

UNCLASSIFIED



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



A Review of the FBI's Use of Section 215 Orders for Business Records in 2012 through 2014

NOTE

A classified version of this report was completed in June 2016 and, as required by the USA Freedom Act, was provided to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives. We also provided the report to cleared members of other relevant Congressional oversight committees. This unclassified version of the report follows the completion of a classification review by the FBI and the Intelligence Community and contains redactions of information that they determined to be classified.

EXECUTIVE SUMMARY	iii
I. INTRODUCTION	1
A. Methodology of the OIG Review	1
B. Organization of the Report	3
II. BACKGROUND	4
A. Legal Background	4
B. The Process for Seeking Section 215 Orders.....	8
C. Minimization Procedures	10
1. Interim Minimization Procedures.....	10
2. Final Minimization Procedures.....	12
3. Retroactive Application of the Final Procedures	16
D. Compliance Issues	17
III. STATUS OF RECOMMENDATIONS	19
A. Handling of Metadata Under the Final Procedures.....	19
1. Initial Review of Metadata.....	20
2. Other Provisions Relating to Metadata	20
B. Retention and Dissemination of U.S. Person Information.....	23
1. "Necessary to Understand Foreign Intelligence Information".....	23
2. Dissemination of Information Relating to Computer Intrusions or Attacks.....	24
IV. OVERVIEW OF BUSINESS RECORDS ORDERS ISSUED FROM 2012 THROUGH 2014	24
A. The Overall Number of Business Records Orders	25
B. Business Records Orders by FBI Field Office	28
C. Analysis of Business Records Orders.....	28
1. Types of Investigations from which Business Records Orders Originated.....	29
2. Subjects of Business Records Orders.....	30
3. Types of Records Requested in Approved Business Records Orders Filed on Behalf of the FBI	31
4. Timeliness of the Business Records Process.....	33
V. SELECTED SECTION 215 ORDERS OBTAINED BETWEEN 2012 AND 2014	37
A. Selected Uses of Section 215 Authority.....	38
1. Business Records Orders ██████████ Related FBI Counterterrorism Investigations	38
2. Multiple Business Records Orders in an FBI Counterintelligence Investigation	43

3.	Request for [REDACTED] Used to [REDACTED] [REDACTED] (Section 215 Order Issued May 2012).....	53
4.	Requests for [REDACTED] (Section 215 Orders Issued 2011, 2012, and November 2014)	55
5.	Request for [REDACTED] (Section 215 Orders Issued October 2013).....	57
6.	Multiple Business Records Orders in an FBI Counterintelligence Investigation	58
B.	Compliance Incidents	60
1.	Full and Partial Subject Lines from [REDACTED]	60
2.	[REDACTED]	61
3.	DWS Release of Quarantined Records.....	63
C.	Current Status of Bulk Collection under Section 215	63
VI.	CONCLUSION	65

EXECUTIVE SUMMARY

This Executive Summary provides a brief overview of the results of the Department of Justice (Department or DOJ) Office of the Inspector General's (OIG) review of the Federal Bureau of Investigation's (FBI) use of the investigative authority granted by Section 215 of the Patriot Act between 2012 and 2014. Section 215 is often referred to as the Foreign Intelligence Surveillance Act (FISA) "business records" provision. This is the OIG's fourth review of the FBI's use of FISA business records. Three previous reports issued in March 2007, March 2008, and May 2015 addressed the FBI's use of Section 215 authority between 2002 and 2009.

This current review is mandated by the USA Freedom Act of 2015.¹ The USA Freedom Act, signed into law on June 2, 2015, directs the OIG to issue within 1 year of the date of enactment a report examining the FBI's use of Section 215 authority for calendar years 2012 to 2014, addressing any noteworthy facts or circumstances relating to Section 215 orders, any illegal or improper use of Section 215 authority, the effectiveness of Section 215 as an investigative tool, and the adequacy of procedures used to "minimize" U.S. person information obtained in response to Section 215 orders.

To conduct this review, the OIG reviewed the Standard Minimization Procedures for Tangible Things Obtained Pursuant to Title V of the Foreign Intelligence Surveillance Act adopted by the Attorney General on March 7, 2013 ("Final Procedures"). We also examined over 90,000 documents obtained from the FBI and the Department's National Security Division's (NSD) Office of Intelligence, including files relating to each FISA Court order approving use of Section 215 authority between 2012 and 2014, Department reports to Congress concerning that use during calendar years 2012 through 2014, documents detailing compliance incidents related to the FBI's use of Section 215 authority, reports documenting the results of internal reviews conducted by NSD between 2012 and 2014, e-mails relating to approved and withdrawn business records applications, and FBI and NSD policies and training materials related to the Final Procedures.

We reviewed each of the FISA Court-approved orders for business records between 2012 and 2014 in order to provide an overview of the characteristics of those orders and the underlying investigations in which they were obtained. In addition, we conducted a more in-depth analysis of the FBI's use of this authority in national security investigations by reviewing a sample of Section 215 orders and withdrawn applications selected from two FBI field offices that had relatively large and diverse uses of Section 215 orders, and by conducting field visits in those offices. Over the course of the review, we also interviewed more than 50 individuals from the FBI and the Department, including Section

¹ "USA FREEDOM Act" is an acronym for *United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, Pub. L. No. 114-23, 129 Stat. 268 (2015). We refer to it in this report as the USA Freedom Act.

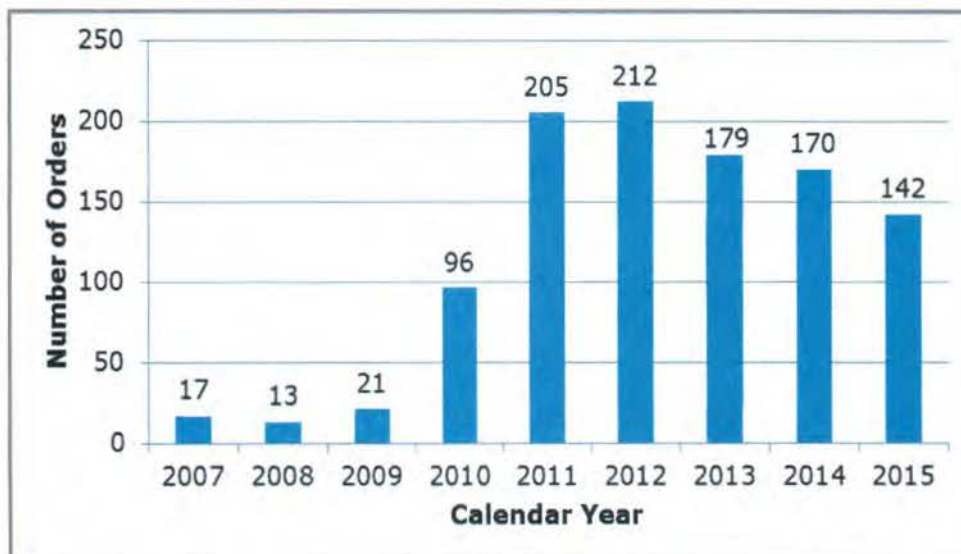
and Unit Chiefs from NSD's Office of Intelligence and the FBI's National Security Law Branch (NSLB), and attorneys, case agents, and supervisors who worked on individual Section 215 orders.

In this report, we provide an overview of the FBI's use of Section 215 authority between 2012 and 2014 that describes the number of Section 215 orders obtained, the type of information requested, the types of FBI cases in which business records orders were used, and the average time between initiation of a business records order request by an FBI field office and issuance of an order by the FISA Court. Our review found that the number of business records orders obtained by the FBI increased significantly between 2007 and 2012, largely driven by the refusal of several communications providers to produce transactional records for e-mail [REDACTED] accounts (known as Electronic Communication Transaction Records, or ECTRs) in response to FBI National Security Letters (NSLs).

Between 2012 and 2014, the FISA Court approved 561 business records orders.² However, as shown in Figure 1, between 2012 and 2014, the number of business records orders dropped from a 9-year high of 212 in 2012 to 170 in 2014 (19.8%). A further decrease occurred in 2015, when the number of orders fell to 142.

² After reviewing a draft of this report, NSD commented that references to the number of business records orders should be changed to the number of approved applications for business records orders. The OIG understands that some business records applications result in more than one order. For example, the FISA Court may issue orders to four separate providers when approving a single application requesting ECTRs for four e-mail addresses. We also recognize that NSD reports the number of applications submitted to the FISA Court in its annual reports to Congress. Nonetheless, we decided to retain the references to the number of business records orders throughout this report as a matter of convenience.

FIGURE 1
Total Number of Approved Business Records Orders,
by Calendar Year, 2007-2015³



Source: FBI.

