concluding that the ECPA "would not forbid electronic communications service providers [redacted][281] In short, the OLC agreed with the FBI that under certain circumstances [redacted] allows the FBI to ask for and obtain these records on a

---

[279] The *Stored Communications Act*, codified in Chapter 121 of Title 18 at 18 U.S.C. §§ 2701-2712, was enacted in 1986 as part of the ECPA. The *Stored Communications Act* contains the relevant NSL and other FBI access to toll billing records provisions at issue in this report.

[280] The FBI presented the issue to the OLC as follows: "Whether Chapter 121 of Title 18 of the United States Code applies to call detail records associated [redacted]

[281] [redacted]

voluntary basis from the providers, without legal process or a qualifying emergency.

It is important to note that the FBI acknowledged in its July 2009 comments to a draft of this report that it had never considered or relied upon [redacted] when it obtained any of the telephone records at issue in this report. Moreover, it cannot be known at this point whether any provider would have divulged such records based on [redacted] alone, and without the FBI's representation to the provider that an NSL or other compulsory legal process would be served.

For the reasons discussed below, we believe the FBI's potential use of [redacted] to obtain records has significant policy implications that need to be considered by the FBI, the Department, and the Congress.

[redacted][282]

[redacted][283]

---

[282] [redacted]

[283] The FBI has stated that it does not intend to rely on [redacted] However, that could change, and we believe that appropriate controls on such authority should be considered now, in light of the FBI's past practices and the OLC opinion.

[redacted]285

[redacted]287

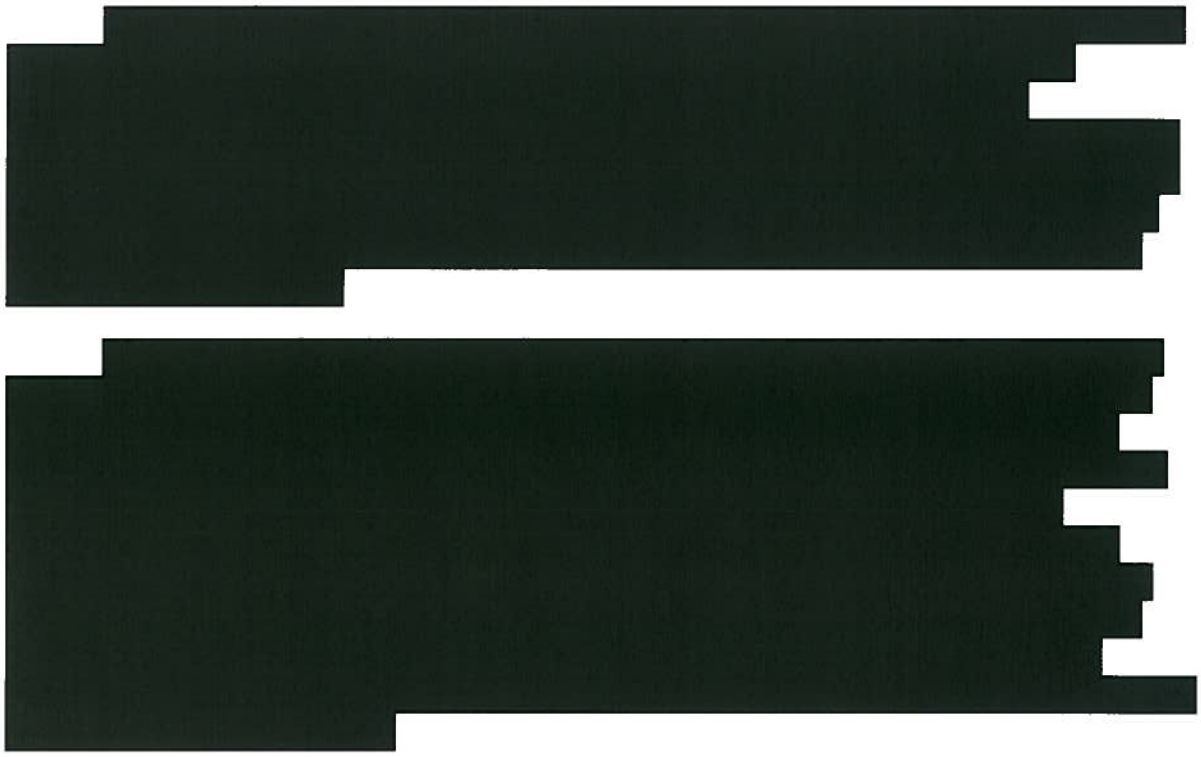
---

284 Under 18 U.S.C. § 2709(b) the FBI may only issue NSLs to obtain such records upon the certification that the records sought are relevant to an authorized counterterrorism or counterintelligence investigation. In the voluntary context, the FBI may request and obtain such records under 18 U.S.C. § 2702(c)(4) only if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."

285 For example, requests for voluntary disclosure under the emergency circumstances provisions of the ECPA NSL statute must be approved at a level not lower than an Assistant Special Agent in Charge in a field office and a Section Chief at Headquarters. See FBI OGC Electronic Communication (EC) to all Divisions (March 1, 2007), at 4. The EC also advises that approval of such requests must be in writing, even if the initial approval was oral. The rank of the approving official for NSLs is set by statute at Special Agent in Charge in field offices and Deputy Assistant Director at Headquarters. See 18 U.S.C. § 2709(b).

286 Under the ECPA NSL statute, the FBI is required to report to certain congressional committees, on a semiannual basis, concerning all NSL requests made under Section 2709(b). See 18 U.S.C. § 2709(e).

287 Moreover, other collections of similar types of records for intelligence activities contain statutorily mandated approval, minimization, and reporting requirements. For example, the FISA business records provisions provide useful comparisons as to how such intelligence activities are regulated, [redacted] Under these provisions, the FBI may apply to the FISA Court for an order requiring the production (Cont'd.)



of business records and other tangible things "to obtain foreign intelligence information not concerning a United States person." See 50 U.S.C. § 1861. By statute, use of this authority is subject to extensive Attorney General-approved minimization procedures governing how information acquired concerning U.S. persons must be retained and disseminated. Id. at § 1861(g). The FBI is also subject to comprehensive congressional reporting requirements as to all orders it obtains, Id. at § 1862.