An NSD Deputy Unit Chief noted the decline after 2012 and told the OIG that the number of ECTRs decreased more than other types of records. He attributed the decline in part to revelations by Edward Snowden about the U.S. government's use of Section 215 to collect bulk telephony metadata, both in terms of the stigma attached to use of Section 215 and increased resistance from providers. In comments provided to the OIG after reviewing a draft of this report, NSD stated that the degree to which the Snowden disclosures affected the number of business records applications was somewhat speculative, and attributed the FBI's increasing use of taskings under Section 702 as likely a "notable cause" in the decrease in business records requests. NSD stated that during the relevant period (and continuing today) it suggested that FBI withdraw business records requests for accounts used by non-U.S. persons located overseas that can instead be tasked under Section 702.⁴ Agents also told the OIG that they increasingly were electing to use criminal legal process instead of FISA authority

³ This table includes the total number of dockets for 2013 (179). This number differs slightly from the number of approved applications for business records the Department reported to Congress for 2013 (178). The OIG recognizes that one submission in 2013 was a copy of the Final Procedures, which did not result in a FISA Court order. As described below, we excluded this docket from our numbers for purposes of analysis.

⁴ Section 702 of the FISA Amendments Act allows the government to acquire foreign intelligence by targeting non-U.S. persons reasonably believed to be outside the United States. Under Section 702, the government is not required to obtain individual surveillance orders from the FISA Court. Instead, the FISA Court approves targeting procedures to ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States, and minimization procedures to guard against the inadvertent collection, retention, and dissemination of U.S. person information.

in counterterrorism and cyber investigations because of their frustrations with the lack of timeliness and the level of oversight in the business records process.

We analyzed data for [REDACTED] of the 561 orders approved during our review period.⁵ Between 2012 and 2014, of the [REDACTED] business records orders analyzed, [REDACTED] business records orders included requests for ECTRs, representing [REDACTED] of all non-bulk orders, compared to [REDACTED] orders in the OIG's previous review period between 2007 and 2009, which constituted [REDACTED] of non-bulk orders.

The median time needed to obtain business records orders during our review period from initiation of a request by a field office until issuance of the order by the FISA Court was 115 days.⁶ While several NSD witnesses said that the volume of requests did not significantly impact their processing of business records orders, others acknowledged that there had been delays in the process "because things get backed up." One NSLB attorney told the OIG that he was "embarrassed" at how long the business records process takes, stating, "We are asking for less [than a full FISA], and it's taking twice as long." According to the witnesses we interviewed, both NSD and NSLB have taken steps to improve the business records process, including streamlining the drafting and review process for ECTRs.

In addition, the OIG found that Section 215 business records orders were used far more frequently in counterintelligence cases than as a counterterrorism or cyber tool. Of the [REDACTED] total orders we analyzed, [REDACTED] were obtained in counterintelligence cases, [REDACTED] in counterterrorism cases, and [REDACTED] in cyber cases. Agents told us that Section 215 orders frequently are [REDACTED]

[REDACTED], while agents handling counterterrorism and cyber cases in some instances can open a parallel criminal case and use the grand jury process to obtain the same information more quickly and with less oversight than a business records order. In particular, agents [REDACTED]

[REDACTED] explaining that the length of time needed to obtain a business records order [REDACTED]

⁵ We reviewed all 561 orders approved during our review period, but excluded [REDACTED] orders in our analysis for statistical purposes: [REDACTED]

⁶ FISA Court rules provide for submission of a proposed application, an advance copy of an application commonly called a "read" copy, no later than 7 days before the government seeks to have the matter entertained by the FISA Court. Our analysis included the time that applications and proposed orders were with the FISA Court to provide the most accurate measurement of the time needed for the FBI to obtain business records orders. While we do not have complete data regarding the FISA Court's processing of business records applications, we were informed that "read" copies generally are provided the week before, and the orders signed within a day or two of submission of the final application. No witnesses cited delays with the FISA Court as an issue.

[REDACTED]

Our report describes [REDACTED] Section 215 applications and orders between 2012 and 2014 that illustrate the varied uses of Section 215 authority. While the FBI used business records orders most frequently to obtain transactional records for e-mail [REDACTED]

[REDACTED]. We also describe several instances where the FBI wanted to use Section 215 authority to obtain particular materials but ultimately chose not to do so, such as [REDACTED].

Agents expressed concern about the length of the process to obtain a business records order, but also told us that Section 215 authority continued to be a valuable investigative tool when companies would not voluntarily produce material sought by the FBI or produce it in response to other investigative authorities. As with our previous reviews, the majority of agents we interviewed did not identify any major case developments that resulted from use of the records obtained in response to Section 215 orders, but told us that the material produced pursuant to Section 215 orders was valuable as a building block of the investigation, and was used to support other investigative requests, develop investigative leads, and corroborate other information. However, in at least two cases, agents we interviewed told us that the business records obtained in their investigation provided valuable information that they would not otherwise have been able to obtain. In other instances, case agents told us that they used the information obtained under Section 215 to exculpate a subject and close the investigation.

The OIG reviewed three compliance incidents that affected numerous business records orders between 2012 and 2014. The first involved the systemic overproduction of full and partial e-mail subject lines by two providers, [REDACTED], which the OIG determined affected [REDACTED] business records orders. In a second compliance incident, [REDACTED] in response to a single business records order, including some [REDACTED]. The FBI subsequently determined that previous [REDACTED] likely contained similar [REDACTED] and worked with the provider to fix the error. A third compliance incident resulted from a system-wide error in an FBI database that released business records returns from a quarantined area prior to initial review and allowed access to un-minimized data. All of these incidents were reported to the FISA Court.

As noted above, during our review period, there were [REDACTED] FISA Court-approved orders issued in connection with [REDACTED]

[REDACTED]. Our third Section 215 report discussed [REDACTED] at length, including the specialized minimization procedures that applied to [REDACTED] reported compliance incidents, and detailed the status of [REDACTED] through May 2015. The USA Freedom Act's revisions to the business records provisions of FISA [REDACTED]
[REDACTED]
[REDACTED].

As part of this review, we also examined the progress the Department and the FBI made in addressing three relevant recommendations from the OIG's March 2008 and May 2015 reports. In the 2008 report, we recommended that the Department implement final minimization procedures, develop procedures for reviewing materials received in response to business records orders issued by the Foreign Intelligence Surveillance Court (FISA Court) to ensure that they do not contain "overproduced" information outside the scope of orders, and develop procedures for handling overproductions. In our May 2015 report, we found that the Department had adopted Final Procedures implementing the OIG's recommendations, but identified several terms used in the Final Procedures that we believed required clarification, including with regard to the minimization of U.S. person information. Based on the information obtained in our current review, we concluded that the Department and the FBI have made these clarifications. We therefore have closed these remaining recommendations.

However, based on the concerns expressed by agents about the time needed to obtain business records orders, we recommend that the FBI and the Department continue to pursue ways to make the business records process more efficient, particularly for applications related to cyber cases where agents

[REDACTED]. Potential measures include using the FBI's FISA Management System (FISAMS) data to track the timeliness of Section 215 applications, using alerts within FISAMS to identify applications that have lingered past a certain period of time without review, and implementing a streamlined drafting and review process [REDACTED]

I. INTRODUCTION

Section 215 of the Patriot Act, otherwise known as the business records provision, allows the Federal Bureau of Investigation (FBI) to acquire “any tangible things (including books, records, papers, documents, and other items) for an investigation. . .” to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, provided that an underlying investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment.⁷ The FBI may use this investigative method only in Preliminary and Full Investigations, and the information sought must be relevant to an open, predicated national security investigation.

This is the Department of Justice (Department or DOJ) Office of the Inspector General’s (OIG) fourth review of the FBI’s use of investigative authority granted by Section 215. The OIG has issued three previous reports regarding the FBI’s use of the business records provision: in March 2007, covering calendar years 2002 to 2005; in March 2008, covering calendar year 2006; and in May 2015, covering calendar years 2007 to 2009.

This fourth review is mandated by the USA Freedom Act of 2015, signed into law on June 2, 2015. The USA Freedom Act directs the OIG to issue within 1 year of the date of enactment a report examining the FBI’s use of Section 215 authority for calendar years 2012 to 2014. As required by the USA Freedom Act, this report addresses noteworthy facts or circumstances relating to Section 215 orders, any illegal or improper use of Section 215 authority, the effectiveness of Section 215 as an investigative tool, and the adequacy of procedures used to “minimize” U.S. person information obtained in response to Section 215 orders.

A. Methodology of the OIG Review

To conduct this review, the OIG examined over 90,000 pages of material obtained from the FBI and the Department’s National Security Division’s (NSD) Office of Intelligence. These documents included files relating to each FISA Court order approving use of Section 215 authority between 2012 and 2014; Department reports to Congress concerning that use during calendar years 2012 through 2014; documents detailing compliance incidents related to the FBI’s use of Section 215 authority; reports documenting the results of Accuracy and Minimization Reviews conducted by NSD between 2012 and 2014; e-mails relating to approved and withdrawn business records applications; minimization procedures in effect during the review period; and FBI and NSD policies and training materials related to final minimization procedures adopted in 2013.

⁷ The term “USA PATRIOT Act” is an acronym for the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001). We refer to it as “the Patriot Act” in this report.

We reviewed each of the 561 Foreign Intelligence Surveillance Act (FISA) Court-approved orders for business records between 2012 and 2014 in order to provide an overview of the characteristics of those orders and the underlying investigations in which they were obtained.⁸ In order to conduct an in-depth analysis of the FBI's use of business records authority, we conducted field visits to two FBI field offices: the [REDACTED]. We identified these field offices based on the overall number and variety of business records orders obtained during the review period. [REDACTED], we reviewed each of the [REDACTED] business records orders obtained during the review period. [REDACTED], we reviewed a sample of [REDACTED] of the [REDACTED] business records orders obtained, which we selected based on various factors, including unique use of Section 215 authority, the type of investigation, or the occurrence of compliance incidents. During these field visits, we examined documents in the FBI's case management system and interviewed agents, supervisors, and counsel about the FISA business records process, the use of Section 215 authority in their individual cases, and the application of the relevant minimization procedures. In several instances, we also examined the materials produced in response to business records orders. We selected [REDACTED] of these applications for more detailed analysis to highlight the varied and evolving uses of Section 215 authority.

In addition to the orders approved by the FISA Court, between 2012 and 2014 there were [REDACTED] pending and [REDACTED] withdrawn applications for Section 215 orders.⁹ We reviewed [REDACTED] withdrawn requests or applications originating from [REDACTED] and questioned agents about [REDACTED] of these. We also reviewed [REDACTED] requests submitted to NSD but not filed with the FISA Court, and [REDACTED] proposed applications filed with the FISA Court as "read" or advance copies that NSD ultimately withdrew prior to formally filing. Where the applications presented novel or unique legal issues, we questioned NSD attorneys about the reasons for these withdrawals.

As noted earlier, during our review period, there were [REDACTED] FISA Court-approved orders related to [REDACTED]. Beginning in 2006, the FBI obtained Section 215 orders [REDACTED]. Our third report discussed [REDACTED] at length, including the specialized minimization procedures that applied to [REDACTED] reported compliance incidents, and the status of [REDACTED] through May 2015. On June 2, 2015, the USA Freedom Act ended bulk collection under Section 215 by requiring that applications for business records identify a person, account, address, or personal

⁸ We reviewed all 561 orders approved during our review period, but excluded [REDACTED] orders in our analysis for statistical purposes, as described in more detail in Section IV.C: [REDACTED] orders concerning [REDACTED], and [REDACTED] order memorializing the Final Procedures.

⁹ Pending applications include applications generated between 2012 and 2014 but not provided to NSD for further processing or submitted to the FISA Court for further approval.

device, or any other specific identifier.¹⁰ See 50 U.S.C. §§ 1861(b)(2), (k)(4) (2015), *as amended by* USA Freedom Act of 2015, §§ 101, 103, 107, 109. Our report provides a brief status update [REDACTED] in light of the changes instituted by the USA Freedom Act.

Over the course of this review, we interviewed more than 50 people from the FBI and the Department, including Section and Unit Chiefs from the FBI's National Security Law Branch (NSLB) and NSD's Office of Intelligence and attorneys, case agents, and supervisors who worked on Section 215 orders. We did not question FBI and NSD personnel about the specifics of every order, nor did we conduct an independent compliance review of each use of Section 215 authority between 2012 and 2014. For purposes of this report, we relied on the Department's reporting to the FISA Court, the FBI's reporting to the Intelligence Oversight Board (IOB), and the reports summarizing Accuracy and Minimization Reviews conducted by NSD in FBI field offices to identify compliance incidents that occurred during the relevant time period.

B. Organization of the Report

This report is divided into six sections. After this introduction, we describe in Section II the legal background related to Section 215 authority, the process for obtaining a Section 215 order, the procedures applicable to the use of business records material, and the procedures for reporting compliance incidents to the FISA Court and the IOB.

In Section III, we discuss the status of recommendations the OIG made in previous reports concerning the FBI's use of Section 215 authority.

In Section IV, we provide an overview of the FBI's use of Section 215 authority between 2012 and 2014. We describe the number of Section 215 orders approved, the type of information requested, the number of FBI offices that used the authority, and the types of investigations in which Section 215 orders were sought.

In Section V, we provide a more detailed discussion of [REDACTED] business records orders obtained between 2012 and 2014. We describe the information requested, the purpose of the requests, the material produced, the manner in which it was used, and any compliance incidents that occurred. We also describe three compliance incidents that affected numerous business records orders during our time period, and briefly discuss the status of [REDACTED] of the USA Freedom Act.

Finally, Section VI contains our conclusions.

¹⁰ As described in more detail below, the effective date of these changes was within 180 days of the date of enactment, which was November 29, 2015. The USA Freedom Act also eliminated bulk collection using pen register/trap and trace authority or various National Security Letter authorities by requiring use of a specific selection term. See USA Freedom Act of 2015, §§ 201, 501.

II. BACKGROUND

This section provides a brief description of the legal background related to Section 215 authority and the process for obtaining Section 215 orders.

A. Legal Background

The Foreign Intelligence Surveillance Act of 1978 (FISA) requires the FBI to obtain an order from the FISA Court to conduct electronic surveillance to collect foreign intelligence information.¹¹ In 1998, Congress amended FISA to authorize the FBI to apply to the FISA Court for orders compelling common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities to “release records in [their] possession” to the FBI. The amendment did not further define “records.” This provision, which was codified at 50 U.S.C. § 1862, became known as the “business records” provision.¹²

The 1998 amendment required the FBI to specify that the business records were sought for an investigation to gather foreign intelligence information or an investigation concerning international terrorism, and that there were “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” 50 U.S.C. § 1862 (2000). This language meant that the FBI was limited to obtaining information regarding a specific person or entity the FBI was investigating and about whom the FBI had individualized suspicion. The amendment also prohibited the entity complying with the order from disclosing either the existence of the order or any information produced in response to the order.

The authority granted by the 1998 amendment was rarely used. Between enactment of the amendment and passage of the Patriot Act in October 2001, the FBI obtained only one FISA order for business records.

In October 2001, Section 215 of the Patriot Act significantly expanded the business records provision. The pertinent part of Section 215 provides:

[T]he Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special

¹¹ FISA provides two definitions of “foreign intelligence information.” Under 50 U.S.C. § 1801(e)(1), foreign intelligence information means information that relates to, and if concerning a U.S. person is necessary to, the ability of the United States to protect against (1) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (2) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (3) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. Under 50 U.S.C. § 1801(e)(2), foreign intelligence information includes information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person is necessary to, the national defense or the security of the United States, or the conduct of the foreign affairs of the United States.

¹² 50 U.S.C. § 1862(b)(2)(B) (1998), *as amended*, 50 U.S.C. § 1861 (2001).

Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

50 U.S.C. § 1861(a)(1) (2001). While the 1998 amendment limited the FBI's business records authority to four types of businesses, the 2001 language did not contain any such limitation. Section 215 also expanded the categories of documents obtainable under the business records provision from "records" to "any tangible things (including books, records, papers, documents, and other items)."

In addition, Section 215 lowered the evidentiary threshold to obtain a business records order. Rather than requiring the FBI to show that the requested information pertained to a person under investigation, Section 215 required that the items sought need only be "for an authorized investigation conducted in accordance with [applicable law and guidelines] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2) (2001). This standard, referred to as the relevance standard, permits the FBI to seek information concerning persons connected in some way to a person or entity under investigation.

Congress twice amended Section 215 in 2006. The first legislative amendment, the USA PATRIOT Improvement and Reauthorization Act of 2005 (Reauthorization Act), was signed into law on March 9, 2006. The Reauthorization Act required that an application for a business records order establish "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."¹³ 50 U.S.C. § 1861(b)(2)(B) (2006). At the same time, the Reauthorization Act provided a presumption of relevance for tangible things that pertain to foreign powers, agents of foreign powers, suspected agents of foreign powers who are the subjects of authorized investigations, or individuals in contact with, or known to, suspected agents of foreign powers who are the subjects of authorized investigations. If an application demonstrates that the information requested pertains to one of these four entities or individuals, it is presumptively relevant to an authorized investigation.

The Reauthorization Act also authorized the collection of certain sensitive records, including library, medical, educational, and tax return records. However, it required that applications for sensitive records be approved by the FBI Director or his specified designee, and required specific reporting about

¹³ *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. 109-177, 120 Stat. 196 to 198 (2006).

these records to Congress.¹⁴ The Reauthorization Act also established a process for recipients of Section 215 orders to challenge their legality before a FISA Court judge.

The second legislative amendment, the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, included additional changes to Section 215. For example, these amendments included a provision allowing a recipient of a Section 215 order to petition the FISA Court to modify or set aside the nondisclosure requirement after 1 year from the issuance of the order if certain findings are made.¹⁵

Section 215, along with other provisions of the Patriot Act, originally was scheduled to sunset on December 31, 2005. The Reauthorization Act extended Section 215 for 4 years, until December 31, 2009. Congress subsequently extended Section 215 to June 1, 2015.