288 As discussed in this report, under the ECPA NSL statute, the FBI may only seek toll billing records when relevant to an authorized counterterrorism or counterintelligence investigation, provided that the investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution. See 18 U.S.C. § 2709(b). Provisions in the FISA statute similarly protect U.S. persons with respect to FBI applications to the FISA Court seeking orders to produce business records (50 U.S.C. § 1861(a)(2)(B)) and to conduct electronic surveillance (50 U.S.C. § 1805(a)).

289 We recognize that the FBI's Domestic Investigations and Operations Guide (DIOG) and Executive Order 12,333, as amended, contain restrictions on how the FBI can collect, use, and disseminate intelligence, particularly with respect to the privacy and civil liberties interests of U.S. persons. However, these constraints are not statutory.

290

In sum, the potential use of [redacted] by the FBI has important policy implications for [redacted] We believe that [redacted] creates a significant gap in FBI accountability and oversight that should be examined closely by the FBI, the Department, and Congress.

It is also important to recognize that the FBI advanced the [redacted] only after the OIG found repeated misuses of its statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary disclosure provisions. We believe that, given the abuses described in this report, it is critical for the Department and Congress to consider appropriate controls on any use by the FBI of its authority to obtain records voluntarily [redacted]

The OIG therefore recommends that the FBI and the Department consider how the FBI may use [redacted] when seeking telephone billing records, particularly with respect to [redacted] We also recommend that the Department notify Congress of this issue and of the OLC opinion interpreting the scope of the FBI's authority under it, so that Congress can consider [redacted] and the implications of its potential use.

B. Other Informal Requests for Telephone Records

We found that without any documentation for the requests except possibly e-mail messages, CAU personnel routinely asked the on-site providers' employees to provide calling activity information in response to what were referred to as "sneak peeks." Using sneak peeks, the FBI requested the providers' employees [redacted] their databases and tell the FBI whether they had any records on specified telephone numbers. At the FBI's request, the providers would conduct sneak peeks and sometimes give the FBI additional information about the telephone records, such as whether there was calling activity between specified numbers or calls to or from certain [redacted] These sneak peeks were conducted without any legal process whatsoever.

We also concluded that many of these sneak peeks violated the ECPA, which prohibits communications service providers from knowingly divulging "a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity" except pursuant to legal process or in certain limited circumstances set forth in the statute. 18 U.S.C. § 2702(a)(3). The relevant exceptions require providers to disclose such records or information in response to compulsory process, such as

NSLs, and also permit voluntary disclosure based on the providers' good faith-belief of a qualifying emergency.[291] We concluded that the FBI did not serve legal process under the ECPA for the information it received pursuant to sneak peeks.

In addition, we do not believe that the sneak peek practice complied with the ECPA's emergency voluntary disclosure provision for several reasons. First, the practice was described to us as a routine occurrence in the CAU and not limited to "exigent" or emergency circumstances. Second, some of the specific instances where the sneak peek practice was used included media leak and fugitive investigations which did not meet the emergency voluntary disclosure provision. Third, the FBI's lack of internal controls over the sneak peek practice has made it impossible to reliably determine how many or in what circumstances sneak peek requests were made, and what the providers were told or believed about the reasons for these requests.

Our review also found that the FBI improperly asked Company A's on-site employees to conduct "community of interest" [redacted] In response to a community of interest [redacted] request, Company A would retrieve [redacted] records [redacted] Although we could not determine due to the FBI's lack of documentation how often the FBI requested these community of interest [redacted] or how often Company A provided such records to the FBI, we found at least 52 exigent letters, 250 NSLs, and 350 grand jury subpoenas served on the on-site providers that included such requests.

The FBI's community of interest [redacted] requests were often included in the boilerplate attachments to NSLs. We found that FBI officials who signed NSLs that contained community of interest requests often were not aware they were making such requests. In such instances, the FBI issued NSLs with community of interest [redacted] requests without first conducting, or documenting in the NSL approval memoranda (approval ECs), any assessment of the possible relevance of [redacted] telephone numbers to the underlying investigation. Absent such an assessment, we believe the FBI did not satisfy the ECPA requirement to issue NSLs in national security investigations only upon certification by those authorized

---

[291] As described previously, prior to March 2006, this exception required the provider to have a "reasonable belief" that a qualifying emergency existed.

to sign NSLs that the records sought are relevant to authorized national security investigations.[292]

We also found that the FBI's community of interest [redacted] practices likely resulted in the FBI obtaining and uploading into a [redacted] database thousands of telephone records for [redacted] telephone numbers without the advance determination by an SES-level official that the records were relevant to an authorized international terrorism investigation. In addition, the FBI is unable with certainty to identify today which records in the database are associated with [redacted] numbers and whether those numbers were relevant to the underlying investigations for which they were requested. We also concluded that the FBI did not recognize the implications of Company A's community of interest [redacted] capability when Company A first posted its analysts on-site at the CAU; did not issue written guidance in coordination with the FBI OGC about the circumstances in which such requests were appropriate under the ECPA; did not establish an approval process for such requests or ensure that the predication for these requests was properly documented in approval ECs; and did not ensure that records sought in community of interest [redacted] requests were included in required reports to Congress on NSL usage.

Our review also uncovered other irregularities in the manner in which the FBI obtained toll billing records and other information from the on-site providers. From 2004 through 2006 Company A and Company C [redacted] calling activity by certain "hot numbers" identified to them by CAU personnel. Without serving legal process or even exigent letters, CAU personnel requested that the companies [redacted] the calling activity information for a total of at least 152 of these hot telephone numbers. The on-site Company A analyst thereafter provided the FBI (either verbally or by e-mail) calling activity information for at least 42 hot numbers during the period covered by our review.

Based on the Office of Legal Counsel's legal analysis of the ECPA in its November 5, 2008, opinion, we concluded that the calling activity information provided to the FBI on the "hot numbers" constituted "a record or other information pertaining to a subscriber or a customer," under the ECPA.[293] Therefore, we concluded that absent valid legal process or a qualifying emergency, the FBI was not authorized to obtain this information.

---

[292] See 18 U.S.C. § 2709(b).

[293] 18 U.S.C. § 2702(a)(3).