In June 2013, information about the NSA's bulk telephony metadata program was publicly disclosed by Edward Snowden.¹⁶ These disclosures revealed, among other things, that the FISA Court had approved Section 215 orders authorizing the bulk collection of call detail records. The telephony metadata collected by the NSA included information from local and long-distance telephone calls, such as the originating and terminating telephone number and the date, time, and duration of each call.¹⁷ The disclosures prompted widespread public discussion about the bulk telephony metadata program and the proper scope of government surveillance, and ultimately led Congress to end bulk collection by the government in the USA Freedom Act.¹⁸

Amid public debate about the bulk telephony metadata program, the sunset provisions of the Reauthorization Act took effect at 12:01 a.m. on June 1, 2015, temporarily reverting the business records provision to the much more limited version in effect between 1998 and October 2001.¹⁹ On June 2, 2015, President Obama signed the USA Freedom Act. While the USA Freedom Act did

¹⁴ As permitted by the Reauthorization Act, the FBI Director delegated approval authority for these records to the Deputy Director and the Executive Assistant Director for the FBI's National Security Branch.

¹⁵ See *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*, Pub. L. No. 109-178, 120 Stat. 278, 280.

¹⁶ See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, *The Guardian* (Jun. 6, 2013). As described in more detail below, metadata refers to dialing, routing, addressing, or signaling information associated with a communication, but does not include any information concerning the substance, purport, or meaning of the communications.

¹⁷ As we described in our second and third reports, NSA placed the call detail records in an archive and then ran "queries" against this archive to identify [REDACTED]. The telephone numbers used to query the archive were telephone numbers that met the "reasonable articulable suspicion" standard.

¹⁸ See generally Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 Wash. & Lee L. Rev. 1307, 1321-22, 1325, 1334 (Summer 2015).

¹⁹ See *id.*

not substantively change the standard for obtaining business records linked to a particular person or identifier, it ended bulk collection under Section 215 by requiring that applications for business records include a “specific selection term,” defined as “a term that specifically identifies a person, account, address, or personal device, or any other specific identifier.” 50 U.S.C. §§ 1861(b)(2), (k)(4) (2015), *as amended by USA Freedom Act of 2015*, §§ 101, 103, 107. This provision became effective 180 days after the date of enactment, ending bulk collection by the government as of November 29, 2015. See USA Freedom Act of 2015, § 109.

To allow the government to continue to obtain call data, the USA Freedom Act created a new mechanism that allows the government to obtain call detail records from providers within two “hops” of the specific selection term on an ongoing basis for 180 days from the date of the FISA Court order.²⁰ Each application to obtain these records must include (a) a specific selection term to be used as the basis for the production of the call detail records, 50 U.S.C. § 1861(b)(2)(A); (b) a statement of facts showing that there are reasonable grounds to believe that the call detail records being sought are relevant to an authorized investigation and that there is a reasonable, articulable suspicion that the specific selection term is associated with a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation thereof, 50 U.S.C. § 1861(b)(2)(C)(i) and (ii); and (c) an enumeration of the minimization procedures adopted by the Attorney General that are applicable to the handling of call detail records obtained by the government in response to the requested order, 50 U.S.C. § 1861(b)(2)(D).²¹

According to NSD, if the FISA Court finds that the application meets the statutory requirements, it will order the production of a first set of records (the “first hop”) using the specific selection term, and a second set of records (the “second hop”) using session-identifying information (such as originating or terminating telephone numbers) or telephone calling card numbers identified by the specific selection term. Session-identifying information and telephone calling card numbers may be identified in the first hop productions or from other information already in the government’s possession. The FISA Court has

²⁰ The term “call detail record” means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call. It does not include the contents of any communication; the name, address, or financial information of a subscriber or customer; or cell site location or global positioning system (GPS) information. See 50 U.S.C. § 1861(k)(3). As a result, the FBI may not obtain identifying, financial, or location information on the basis of an individual being in first- or second-degree contact with the original person, account, address, or personal device, or other specific identifier used as a specific selection term.

²¹ The “reasonable, articulable suspicion” (RAS) standard [REDACTED]. The FISA Court orders permitted authorized personnel to search the data collected under those orders when “based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that a particular known identifier is associated with” one or more of the foreign powers identified in the orders. We discuss the evolution of the [REDACTED] RAS standard in our May 2015 report.

concluded that FISA, as amended by the USA Freedom Act, does not require a showing of relevance for second hop records. To guard against overbroad collection, the USA Freedom Act requires “the prompt destruction of all call detail records” collected by the government not determined to be foreign intelligence information. See 50 U.S.C. §§ 1861(b)(2)(C), (c)(2)(F), *as amended by USA Freedom Act of 2015*, § 107.

The USA Freedom Act also added a provision allowing the Attorney General to require the emergency production of business records when certain criteria are met, including applying relevant minimization procedures and obtaining a FISA Court order approving the production within 7 days of the emergency authorization. See 50 U.S.C. § 1861(i), *as amended by USA Freedom Act of 2015*, § 102. Finally, the USA Freedom Act extended the sunset date for Section 215 as amended until December 15, 2019. See USA Freedom Act of 2015, § 705(a).

B. The Process for Seeking Section 215 Orders

As we described in our previous Section 215 reports, the process to obtain and utilize a Section 215 order generally involves five phases: FBI field office initiation and review, FBI Headquarters review, NSD Office of Intelligence review, FISA Court review, and FBI service of the order.

The process to obtain a Section 215 order generally begins when an FBI case agent prepares a business records request form, which requires the agent to provide, among other things, the following information: a brief summary of the investigation, a specific description of the items requested, an explanation of the manner in which the requested items are expected to provide relevant information, and the identity of the custodian or owner of the requested items. The request form must be approved by the agent’s supervisor and the field office’s Chief Division Counsel and Assistant Special Agent in Charge. The approval process is automated through the FBI’s FISA Management System (FISAMS), which sends electronic notifications to each individual responsible for taking the next action in order to process the business records in the field office. After the approvals are completed in the field office, the FISAMS notifies the “substantive desk” (in the Counterterrorism, Counterintelligence, or Cyber Divisions) at FBI Headquarters.

At FBI Headquarters, the business records request form is reviewed and approved by both the substantive desk and NSLB. Once FISAMS delivers the request to the substantive desk, it is assigned to an NSLB attorney who works with the case agent and other FBI personnel to obtain any additional information the NSLB attorney believes is necessary to support the request. The request package then is reviewed by NSLB supervisors and forwarded to NSD, where the request is assigned to an NSD attorney.

The NSD attorney works with the NSLB attorney and case agents to obtain any additional information necessary to include in the draft application and order. NSD uses an internally-created software program called “TurboFISA” that produces a template with standardized language for various types of

business records applications. An NSD supervisor then reviews the draft application package. In most cases, the NSD attorney then sends the draft to the FBI for review, including having agents answer any questions regarding the application. The application is then finalized by NSD. The final application package is returned to the FBI for an accuracy review, and additional edits may be made based on the FBI's review of the final package. Upon completion of the final version of the application, signatures of the designated senior FBI personnel are obtained and an NSD attorney prepares the package for presentation to the FISA Court.

Pursuant to Rule 9 of the FISA Court Rules of Procedure, NSD provides the FISA Court with a proposed application, an advance copy of the application commonly called a "read" copy, no later than 7 days before the government seeks to have the matter entertained by the FISA Court. The FISA Court, through a FISA Court legal advisor, may identify questions or concerns and request changes or additional information to the documents after reviewing the "read" copy. NSD and the FBI then address these questions or concerns and make any necessary revisions to the application and order prior to submitting a formal or final application and order for the Court's approval, or decide to withdraw the application before submission. The FISA Court will either sign the formal submission or request that NSD present the formal application package to the FISA Court at a scheduled hearing. If the FISA Court judge approves the formal application, the judge signs the order.

The order is then entered into FISAMS and served by the FBI field office nearest to the company or provider designated in the order. Among other things, the order sets forth the deadline for producing the items. The FBI can receive business records returns electronically or in hard copy. Hard copies of business records returns typically are sent directly to the case agent. Electronic records, particularly business records returns from certain Internet Service Providers, typically are sent to the FBI's Data Intercept Technology Unit (DITU). DITU then uploads the records into the Data Warehouse System (DWS), the FBI's primary repository for raw FISA-acquired material. Un-minimized business records returns are quarantined in a separate area of DWS that is accessible only to personnel involved in the case. When returns are uploaded, DWS automatically notifies the case agent, who must then review the records in a restricted area of DWS to determine whether the records are responsive to the FISA Court order. If so, DITU releases the records from the quarantined area into DWS, where they are available to FBI personnel with appropriate access. Once the information is in DWS, the case agent must assess its intelligence value. Only information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime may be placed in other FBI electronic storage systems, such as the Automated Case System (ACS) and Sentinel, where the information will be more widely accessible to FBI personnel (discussed in more detail below).²²

²² ACS and its successor, Sentinel, are the FBI's case management systems.

C. Minimization Procedures

FISA requires the FBI to “minimize” U.S. person information it receives in response to business records orders. Under current procedures, this means that the FBI may retain and disseminate nonpublic U.S. person information only if it reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime, referred to as meeting the “FISA Standard.”

The FBI adopted interim minimization procedures for business records returns following the passage of the Reauthorization Act in March 2006, and revised procedures in 2013.²³ Two sets of minimization procedures thus governed business records orders issued between 2012 and 2014: Interim Procedures between January 1, 2012 and June 30, 2013, and Final Procedures after July 1, 2013. In this section we discuss these minimization procedures and describe the decision by FBI and NSD to implement the Final Procedures retroactively.

1. Interim Minimization Procedures

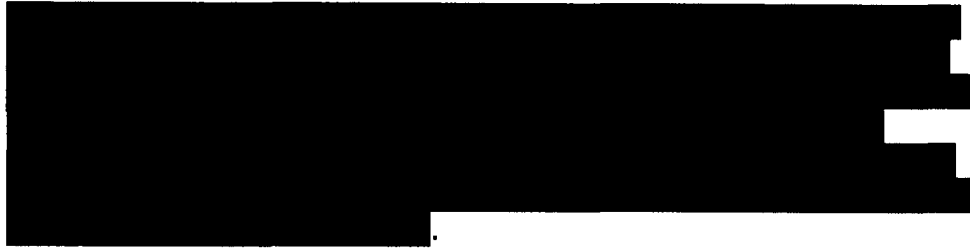
The Reauthorization Act mandated that the Department adopt minimization procedures to govern the retention and dissemination of nonpublic U.S. person information produced in response to a Section 215 order. One critical requirement was that the minimization procedures prohibit the dissemination of nonpublic U.S. person information, unless the identity of the U.S. person was foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime (*i.e.*, met the FISA Standard).

The Department adopted Interim Procedures in September 2006. Rather than providing new procedures designed to comply with the requirements of the Reauthorization Act, the Interim Procedures incorporated six existing provisions from the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines):

- Part I.B.3., which prohibited the FBI from investigating or maintaining information on U.S. persons solely for the purpose of monitoring First Amendment activities or the lawful exercise of Constitutional or statutory rights.
- Part I.C.1., which defined “U.S. person” to include U.S. citizens or lawful permanent residents, unincorporated associations substantially composed of individuals who are U.S. persons, and corporations incorporated in the United States.

- [REDACTED]

²³ See 50 U.S.C. § 1861(g)(2).



- Part VII.A.1., which required that the FBI retain investigative records in accordance with a plan approved by the National Archives and provided for NSD oversight of information obtained in the course of investigations.
- Part VII.B., which allowed the FBI to disseminate information within the Department, to the intelligence community and federal law enforcement agencies, to other federal, state, and local authorities, and to foreign authorities when the information related to the recipient's authorized responsibilities and dissemination was consistent with national security interests.
- Part VIII, which defined certain terms used in the NSI Guidelines, including "foreign intelligence" and "publicly available."

The Interim Procedures stated that these provisions were to be construed to minimize retention and prohibit dissemination of nonpublic U.S. person information, and to prohibit the FBI from disseminating nonpublic U.S. person information that was not foreign intelligence information in a manner that identified a U.S. person, unless the person's identity was "necessary to understand foreign intelligence information or assess its importance" or evidence of a crime. However, the Interim Procedures did not define or explain what "necessary to understand foreign intelligence information or assess its importance" means, nor did they define or provide guidance on what constitutes U.S. person identifying information.

In our March 2008 report, we found that the Interim Procedures did not meet the requirements of the Reauthorization Act because they failed to provide FBI agents with specific guidance regarding the retention and dissemination of nonpublic U.S. person information obtained under Section 215 authority. We recommended that the FBI develop final minimization procedures that provided such guidance, require an initial review of records received in response to business records orders, and provide guidance on handling overproductions (*i.e.*, material outside the scope of the Section 215 order).

Although the FBI stated that it would replace the Interim Procedures with final minimization procedures that addressed the recommendations in the March 2008 report, it had not done so by spring 2009. As a result, in May 2009, a FISA Court judge requested that the FBI voluntarily apply additional minimization procedures to the productions of [REDACTED] related Section 215 orders. The Department agreed to implement these additional minimization procedures and filed reports with the FISA Court describing how the FBI had minimized U.S. person information.

In June 2009, FISA Court judges began to issue Supplemental Orders with most Section 215 orders. These Supplemental Orders required the Department to submit a written report to the FISA Court describing the FBI's minimization of U.S. person information no later than 90 days after the production of materials, with sufficient detail to allow the FISA Court to assess the adequacy of the FBI's implementation of the Interim Procedures. Between January 1, 2012, and June 30, 2013, the FISA Court issued Supplemental Orders for [REDACTED] total business records orders.²⁴

2. Final Minimization Procedures

On March 7, 2013, the Attorney General adopted and the Department filed with the FISA Court final minimization procedures for material received in response to Section 215 orders. These Final Procedures became effective on July 1, 2013.

The Final Procedures are designed to minimize the retention and prohibit the dissemination of "nonpublicly available information concerning unconsenting [U.S.] persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." The Final Procedures do not apply to publicly available U.S. person information, nor do they apply to acquiring, retaining, or disseminating U.S. person information with the person's consent. With the exception of provisions requiring an initial review of business records returns, and dictating the handling and retention of overproduced material and attorney-client communications, the Final Procedures do not apply to non-U.S. person information.

The Final Procedures set forth [REDACTED]

[REDACTED]:

- [REDACTED].
- [REDACTED].
- [REDACTED].

²⁴ Of the [REDACTED] orders for which the FISA Court did not issue Supplemental Orders, [REDACTED] were in counterintelligence investigations, [REDACTED] were in counterterrorism investigations, and [REDACTED] were in cyber investigations. These numbers exclude [REDACTED] business records orders issued under the Interim Procedures [REDACTED] or to restricted counterespionage investigations.

overproduction, he must return it to the producing party or destroy it as soon as practicable, ensure that the information has not been uploaded into any widely-accessible FBI system, and inform NSD of the overproduction to facilitate proper notification of the FISA Court. [REDACTED]

[REDACTED] 27

The Final Procedures allow the FBI to disseminate information obtained using business records orders to [REDACTED]. In general, the FBI must determine that nonpublic U.S. person information meets the FISA Standard before disseminating it [REDACTED]. Key dissemination provisions are summarized below:

- The FBI may disseminate foreign intelligence information [REDACTED], to federal, state, local, or tribal officials and agencies [REDACTED].
- Where the foreign intelligence information relates to a foreign power or foreign territory and reasonably appears to be necessary to the national defense, security, or foreign affairs of the United States, [REDACTED].

[REDACTED] 28

[REDACTED] 27

[REDACTED] 28

(Cont'd.)

• [REDACTED]

[REDACTED] 29 [REDACTED]

[REDACTED] 30 [REDACTED]

The Final Procedures include oversight provisions requiring NSD to review the FBI's compliance with them, stating that NSD [REDACTED]

[REDACTED] In accordance with this provision, NSD includes business records orders in the Minimization and Accuracy reviews it conducts in FBI field offices. During these reviews, NSD attorneys examine information produced in response to business records orders to identify overproductions, confirm that the information has been properly

[REDACTED]

²⁹ As described in more detail below, metadata refers to dialing, routing, addressing, or signaling information associated with communications, such as e-mail addresses, telephone numbers, or IP addresses.

³⁰ [REDACTED]

classified and marked in FBI systems as FISA-derived, evaluate compliance with minimization procedures, and assess retention and dissemination decisions. NSD attorneys also audit the searches conducted by FBI personnel in multiple FBI databases, including two databases that contain business records material, DWS and Data Integrated Visual System (DIVS), which operates as a search engine for a collection of other databases to which the FBI has access, to ensure that the queries comply with the minimization procedures. Between 2012 and 2014, NSD conducted 90 Minimization and Accuracy Reviews, including business records minimization reviews in every FBI field office.

After the Final Procedures became effective, NSD began requiring its attorneys to conduct post-order briefings within 5 days of an order being signed. These briefings are designed to ensure that FBI personnel understand and comply with the requirements of the Final Procedures. NSD attorneys contact FBI personnel to review the Final Procedures, including the definitions of "U.S. person" and "foreign intelligence information," [REDACTED], the requirement that agents conduct an initial review of returns before placing information in widely-accessible FBI systems, the proper handling of overproduced materials, and the standards for retaining and disseminating information. NSD attorneys told us that they typically conduct the briefings with case agents and cover the major requirements of the Final Procedures, the information requested by the order, and any special minimization or reporting requirements imposed by the FISA Court in a Supplemental Order.