We found that the FBI did not serve legal process on the providers in advance of receiving information about hot numbers. Moreover, we found no evidence that the FBI requested, or the providers gave the FBI, this information pursuant to the emergency voluntary disclosure provision of the ECPA. Instead, it appears that the information was disclosed as part of the contractual arrangement between two of the providers and the FBI, and was often used in connection with fugitive matters that did not qualify as emergency situations under Section 2702.

Therefore, we concluded that the FBI's practice of requesting and obtaining calling activity information about hot numbers without service of legal process violated the ECPA.

We also examined whether information obtained in response to exigent letters or other informal requests were used in applications for electronic surveillance or pen register/trap and trace orders filed with the Foreign Intelligence Surveillance Court (FISA Court). The Department's National Security Division (NSD) and the FBI reviewed 37 FISA applications, which together referenced a total of 35 unique telephone numbers, to determine whether FBI declarations filed in support of the applications accurately stated the basis for verifying subscriber or calling activity information. We found five misstatements in four declarations, which were filed under oath by FBI personnel. The declarations inaccurately stated that the FBI had acquired subscriber or calling activity information from NSLs when in fact the information was acquired through other means, such as exigent letters, an emergency disclosure letter, and a verbal request to the communications service providers. Moreover, several of the NSLs referred to in the four applications were served at least 2 months after the FISA Court issued the requested orders.

As a result of this review, the NSD notified the FISA Court of the inaccurate statements. The NSD concluded that, under the ECPA, the inaccurate statements made in the FBI declarations were non-material. Yet, even though the inaccurate statements may have been non-material to the FISA application, we believe that any inaccurate statements to the FISA Court are serious and affect the credibility of representations made by the government.

It is also important to note that we reviewed only a small percentage of the FISA Court applications that may have relied upon information derived from exigent letters or other improper means. Based on our results in these cases, we believe there are likely other similar inaccurate statements in other applications. Moreover, no one in the FBI and the NSD who reviewed these applications prior to their submission to the Court had identified the inaccurate statements. Thus, our review concluded that the FBI and the NSD failed to provide adequate supervision and oversight to

ensure the accuracy of the FBI's declarations filed in support of applications seeking FISA Court orders.

Our investigation also uncovered FBI misuse of administrative subpoenas to obtain telephone records. We determined that some administrative subpoenas served on the on-site communications service providers were preceded by "sneak peek" requests through which the on-site providers' employees would first check their databases to determine if records of interest were contained in the databases. In some cases, the providers even gave the FBI records or other calling activity information prior to the service of administrative subpoenas.

We concluded that the ECPA was violated when the FBI obtained ECPA-protected telephone records without first issuing appropriate legal process. The ECPA requires communications service providers to disclose local and long distance non-content telephone records "when [the FBI] uses an administrative subpoena authorized by a Federal . . . statute . . . ."[294] However, the ECPA does not authorize the FBI to obtain ECPA-protected records or information and then serve an administrative subpoena. Accordingly, we believe that the FBI's receipt of records obtained prior to issuance of administrative subpoenas violated the ECPA.[295]

We also found that from 2003 to 2006 the FBI served at least 54 administrative subpoenas pursuant to 21 U.S.C. § 876 for toll billing records as part of the fugitive investigation conducted by the FBI's [redacted] Field Division regarding [redacted] This statute authorizes the use of administrative subpoenas in connection with an active narcotics investigation to which the records sought are relevant. However, some of these subpoenas were issued when the FBI's [redacted] Field Division had no active narcotics investigation to which the requested records were relevant. Therefore, this was an improper use of Title 21 administrative subpoenas. Further, the CAU SSA who signed seven of the subpoenas was not among those officials delegated authority under the statute to sign administrative subpoenas.

C. FBI Attempts at Corrective Actions

As discussed in Chapter Four of this report, from late 2003 through March 2007 when the OIG issued its first NSL report the FBI made various

---

[294] 18 U.S.C. § 2703(c)(2).

[295] We found no evidence that these were emergency voluntary disclosures pursuant to Section 2702.

attempts to address issues arising from the CAU's use of exigent letters and other informal means to obtain telephone records. However, during this time period the FBI's actions were seriously deficient and ill-conceived, and the FBI repeatedly failed to ensure that it complied with the law and FBI policy when obtaining telephone records from the on-site communications service providers. For example, during this period the FBI regularly issued after-the-fact NSLs, which were an inappropriate tool for remedying the FBI's improper exigent letter practices. Additionally, the FBI issued 11 improper blanket NSLs to try to "cover" or validate the improperly obtained records. These attempts were inconsistent with the ECPA NSL statute, the Attorney General's NSI Guidelines, and FBI policy.

By contrast, after the OIG issued its first NSL report in March 2007, the FBI took several appropriate actions to address the problems created by exigent letters. The FBI ended the use of exigent letters; issued clear guidance on the proper use of NSLs and the ECPA emergency voluntary disclosure statute; and conducted an audit of NSLs issued by field and Headquarters divisions from 2003 through 2006, the results of which were summarized in the OIG's second NSL report released in March 2008. The FBI also directed that its personnel be trained on NSL authorities; agreed to the move of the communications service providers' employees off FBI premises; and expended significant efforts to determine whether improperly obtained records should be retained or purged from FBI databases.

1. The FBI's Initial Attempts at Corrective Action

As detailed in Chapter Four of this report, in late-December 2004 the CAU asked NSLB attorneys to issue an after-the-fact NSL to cover records that had previously been provided to the CAU. By late 2004, FBI National Security Law Branch attorneys, including Deputy General Counsel Julie Thomas, learned about the CAU's use of exigent letters, but the NSLB failed to examine the practice adequately to ensure that it comported with the law, the Attorney General's NSI Guidelines, and FBI policy. Instead, the NSLB sought to devise a process to expedite issuing after-the-fact NSLs for records that the CAU had requested in emergency circumstances pursuant to exigent letters.

Yet, these after-the-fact NSLs were legally flawed. Although the NSLB accepted the CAU's use of exigent letters with the promise of future legal process, the ECPA authorizes the FBI to compel the production of records or other covered information only upon certification in writing by specified senior officials that the records sought "are relevant to an authorized

investigation to protect against international terrorism or clandestine intelligence activities" and that any investigation of a U.S. person "is not conducted solely on the basis of activities protected by the first amendment."[296] After-the-fact legal process, no matter how soon after the fact, is not authorized either by the ECPA NSL statute, the Attorney General's NSI Guidelines, or FBI policy. Additionally, none of the after-the-fact NSLs cited the ECPA emergency voluntary disclosure statute as authority for the previous [redacted]

Although the CAU began to obtain after-the-fact legal process more quickly, the backlog of records requests persisted. The backlog began during Glenn Rogers's tenure as CAU Unit Chief and continued after Bassem Youssef became the CAU Unit Chief in November 2004. While some after-the-fact NSLs were issued by FBI field and Headquarters divisions and the NSLB to address the backlog, we found that neither Rogers nor Youssef took appropriate steps to ensure that the CAU tracked or adequately addressed the backlog. Neither supervisor ensured that FBI personnel who had asked the CAU for records issued the appropriate NSLs or, if these efforts were unsuccessful, alerted senior CTD managers to the problem. As a result, by mid-2006 the FBI had a backlog of record requests for more than 900 telephone numbers. In addition, neither Youssef nor any other CAU personnel sufficiently informed NSLB attorneys of the full scope of the problems the CAU was facing regarding the backlogged record requests.

The FBI attempted to address the backlog by issuing 11 blanket NSLs that were designed to "cover" or validate telephone records that had been provided to the FBI pursuant to exigent letters or other informal requests. The FBI attached to the blanket NSLs signed by senior CTD officials lists that included telephone numbers that had been [redacted] by the on-site providers as long as 3 years earlier.

However, these blanket NSLs were improper and flawed, and they did not comply with the ECPA NSL statute, Attorney General's NSI Guidelines, and FBI policy. As noted above, the ECPA does not authorize the FBI to cover the prior production of telephone records or ECPA-protected calling activity information by issuing after-the-fact NSLs. In addition, the blanket NSLs included telephone numbers relevant to criminal or domestic terrorism investigations for which NSLs were not an authorized technique under the ECPA NSL statute, the Attorney General's NSI Guidelines, or FBI policy. Additionally, the blanket NSLs were not accompanied by required approval ECs, and most of them did not contain the required certifications

---

[296] See 18 U.S.C. § 2709(b).

for NSLs imposing non-disclosure and confidentiality obligations on the recipients. Finally, the after-the-fact blanket NSLs did not retroactively cure any violations of the ECPA that occurred when the FBI requested and received records without legal process and in the absence of a qualifying emergency.

2. Corrective Actions after the OIG's First NSL Report

By contrast, after the FBI received the OIG's first NSL report it began to take appropriate steps to address the improper use of exigent letters and other informal requests for telephone records. In March 2007, the FBI OGC issued guidance directing that FBI personnel no longer use exigent letters. The guidance explained the distinctions between the FBI's authority to compel the production of ECPA-protected records or to request emergency voluntary disclosures. The guidance made clear the legal avenues that were available to FBI investigators who seek to obtain telephone records, including a description of the legal basis for emergency voluntary disclosure requests. In June 2007, the FBI issued comprehensive guidance to all FBI personnel regarding the FBI's NSL authorities.

In 2007 and 2008, the FBI conducted three audits to assess the extent of its errors in NSL usage. The FBI reviews generally confirmed the OIG's findings in its first NSL report 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 who provided the FBI with information that was not requested.

In December 2007 and January 2008, the employees of the three on-site providers moved out of the FBI. These moves were also accompanied by changes in the FBI's protocols for obtaining telephone records from the three providers.

Additionally, the FBI developed a process to determine whether to retain or purge telephone records obtained through exigent letters and those listed in blanket NSLs. As part of this process, the FBI reviewed records for the 4,379 unique telephone numbers listed in exigent letters and the 11 blanket NSLs to determine whether there was a basis to justify retention of the records. In deciding whether to retain records based on the results of that research, the FBI developed a 5-step "decision tree" based upon the two ECPA authorities for obtaining telephone records. Since the ECPA does not authorize the FBI to compel the production of ECPA-protected records with a promise of future legal process, the FBI's decision tree was used by the FBI not as a basis for the original record requests, but as a basis upon which to analyze whether the FBI would retain the records.

In a complex and time-consuming review, the FBI determined that it would retain most of the records but purge others. In essence, the process attempted to determine if the FBI could find legal process issued in connection with the [redacted] request, if the FBI would issue new legal process modeled on the ECPA standard for issuing legal process, or if neither of those options was available, if the FBI could justify retention under an after-the-fact application of the ECPA emergency voluntary disclosure statute.

Under the FBI's analysis, the FBI will retain records for 3,352 telephone numbers because it found either that (1) appropriate legal process associated with the request was previously issued or could be issued for these records; or (2) because the circumstances at the time of the requests satisfied the statutory standard for emergency voluntary disclosures.

The FBI also concluded that it would purge records for 739 telephone numbers because the circumstances under which the records were requested did not meet any of the criteria for retention available in the FBI's decision tree. In addition, the FBI concluded that it must purge a portion of the records for 302 of these telephone numbers because the records obtained were outside the time period specified in the legal process identified by the FBI.

The FBI faced a difficult challenge in reviewing the records improperly acquired from exigent letters or listed in the 11 blanket NSLs. However, under the circumstances it created, we believe the FBI's approach to determine which records to retain and which to purge was reasonable.

In sum, we concluded that the FBI initial attempts to cover the improperly obtained records were deficient, ill-conceived, and poorly executed. However, we believe its review process and other corrective measures since issuance of our first NSL report in March 2007 have been reasonable, given the difficult and inexcusable circumstances that its deficient exigent letter practices created.

D. Improper Requests for Reporters' Telephone Records or Other Calling Activity in Three Media Leak Investigations

We also found that in three media leak investigations the FBI requested, and in two of these instances obtained from on-site communications service providers, telephone records or other calling activity information for telephone numbers assigned to reporters. However, the FBI did not comply with federal regulation and Department policy that requires Attorney General approval before requesting such records and that also requires a balancing of First Amendment interests and the interests of

law enforcement before issuing subpoenas for the production of reporters' telephone toll billing records.[297]

The first leak investigation involved the disclosure of classified information in articles published by the Washington Post and The New York Times in [redacted] about the [redacted] Without a request from FBI investigators, and without the knowledge of any prosecutor, a CAU SSA issued an exigent letter to an on-site Company A analyst for the telephone records of the Post and Times reporters who wrote the articles and their bureaus in [redacted] Company A provided the records to the FBI, and the FBI uploaded the records into a [redacted] database.