The first business records application referencing the Final Procedures was filed with the FISA Court on August 6, 2013. Once the Final Procedures were in place, the FISA Court ceased issuing Supplemental Orders requiring the Department to report on its handling of U.S. person information as a matter of standard practice. However, between August 9, 2013, and January 3, 2014, the FISA Court issued Supplemental Orders for [REDACTED] applications that requested e-mail transactional records from various service providers, requiring the Department to submit written reports stating whether the returns included the contents of any communications. An NSD Deputy Unit Chief told us that the FISA Court began requiring content reporting for business records orders directed at [REDACTED] and other communications providers following a series of overproductions of e-mail subject lines. He characterized Supplemental Orders as "relatively unusual" since resolution of the systemic overproductions, stating that they are only issued if the FISA Court has particular concern about the breadth or potential volume of the material requested. We describe these systemic errors in more detail in Section V.

3. Retroactive Application of the Final Procedures

When the government submitted the Final Procedures to the FISA Court in March 2013, the then-Assistant Attorney General of NSD stated in a letter to the Court that the FBI [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The FBI also is required to report activities that may be unlawful or contrary to executive orders or directives to the IOB and Director of National Intelligence (DNI).³¹ The subjects of these reports to the IOB are commonly referred to as "IOB violations." FBI policy requires employees to report potential IOB violations to NSLB within 30 days of discovery. Once an agent reports a potential IOB matter, NSLB reviews the facts to determine whether Executive Order 13462 and the Intelligence Oversight Reporting Criteria require the violation to be reported to the IOB and the DNI.

For business records, there are two types of potential IOB violations. [REDACTED]

[REDACTED]. On August 1, 2011, the IOB mandated that the FBI begin providing information [REDACTED].

Agents are required to report third-party overproductions to NSLB within 90 days of the date of discovery.³² The FBI must then submit this information to the IOB in quarterly reports containing the following information:

1. [REDACTED];
2. [REDACTED]; and
3. [REDACTED].

Between 2012 and 2014, the FBI reported [REDACTED] violations related to business records orders to the IOB. Of these, [REDACTED] involved overcollections, including systemic overproductions of e-mail subject lines by [REDACTED]; [REDACTED] involved other issues, such as the production of materials outside the date range specified in a business records order; and [REDACTED] was the result of a typographical error in a business records order. NSLB also deemed [REDACTED] overcollections and [REDACTED] typographical error to be non-reportable.

³¹ See Exec. Order 12333 § 1.6(c), *as amended*; Exec. Order 13462 § 6(b), *as amended*; Criteria on Thresholds for Reporting Intelligence Oversight Matters (Sept. 8, 2010) ("Intelligence Oversight Reporting Criteria").

³² [REDACTED].

III. STATUS OF RECOMMENDATIONS

Previous OIG reports recommended changes to the minimization procedures used by the FBI. Our second report, issued in March 2008, recognized that the FBI had adopted Interim Minimization Procedures but made the following three recommendations:

- The FBI should develop procedures for reviewing materials received from Section 215 orders to ensure that it has not received information that is not authorized by the FISA Court orders;
- The FBI should develop procedures for handling material that is produced in response to, but outside the scope of, a Section 215 order; and
- The FBI should develop final standard minimization procedures for business records that provide specific guidance for the retention and dissemination of U.S. person information.

Our third report, issued in May 2015, analyzed the FBI's compliance with these recommendations. We concluded that the FBI had resolved the first recommendation in adopting the Final Procedures, but that it nonetheless should clarify in policy guidance or training materials that the initial review requirements in the Final Procedures apply to metadata. We determined that the second recommendation was closed, as the Final Procedures include a provision for handling "overproduced" material. Finally, we concluded that the third recommendation was resolved by the Final Procedures, but that the FBI should consider using training materials or policy guidance to clarify several provisions regarding the retention and dissemination of U.S. person information.

Below we describe the FBI's progress in implementing these recommendations.

A. Handling of Metadata Under the Final Procedures

As noted above, metadata refers to dialing, routing, addressing, or signaling information associated with a communication. In the context of wire or electronic communication transaction records, metadata may include e-mail addresses, telephone numbers, IP addresses, and similar information. Metadata *does not* include information concerning the substance, purport, or meaning of the communications.

1. Initial Review of Metadata

In our second report, we recommended that the FBI develop procedures for reviewing materials received from Section 215 orders to ensure that it had not received information outside the scope of the FISA Court orders. In our third report, we observed that the FBI had adopted Final Procedures requiring that agents conduct an initial review of materials produced pursuant to a Section 215 order. We concluded that this provision requires case agents to review materials for overproduced material, but that it does not expressly subject metadata to the initial review requirement. We recommended that the FBI clarify that the initial review requirement applies to metadata.

In the course of our current review, the FBI and NSD produced copies of internal policies and training materials that make clear that the initial review provision applies to all FISA business records materials, including metadata. The FBI Policy Implementation Guide for Business Records Standard Minimization Procedures (SMP PG) states, [REDACTED] and emphasizes that agents must complete the initial review before uploading the information to any widely accessible FBI system. Training materials provided by the FBI also state [REDACTED]

[REDACTED]. Agents we interviewed told us that they had received multiple trainings on the Final Procedures and understood that the requirement to conduct initial reviews applies to all business records returns, including those involving e-mail transactional data or other metadata.

In addition, as described above, NSD attorneys are required to conduct post-order briefings with the case agent within 5 days of a business records order being signed. NSD's Post-Order Briefing Policy provides that the NSD attorneys must remind agents that they are required to conduct an initial review of FISA-acquired business records information to ensure that the production is generally responsive to the order, and that this initial review must take place before placing the information in any widely accessible FBI system. NSD attorneys told us that they make clear in these briefings that the initial review requirement applies to every business records production, including metadata.

Accordingly, we consider this recommendation closed.

2. Other Provisions Relating to Metadata

[REDACTED]

[REDACTED]

In our third report, we identified two potential issues regarding application of these provisions that we believed required attention and oversight.

- We stated that NSD and the FBI should periodically review the application of [REDACTED]

[REDACTED]

- We encouraged the FBI to pay attention [REDACTED]

[REDACTED]

In our current review, we assessed whether NSD and the FBI have addressed these issues. Training materials released in early 2016 state that [REDACTED]

[REDACTED]

The training materials also provide guidance on applying [REDACTED]

[REDACTED]

33

In 2012 and 2013, the FBI used business records orders to request by a subject on two occasions.³⁴ The first order requested

. The business records order specifically requested . In that case, the produced included .

Since issuance of the OIG's third report in May 2015, NSD has revised its policy

35

33

³⁴ Two other business records orders requested different types of

35

Given these steps, we believe that the FBI and NSD have sufficiently addressed the concerns we raised regarding other provisions related to metadata in our third report.

B. Retention and Dissemination of U.S. Person Information

In our second report, we recommended that the FBI develop final minimization procedures providing specific guidance on the retention and dissemination of U.S. person information. In our third report, we recognized that the FBI had resolved this recommendation by adopting Final Procedures providing such guidance, but stated that the FBI should consider clarifying two provisions in policy guidance or training materials: the definition of "necessary to understand foreign intelligence information," and the provision allowing

[REDACTED]. We briefly discuss each in turn below.

1. "Necessary to Understand Foreign Intelligence Information"

We recommended that the FBI define the term "necessary to understand foreign intelligence information" and provide actual examples of its application in training materials or policy guidance. Training materials produced by the FBI and NSD address this issue. One presentation states that when [REDACTED]

[REDACTED] The training provided the following example of this analysis:

[REDACTED]

According to the training slides, [REDACTED], and thus it meets the FISA Standard. Standing alone, however, it may be difficult to articulate why [REDACTED] would be appropriate.

Based on this guidance, we believe the FBI has addressed our concerns.

2. Dissemination of Information Relating to Computer Intrusions or Attacks

We also recommended that the FBI provide further guidance regarding the provision in the Final Procedures that allows the FBI to [REDACTED]

We stated the FBI should consider clarifying that the material must meet the FISA Standard, as well as define the term "U.S. person identifying information" and provide actual examples of its application.

The FBI has made these clarifications. The SMP PG makes clear that agents must first analyze whether the information meets the FISA Standard, stating, [REDACTED]

While the current version of the SMP PG does not further define or illustrate "U.S. person identifying information," an NSLB attorney told the OIG that the FBI is in the process of revising and consolidating its FISA policy guidance, and that the revised guidance will include a definition. In addition, materials used in trainings beginning in March 2016 define "U.S. person identifying information" and provide guidance on its application. Training slides and speaker's notes state that [REDACTED]

[REDACTED]. The training materials list examples that include [REDACTED]

[REDACTED]. The materials emphasize that determining whether information constitutes "U.S. person identifying information" requires a case-by-case assessment, and that agents should consult with NSLB if questions arise.

As a result, we consider this recommendation closed.