The records remained in that database for over 3 years, unbeknownst to the prosecutor, CTD management, and FBI OGC attorneys until 2008 when OIG investigators determined that the records had been improperly acquired and notified the FBI General Counsel. We concluded that the FBI's acquisition of these records constituted a complete breakdown in the required Department procedures for approving the issuance of grand jury subpoenas to obtain reporters' toll billing records.

In the same investigation, we also found that the FBI sent the counterintelligence squad case agent [redacted] to [redacted] This case agent was accompanied [redacted] The agents in the [redacted] – the leak investigation [redacted] Pursuant to instructions from his supervisor, the FBI case agent [redacted]

In August 2008, following the OIG's notification to the FBI that it had improperly acquired the reporters' records, the FBI informed the newspapers and the reporters that their telephone records had been obtained, as required by federal regulation. However, the FBI's notification did not disclose that [redacted]

---

[297] See 28 C.F.R. § 50.10.

[redacted]

In the second media leak investigation an Assistant United States Attorney (local AUSA) and a federal prosecutor approved grand jury subpoenas that directed a communications service provider to deliver [redacted] This language meant that the subpoenas sought not [redacted] but also the toll billing records for [redacted] reporters.

After the subpoenas were served and records were sent to the FBI case agent as e-mail attachments, the prosecutor realized by virtue of a fortuitous conversation with an FBI Special Agent that the provider could have given the FBI reporters' records [redacted] requested. The prosecutor took steps to sequester the telephone records and notified the Department's Criminal Division of the issue. In our review, we found no evidence [redacted] or that reporters' toll billing records were provided to the FBI in response to the subpoenas.

Following consultations with the Office of Legal Counsel, the Criminal Division concluded that it was not required to notify the reporters of the subpoenas, even though the subpoenas, if fulfilled, would have resulted in acquisition of reporters' records.

We concluded that the way in which the Department drafted and issued the two subpoenas in this leak investigation was deficient. The prosecutor drafted and approved language in the subpoena attachments that neither the FBI agent nor the prosecutor correctly understood; the local AUSA assigned to assist the investigation in the jurisdiction where the grand jury was empanelled initialed the grand jury subpoenas without reviewing the attachments, which were prepared by the prosecutor and attached after the local AUSA initialed the subpoenas; and but for a fortuitous conversation between a Special Agent not involved in the investigation and the prosecutor, FBI and Criminal Division attorneys would likely not have learned about the problems with the language in the subpoenas.

In the third media leak investigation the Department served on an on-site Company A analyst a grand jury subpoena requesting a [redacted] for records of a [redacted] the FBI believed was in telephonic contact with a reporter. [redacted]

[redacted]

In addition, based on information provided to the Company A analyst by an FBI Special Agent, the Company A analyst [redacted] Company A's database and downloaded records for the reporter's cellular phone calling activity. After the [redacted] which was [redacted] without any legal process, the Company A analyst informed the FBI Special Agent that there were no records of calling activity between the reporter's and the [redacted] numbers during the specified date range. The Company A analyst [redacted] this [redacted] without the knowledge of the Special Agent.

Also, at the request of the CAU's Primary Relief Supervisor, without any legal process, the on-site Company B and Company C employees [redacted] their databases for calling activity by the reporter's cellular phone number. The Company B employee found responsive records, although Company B reported to us that the employee did not recall whether he had provided responsive information to the FBI. We found no evidence that these records were uploaded into FBI databases. The on-site Company C employee determined that Company C had no responsive records.

In sum, we concluded that serious lapses in training, supervision, and oversight led to the abuses involving the FBI's improper requests for reporters' records in these three leak investigations. CAU personnel told us they did not know about the special approval requirements for subpoenaing reporters' toll billing records. The federal prosecutors involved with these matters, said they did not know the subpoenas sought reporters' records either because they did not see or examine the attachments or because they did not correctly understand that the terminology used in the subpoenas or attachments could result in the acquisition of reporters' records. The failures in training, the diffusion of prosecutorial responsibility for the grand jury subpoenas, and the absence of oversight within the CAU or from the CTD or the FBI OGC resulted in the Department not following legal requirements and its own policies for issuing subpoenas to obtain reporters' toll billing records.

E. OIG Findings on Management Failures and Individual Accountability for Exigent Letters and other Improper Requests for Telephone Records

In Chapter Five of this report, we assessed the accountability of FBI employees, their supervisors, and the FBI's senior leadership for the use of exigent letters and other improper practices we described in this report.

We concluded that numerous, repeated, and significant management failures led to the FBI's use of exigent letters and other improper requests

for telephone transactional records over an extended period of time. These failures began shortly after the CAU was established within the Counterterrorism Division (CTD) in 2002, and they continued until March 2007 when the OIG issued its first NSL report describing the improper use of exigent letters. We believe that every level of the FBI – from the most senior FBI officials, to the FBI's Office of the General Counsel (FBI OGC), to managers in the CTD, to supervisors in the CAU, to the CAU agents and analysts who repeatedly signed the letters were responsible in some part for these failures.

FBI Director Mueller, Deputy Director Pistole, and FBI General Counsel Caproni said they were unaware until late 2006 that the CAU was obtaining telephone records without appropriate legal process. In addition, all but one of the CTD supervisors we interviewed said they did not know prior to the OIG's first NSL investigation that the CAU was using exigent letters to obtain telephone records from the on-site providers.

We found that beginning in 2003, shortly after the CAU was established and the FBI contracted to have Company A's employees work on-site, FBI officials failed to recognize and address clear risks for potential misuse of the FBI's NSL and other authorities to obtain telephone records. These risks arose from the combination of several factors, including the FBI's expanded authority to obtain records protected by the ECPA, the close proximity of the on-site providers' employees to FBI personnel in a common FBI work area, and the assignment of SSAs and Intelligence Analysts to the CAU who had no background or training in national security investigations or in using NSLs.

At the same time, FBI officials at all levels failed to develop a plan and implement procedures to ensure that telephone records were properly obtained from the on-site communications service providers. The FBI compounded its planning failures when it did not ensure that all CAU personnel were trained on the legal requirements for obtaining ECPA-protected records. In particular, FBI managers – from CAU Unit Chiefs, to the FBI OGC, to the senior leaders of the FBI – failed to ensure that CAU personnel were properly trained to request telephone subscriber and toll billing records information from the on-site communications service providers in national security investigations only in response to legal process or under limited emergency situations defined in 18 U.S.C § 2702(c)(4). They also failed to ensure that CAU personnel were trained to comply with the Attorney General's NSI Guidelines and internal FBI policies governing the acquisition of these records. They also failed to recognize the need for, and assure adequate oversight of, the practices employed by the CAU to obtain subscriber information, toll billing records, and other calling activity information from the on-site providers.

In reviewing the FBI's responsibility for exigent letters and other improper requests for telephone records and the performance of FBI personnel involved in the practices covered in this review, we recognize that the FBI was confronting major organizational and operational challenges during the period covered by our review. As we noted in our first NSL report, following the September 11 attacks the FBI overhauled its counterterrorism operations, expanded its intelligence capabilities, and began to upgrade its information technology systems. Throughout the 4-year period covered by this review, the CTD also was responsible for resolving hundreds of threats each year, some of which, such as bomb threats or threats to significant national events, needed to be evaluated quickly. Many of these threats, whether linked to domestic or international terrorism, resulted in a large number of high-priority requests to the CAU for analysis of telephone communications associated with the threats, which was the CAU's core mission.

Members of the FBI's senior leadership told us that they placed great demands on the CAU and other Headquarters' units. The FBI Director stated that he placed "tremendous pressure" on CTD personnel to respond to terrorism threats. Other senior FBI officials stated that there were countless "hair on fire" days when Headquarters personnel worked through nights and on weekends to determine whether information the FBI received from various sources presented threats to the United States. Indeed, some of the exigent letters and other improper practices we describe in this report were used to obtain telephone records that the FBI used to evaluate some of the most serious terrorist threats posed to the United States in the last few years. In our view, these circumstances do not excuse the management and performance failures we describe in this report, but they provide important context to the events that led to the serious abuses we found in this review.

We also believe the management failures we described do not explain all the deficiencies we found in this review. In this review, we concluded that FBI supervisors and attorneys did not take sufficient action to prevent or promptly correct the improper use of exigent letters and other informal requests for telephone records. We also concluded that the performance of some FBI employees who signed letters that were inaccurate on their face was not in accord with the high standards expected of FBI and other law enforcement personnel.

First, we found that Glenn Rogers, the CAU's first Unit Chief, authorized the CAU's use of exigent letters without proper legal review by the NSLB, and failed to ensure that the personnel assigned to the CAU received proper guidance on national security investigations and using NSLs. Rogers also personally signed 12 exigent letters without making an effort to confirm that exigent letters were appropriate for use by the CAU in

national security investigations. Moreover, he signed and allowed his subordinates to sign letters that inaccurately stated that subpoenas requesting the telephone records had been submitted to the U.S. Attorney's Office and would be served expeditiously. He also instructed subordinates who questioned him about using such inaccurate letters to continue to use them. In addition, Rogers failed to implement a system for tracking the use of exigent letters, which resulted in a growing backlog of [redacted] of records for which the providers were promised follow-up legal process. These failures led to the routine use of exigent letters and after-the-fact NSLs, as well as the use of sneak peeks and other improper practices detailed in this report. Finally, Rogers failed to ensure that Bassem Youssef, his successor as CAU Unit Chief, was adequately briefed on the unit's methods and procedures, including the specific methods the CAU used for obtaining records from the providers.

Second, we found that Bassem Youssef inherited the improper practices that were in place during Rogers's tenure but that he, too, did not do all he could have, and should have, to address the improper use of exigent letters and other informal requests for telephone records. Youssef failed to understand or adequately assess, in coordination with CTD management and the NSLB, the various methods by which CAU personnel were obtaining records from the on-site providers. Youssef told us that he was unaware of the details of the CAU's requests for community of interest [redacted] sneak peek requests, hot number [redacted] and the unauthorized use of administrative subpoenas. In addition, Youssef personally signed 1 exigent letter, although he did not review or read the exigent letter for more than 5 months after he signed the letter and 18 months after he became the CAU Unit Chief.

Third, we believe Julie Thomas did not properly perform her duties as the NSLB Deputy General Counsel with respect to the CAU's use of exigent letters. Many of the improper practices described in this report pre-dated Thomas's tenure in the NSLB. However, after she became the NSLB Deputy General Counsel and became aware of exigent letters, she did not adequately review and assess the legality of their use in a timely fashion, halt their use, ensure in coordination with CTD officials that CAU personnel understood the lawful methods for obtaining records from the on-site communications service providers, or ensure that the NSLs that she personally signed complied with the ECPA NSL statute.

We found that the Assistant General Counsel, an FBI senior line attorney who was the NSLB point-of-contact for NSL-related policies and issues, did not recognize that exigent letters promising future legal process were an improper tool for obtaining ECPA-protected records and that after-the-fact NSLs also were unauthorized. The Assistant General Counsel also provided inaccurate guidance on the use of exigent letters, and she did

not review a copy of any exigent letter until May 2006, more than 18 months after first learning of their use in the CAU. After reviewing an exigent letter, she merely revised the letter to substitute the term "NSL" for the inaccurate reference to after-the-fact issuance of grand jury subpoenas, and she advised the CAU that it could continue to use the revised exigent letter. The Assistant General Counsel also did not recognize that many of the exigent requests that came to the CAU qualified for emergency voluntary disclosure requests under the ECPA. By these actions and inaction, the Assistant General Counsel allowed the FBI's improper use of exigent letters and after-the-fact NSLs to continue. Although the Assistant General Counsel kept her supervisors informed of the advice she was giving and the actions she was taking, we believe based on her experience in national security investigations and the senior policy position she held in the NSLB that she should have directly confronted the legal deficiencies in the use of exigent letters and, through her supervisors in the NSLB and in conjunction with CTD managers, ensured that the use of exigent letters ended.

As described in Chapter Four of this report, we found that 4 senior CTD officials – Joseph Billy, Jr., Arthur Cummings III, Michael Heimbach, and Jennifer Smith Love – signed a total of 11 improper blanket NSLs in 2006. Each of these NSLs had multiple deficiencies. None of them was accompanied by required approval Electronic Communications (EC) documenting the predication for the requests, and some were issued without the required ECPA certifications. While we recognize that each of these four officials had other significant responsibilities in the FBI and that they each worked in a high-pressure environment in furtherance of the FBI's counterterrorism mission, we believe they should have taken more care to ensure that the NSLs they signed complied with the ECPA, the Attorney General's NSI Guidelines, and FBI policy. In signing these improper NSLs, we believe that these CTD senior officials contributed to misuses of NSL authorities.