IV. OVERVIEW OF BUSINESS RECORDS ORDERS ISSUED FROM 2012 THROUGH 2014

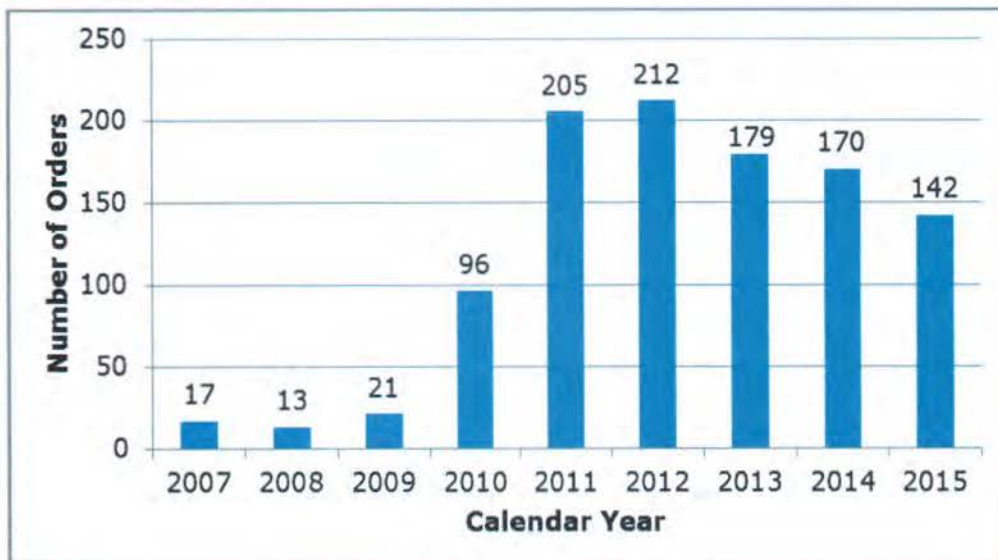
In this section, we provide an overview of the characteristics of business records orders approved in calendar years 2012 through 2014. We describe the number of business records orders approved, the type of information requested, the number of FBI offices that used the authority, and the types of investigations in which business records orders were sought. We provide information about the number of business records orders in which U.S. persons were the subject of the underlying investigations.

Additionally, we examine the timeliness of the business records process. We analyze the length of time that elapsed between the initiation of a business records request and the signing of the business records order by the FISA Court.

A. The Overall Number of Business Records Orders

From 2012 to 2014, the FISA Court approved 561 business records orders.³⁶ This continued a dramatic increase in the use of business records authority compared to the number of orders that we have observed during our prior reviews. For example, the FISA Court approved 51 orders from 2007 through 2009, the 3 year time period that we reviewed in our 2015 report. Figure 1 illustrates the increase in number of approved business records orders by calendar year.

FIGURE 1
Total Number of Approved Business Records Orders,
by Calendar Year, 2007-2015³⁷



Source: FBI.

³⁶ After reviewing a draft of this report, NSD commented that references to the number of business records orders should be changed to the number of approved applications for business records orders. The OIG understands that some business records applications result in more than one order. For example, the FISA Court may issue orders to four separate providers when approving a single application requesting ECTRs for four e-mail addresses. We also recognize that NSD reports the number of applications submitted to the FISA Court in its annual reports to Congress. Nonetheless, we decided to retain the references to the number of business records orders throughout this report as a matter of convenience.

³⁷ This table includes the total number of dockets for 2013 (179). This number differs slightly from the number of approved applications for business records the Department reported to Congress for 2013 (178). The OIG recognizes that one submission in 2013 was a copy of the Final Procedures, which did not result in a FISA Court order. As described below, we excluded this docket from our numbers for purposes of statistical analysis.

As we describe in more detail in Section IV.C.I., a primary factor in the increase between 2010 and 2012 was the refusal of certain communications providers to produce transactional records for e-mail [REDACTED] accounts (Electronic Communication Transaction Records, or ECTRs) in response to National Security Letters (NSL) beginning in late 2009. NSD and FBI personnel attributed the subsequent decline between 2013 and 2015 to several factors, including the stigma attached to the use of Section 215 authority following the Snowden revelations, increased use of Section 702 of the FISA Amendments Act, providers' resistance to business records orders, agents' frustrations with the lack of timeliness and level of oversight in the business records process, and agents' increasing use of criminal legal process instead of FISA authority in counterterrorism and cyber investigations.

In addition, between 2012 and 2014 there were [REDACTED] pending and [REDACTED] withdrawn applications for business records orders.³⁸ While we did not seek to ascertain the basis for each withdrawn request or application, we did review [REDACTED] that originated from the [REDACTED] and questioned agents about [REDACTED] of these. The reasons for the withdrawals varied, but many were withdrawn for administrative reasons, such as inadvertent initiation in FISAMS or a duplicate request, while others were withdrawn because the agents determined that the information was no longer necessary [REDACTED]. As a result, the number of applications withdrawn for substantive reasons is likely significantly lower.

We also reviewed [REDACTED] requests submitted to NSD but not filed with the FISA Court, and [REDACTED] draft applications submitted to the FISA Court as read copies but subsequently withdrawn. The requested information and targets in these applications varied substantially, and witnesses were unable to identify a common factor leading to their withdrawal. The withdrawn applications included several requests that were based on [REDACTED] or statements advocating jihad that raised potential First Amendment concerns.³⁹ [REDACTED] withdrawn application requested toll records [REDACTED].

³⁸ Pending applications include applications generated between 2012 and 2014 but not provided to NSD for further processing or submitted to the FISA Court for further approval.

³⁹ In February 2013, the FISA Court issued a legal opinion that addressed the line between First Amendment-protected activity and information establishing predication for an international terrorism investigation. The opinion was issued in response to the Department's application [REDACTED].

[REDACTED]. The FISA Court considered whether the application established reasonable grounds to believe that the investigation of the target was not being conducted solely upon the basis of activities protected by the First Amendment. The FISA Court concluded [REDACTED].

[REDACTED]. The Department reported and provided copies of this opinion to Congress in April 2013.

[REDACTED]. The agent ultimately re-submitted the business records request, and it was approved in 2015.⁴⁰ [REDACTED]

[REDACTED], which we discuss in more detail in Section V.

The FISA Court did not deny any business records applications between 2012 and 2014. When asked why applications withdrawn after submission of a read copy to the FISA Court were not reported to Congress, potentially creating the inadvertent impression that the FISA Court is a “rubber stamp,” NSD supervisors told us that the Department includes only business records applications formally submitted to the FISA Court and denied or withdrawn, not those filed in “read copy” and subsequently withdrawn.⁴¹ The NSD supervisors acknowledged that excluding applications withdrawn after the FISA Court indicates that it will not sign an order might lead to misunderstandings about the FISA Court’s willingness to question applications, but the supervisors noted that NSD and the FISA Court have talked about the “read” process publicly to address concerns about this.⁴² In comments provided to the OIG after

⁴⁰ The request for toll records originally was submitted as an NSL [REDACTED]. According to information produced by the FBI, the NSL required FBI Headquarters approval [REDACTED]. The case agent told the OIG that [REDACTED]

[REDACTED]. In September 2013, the agent submitted a business records request for the information, but NSLB asked him to withdraw the request since the information that could be obtained with an NSL. The agent added a request for e-mail transactional data, and the request ultimately went forward as a business records application in early 2015. It received approval from the Deputy Attorney General (DAG) in May 2015. An NSD Section Chief explained that [REDACTED]

⁴¹ As described above, the FISA Court Rules of Procedure require the government to file a propose application, or “read copy,” with the FISA Court no later than 7 days before it seeks to have the application considered.

⁴² See, e.g., Letter from the Honorable Reggie B. Walton, Presiding Judge of the FISA Court, to Sen. Charles E. Grassley, Ranking Member of the Sen. Comm. on the Judiciary (Jul. 29, 2013) (“The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b)—frequently cited to in press reports as a suggestion that the Court’s approval rate of applications is over 99%—reflect only the number of *final* applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.”); Remarks of John Carlin, Acting Assistant

(Cont’d.)

reviewing a draft of this report, NSD stated that it is currently considering whether to revise the methodology for counting withdrawn applications.

B. Business Records Orders by FBI Field Office

The OIG analyzed the number of FBI field offices with approved business records orders in 2012 through 2014. We determined that [REDACTED] of the FBI's 56 field offices obtained business records orders during this period.⁴³ The following 3 field offices had the most approved business records orders during our review period: [REDACTED]. Sixteen field offices each had between [REDACTED] and [REDACTED] business records orders approved between 2012 and 2014. The remaining 37 field offices each had fewer than [REDACTED] business records orders approved during our review period.

C. Analysis of Business Records Orders

We also analyzed various characteristics of the business records orders during our review period. Factors we considered included the type of information requested, the type of underlying investigation (*e.g.*, counterterrorism, counterintelligence, or cyber), the status of the subject of the investigation (either a U.S. person or non-U.S. person), and the timeliness of the business records process.