As described in Chapter Two of this report, we determined that many CAU employees signed the inaccurate and improper exigent letters issued by the CAU. In evaluating the accountability of the CAU employees who signed these exigent letters, we asked them whether they knew when they signed the letters that the factual statements they contained were inaccurate. We specifically asked whether they knew that exigent circumstances existed at the time they signed the letters and whether they knew that requests for grand jury subpoenas had been submitted to the U.S. Attorney's Office, as specifically stated in the letters.

With few exceptions the CAU employees who signed the letters said they believed exigent circumstances were present. However, most of the CAU SSAs we interviewed told us they did not know whether grand jury subpoenas had been requested at the time they signed the exigent letters,

although some said they recognized that the letters inaccurately described the process for obtaining grand jury subpoenas. Some CAU employees explained their signing the letters by stating they "thought it was all part of the program coming from the phone companies themselves," and they assumed the letters were approved by the FBI or communications service providers' attorneys. Another CAU employee said that he knew that subpoenas had not been issued but signed the exigent letters anyway because he saw the letter used by other CAU personnel as a standard practice and he received assurances from CAU Unit Chief Rogers that the exigent letter was okay to use. Other CAU employees said they said that they did not pay much attention to and were not concerned about the reference to a grand jury subpoena. Still others told us that when they signed the letters they did not know for sure what type of after-the-fact legal process would be used by the field division or Hedquarters unit that initiated the request. Others said that they considered the reference to grand jury subpoenas to broadly include all categories of legal process, such as NSLs. And others told us that they never read the exigent letters closely enough to notice any of the statements they contained.

It is important to recognize several mitigating factors regarding these CAU signers of exigent letters. For example, CAU Unit Chief Rogers and the NSLB approved the use of exigent letters, the FBI failed to train CAU personnel on the authorized means of requesting records from the on-site providers, and the communications service providers readily accepted the exigent letters.

However, we believe that none of these factors excuses FBI employees who signed an exigent letter from not making the effort to confirm the factual accuracy of the letter or, knowing the letter was inaccurate, not raising concerns about the letter's accuracy to FBI supervisors. Simply put, we do not believe employees of the FBI should sign their names to letters making a statement that is not true, even if the letters are approved by management, sanctioned by FBI attorneys, part of an established practice, or accepted by the recipients.

We also recognize that a few SSAs raised concerns about the exigent letters to their supervisor, CAU Unit Chief Rogers, and that he instructed them to continue using the letters without changing the wording. Even in this circumstance, we believe that FBI employees confronted with this problem had options other than to simply sign the letters. They could have sought further guidance from more senior managers in the FBI, either directly or anonymously. They could have complained to a senior CTD official or the FBI Inspection Division. They could have contacted the OIG. None of them took any of these steps. Instead, they continued to sign inaccurate exigent letters.

Finally, as discussed above, FBI personnel were involved with requests to [redacted] reporters' toll billing records in three different media leak investigations, without first complying with Departmental regulation or obtaining the required Attorney General approvals. We believe that these matters involved some of the most serious abuses of the FBI's authority to obtain telephone records. As described in Chapter Five of this report, we recommend that the FBI consider appropriate action for the FBI employees who sought to obtain these records without first obtaining the required Attorney General approval.

II. Recommendations

As discussed above, after we issued our first NSL report in March 2007 the FBI ended the use of exigent letters and took other corrective actions to address the improper use of exigent letters. However, as a result of further deficiencies we uncovered in this review, we believe the FBI and the Department need to take additional action to ensure that FBI personnel comply with the statutes, guidelines, regulations, and policies governing the FBI's authority to request and obtain telephone records. We therefore provide the following recommendations to the FBI and the Department:

1. The FBI should assess this report and the information we developed in this review to determine whether administrative or other personnel action is appropriate for the individuals involved in the use of exigent letters and other improper requests for telephone records.

2. The FBI should issue periodic guidance and conduct periodic training of FBI Headquarters and field personnel engaged in national security investigations regarding the authorities available to the FBI under the *Electronic Communications Privacy Act* (ECPA) and other federal statutes to obtain telephone subscriber and toll billing records information and other information protected by the ECPA. Such training should cover not only the provisions of the ECPA, but also other federal statutes and regulations governing the FBI's authority to obtain to such records, including the Pen Register Act, the federal regulation governing subpoenas for toll billing records of reporters, and the FBI's administrative subpoena authorities.

3. The FBI should periodically review its existing guidance and directives to determine if clarifications or updates are needed to describe the authority of FBI personnel serving in "acting" positions (whether appointed or on temporary duty assignments) to sign documents or approve activities for which signature or approval authority is delegated by the FBI Director. As described in Chapter Four of this report, CTD officials signed improper blanket NSLs while serving as Acting Deputy Assistant Directors. At the time these NSLs were signed, the FBI had not issued guidance on whether

FBI personnel serving in acting positions were authorized to sign NSLs. To ensure that all FBI personnel serving in acting positions understand what they are authorized or not authorized to approve or sign under various federal statutes, Attorney General Guidelines, and FBI policies, we believe the FBI should clarify the authorities of FBI personnel serving in various acting positions.

4. The FBI OGC should review existing contracts between the FBI and private entities or individuals that provide for the FBI's acquisition of telephone records, e-mail records, financial records, or consumer credit records to ensure that the methods and procedures used by the FBI for requesting, obtaining, storing, and retaining these records are in conformity with the NSL statutes and other applicable federal statutes, regulations, Executive Orders, Attorney General Guidelines, and FBI policy.

5. The FBI should issue a directive requiring that FBI personnel, including FBI OGC attorneys with expertise pertinent to the subject matter of the contract, review contract proposals, responses to requests for contract proposals, and proposed contracts or arrangements with wire or electronic communications service providers. The objective of the review should be to ensure that any records requested, obtained, stored, or retained pursuant to any such contracts are done so in conformity with applicable federal statutes, regulations, Executive Orders, Attorney General Guidelines, and FBI policy.

As described in Chapter Two of this report, NSLB attorneys did not review the contracts with the three on-site providers until after reviewing a draft of the OIG's first NSL report. Although the FBI has stated that these contracts did not require FBI OGC review, the FBI OGC informed the House Judiciary Committee that procurement attorneys reviewed certain portions of the contract documents relating to the justification and approval of the contacts.[298] The FBI also informed the Judiciary Committee that FBI OGC attorneys will be more involved in the contract review process in the future. To ensure that FBI personnel who are familiar with the laws and policies affected by such contracts review analyze these important contract proposals and contracts before they are finalized, the FBI should require that FBI personnel with relevant expertise – not just procurement attorneys

---

[298] Letter to The Honorable John Conyers, Jr., Responses of the Federal Bureau of Investigation Based Upon the March 20, 2007 Hearing Before the House Judiciary Committee Regarding The FBI's Use of National Security Letters Requested by April 19, 2007 Letter (January 13, 2009), at 6-7.

– review contract proposals and approve the final wording of such contracts.

6. If the FBI places employees of communications service providers in the same work space as FBI employees, the FBI should establish appropriate written guidance, supervisory and oversight procedures, and appropriate training to ensure that the methods and procedures used to obtain records from the providers conform to the ECPA and other applicable federal statutes, regulations, Executive Orders, Attorney General Guidelines, and FBI policy.

7. The FBI should issue guidance specifically directing FBI personnel that they may not use the practices known as hot number [redacted] to obtain calling activity information from electronic communications service providers.

8. The FBI should issue guidance regarding when FBI personnel may issue [redacted] community of interest [redacted] requests. As described in Chapter Two, in November 2007 the FBI Counterterrorism Division prepared draft guidance that would require advance determinations of the relevance of [redacted] telephone numbers included in the community of interest [redacted] requests. The draft guidance also would require that senior FBI officials and a Department attorney approve such requests and that telephone numbers [redacted] pursuant to these requests be documented for purposes of congressional reporting on NSL usage. We recommend that the FBI finalize and issue this guidance to FBI personnel.

9. The FBI should carefully review the circumstances in which FBI personnel asked the on-site communications service providers [redacted] on specified "hot numbers" to enable the Department to determine if the FBI obtained calling activity information under circumstances that trigger discovery or other obligations in any criminal investigations or prosecutions.

10. The Department should determine if, in addition to the grand jury subpoenas identified in this review, the Department has issued other grand jury subpoenas in media leak investigations that included a request for [redacted] community of interest or calling circle [redacted] If so, the Department should determine whether at the time the subpoenas were issued responsible Department personnel were aware of or suspected contacts between the target numbers in the subpoenas and members of the news media and whether the Department obtained the toll billing records of news reporters in compliance with Departmental regulations, including the notification requirements.

11. The FBI, in conjunction with the National Security Division (NSD) and other relevant Department components, should review current policies and procedures governing [redacted] reporters by Department personnel. We recommend that after conducting this review, the FBI and the NSD consider under what circumstances FBI personnel may [redacted] reporters, and specifically whether approval by senior FBI officials at the level of an Assistant Director or higher should be required for [redacted]

12. The FBI, in conjunction with the NSD, should determine whether any FISA Court orders for electronic surveillance or pen register/trap and trace devices currently in place relied upon declarations containing FBI statements as to the source of subscriber information for telephone numbers listed in exigent letters or the 11 blanket NSLs. If the FBI and the NSD identify any such pending orders, we recommend that the FBI and the NSD determine if any of the statements characterizing the source of subscriber information are inaccurate or incomplete. If any declarations are identified as containing inaccurate or incomplete statements, we recommend that the FBI and the NSD determine whether any of these matters should be referred to the FBI Inspection Division or the Department's Office of Professional Responsibility for further review.

13. The FBI and the Department should consider how the FBI may use [redacted] when seeking telephone billing records, particularly with respect to [redacted] We also recommend that the Department notify Congress of this issue and of the OLC opinion interpreting the scope of the FBI's authority under it, so that Congress can consider the [redacted] and the implications of its potential use.

III. OIG Conclusion on Exigent Letters and Other Improper Requests for Telephone Records

In sum, in this review we found widespread use by the FBI of exigent letters and other informal requests for telephone records. These other requests were made by e-mail, face-to-face, on post-it notes, and by telephone, without first providing legal process or even exigent letters. The FBI also obtained telephone records through improper "sneak peeks," community of interest [redacted], and hot-number [redacted] Many of these practices violated FBI guidelines, Department policy, and the ECPA statute. In addition, we found that the FBI also made inaccurate statements to the FISA Court related to its use of exigent letters. Some of the most troubling improper requests for telephone records occurred in media leak cases, where the FBI sought and acquired reporters' telephone toll billing records

and calling activity information without following federal regulation or obtaining the required Attorney General approval.

Our review also found that the FBI's initial attempts at corrective action were seriously deficient, ill-conceived, and poorly executed. However, after our first NSL report was issued in March 2007, the FBI took appropriate action to stop the use of exigent letters and to address the problems created by their use. Yet, we believe the FBI should take additional action regarding the use of other improper requests for telephone records. We therefore believe the FBI should implement the recommendations in this report and ensure that similar abuses of exigent letters or other improper requests for telephone records do not occur in the future.

APPENDIX

U.S. Department of Justice
Federal Bureau of Investigation

In Reply, Please Refer to File No.

FBIHQ
935 Pennsylvania Avenue NW
Washington, DC 20535
Room [redacted]
May 27, 2003

[redacted]

Telephone: [redacted]
Facsimile:
Attn: [redacted]

RE: Special Project / [redacted]

Dear Mr. [redacted]:

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

Sincerely,

Glenn Rogers
Unit Chief
Communications Analysis Group
[redacted]

By: [redacted]
Supervisory Special Agent

3020 X
NSL
[redacted]000021

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 4, 2006

[redacted]

Attention: [redacted]

Re: Special Project / SSA [redacted]

Dear Mr. [redacted]

Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. National Security Letters directing you to provide this information will be processed and served upon [redacted] as expeditiously as possible.

For the following U.S. numbers:

[redacted]

Sincerely,

Bassem Youssef
Unit Chief
Communications Analysis Unit

By: [redacted]
Supervisory Special Agent