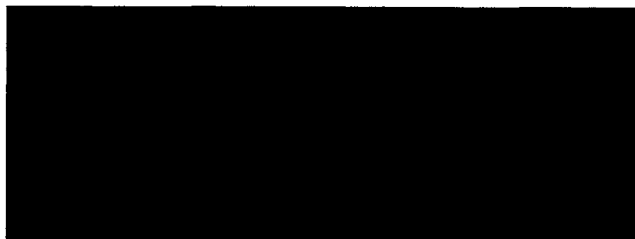
To conduct this analysis, we excluded [REDACTED] of the 561 total business records orders in our dataset based upon the unique characteristics of those orders. [REDACTED] of the excluded business records orders involved the bulk collection of information [REDACTED], which we briefly address in Section V of this report. [REDACTED] business records orders involved restricted counterespionage investigations and were handled outside of FISAMS. Finally, one order was an administrative document memorializing the Final Procedures. Therefore, the dataset in our analysis includes a total of [REDACTED] approved business records from 2012 through 2014.

Figure 2 shows the number of business records orders included in our analysis, by calendar year.

Attorney General for National Security, at the American Bar Assoc. Homeland Security Law Institute (Jun. 20, 2013) ("That the [Foreign Intelligence Surveillance Court (FISC)] ultimately denies very few applications is simply a reflection of the unique nature of *ex parte* FISC proceedings [T]he Department of Justice has 'an independent obligation to determine that every FISA application meets the statutory standard before we submit it' and treats that obligation with the utmost seriousness and care.").

⁴³ The [REDACTED] field offices submitted business records requests during our review period, but those requests were later withdrawn.

FIGURE 2
Total Number of Business Records Orders Included in Analysis,
2012-2014



Source: FBI.

1. Types of Investigations from which Business Records Orders Originated

First, we examined the types of investigations from which business records orders originated. The [REDACTED] business records orders we reviewed originated from counterintelligence (CI), counterterrorism (CT), and cyber investigations. Figure 3 shows the numbers of business records orders approved in each type of investigation.

FIGURE 3
Types of Investigations from which Business Records Orders Originated,
2012-2014

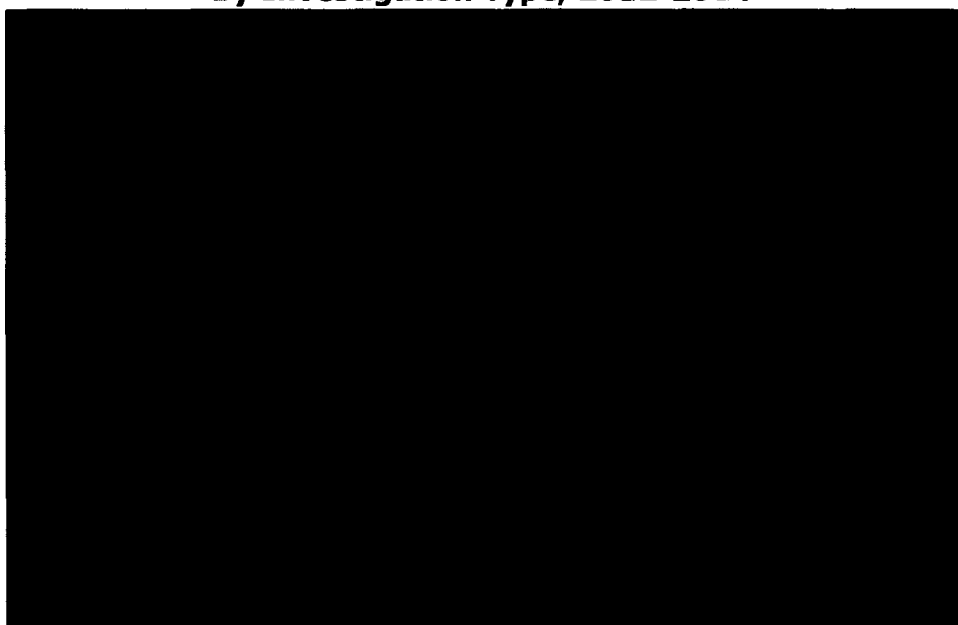


Source: NSD and FBI.

We found that business records orders were used far more frequently in counterintelligence investigations than in counterterrorism or cyber investigations. Of the [REDACTED] total orders we analyzed, [REDACTED] were obtained in counterintelligence investigations ([REDACTED]), [REDACTED] in counterterrorism investigations ([REDACTED]), and [REDACTED] in cyber investigations ([REDACTED]). Figure

4 shows that this gap increased during our review period, during which the usage of business records orders in counterintelligence investigations increased slightly, while the orders' usage decreased more substantially in both counterterrorism and cyber investigations.

FIGURE 4
Usage of Business Records Orders
By Investigation Type, 2012-2014



Source: FBI.

When asked about this disparity, agents told us that business records orders frequently are the only option available in counterintelligence investigations given the nature and classification of the information involved. By contrast, agents handling counterterrorism and cyber investigations can in some instances open a parallel criminal investigation and use the grand jury process to obtain the same information more quickly and with less oversight than a business records order. As described in more detail below, agents told the OIG that the business records process frequently takes several months, versus several weeks to obtain a grand jury subpoena. This was particularly true in cyber cases, [REDACTED] ([REDACTED]), during the reporting period, as discussed below.

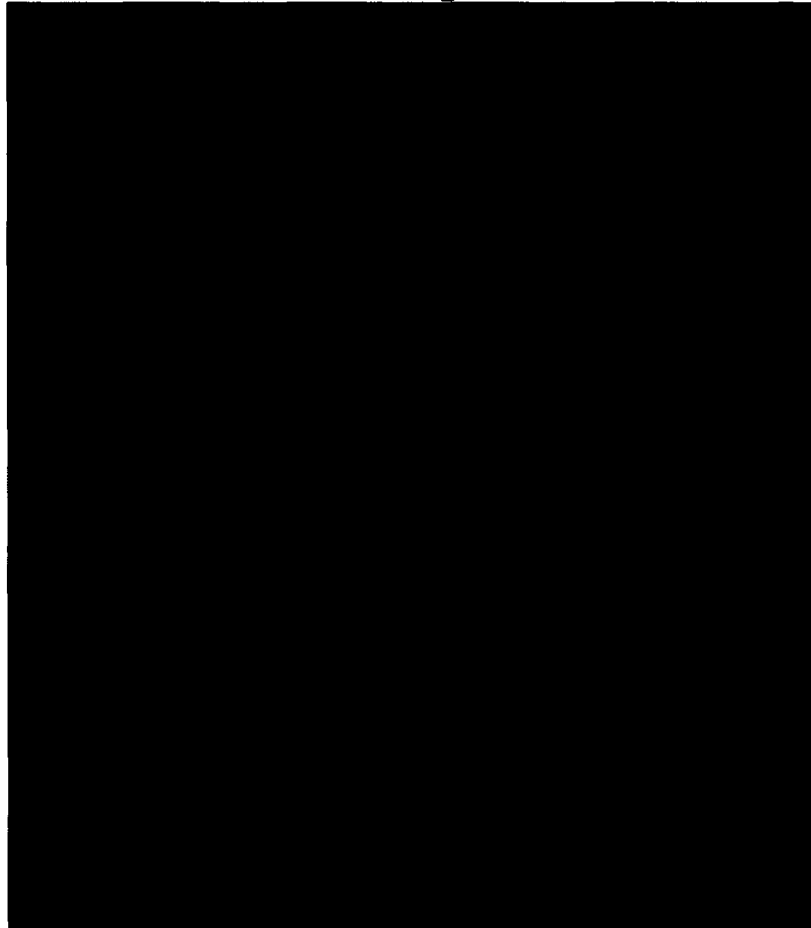
2. Subjects of Business Records Orders

We also analyzed approved business records orders to determine the number of orders that had U.S. persons and non-U.S. persons as subjects of the underlying investigations. We found that U.S. persons were listed as subjects in [REDACTED] orders, while non-U.S. persons were listed as subjects in [REDACTED] orders. [REDACTED] orders identified both a U.S. person and a non-U.S. person as subjects of the underlying investigations.

3. Types of Records Requested in Approved Business Records Orders Filed on Behalf of the FBI

Next, we examined our dataset for the types of business records requested during our review period. Figure 5 shows the types of records requested, as well as the number of orders requesting each type of record.

FIGURE 5
Types of Records Requested in Business Records Orders, 2012 through 2014



⁴⁴ [REDACTED]

⁴⁵ Records detailing [REDACTED]

⁴⁶ Records detailing customer [REDACTED]

⁴⁷ For our review period, these included records from [REDACTED]

We found that [REDACTED] different types of records were requested during our review period. Transactional records for e-mail [REDACTED] accounts (ECTRs) were the most common type of records requested, accounting for [REDACTED] of the non-bulk business records orders we reviewed ([REDACTED] records).⁴⁸ The [REDACTED] business records orders requesting ECTRs between 2012 and 2014 are a dramatic increase from [REDACTED] approved orders requesting ECTRs in the OIG's previous review period, which constituted only [REDACTED] of the approved non-bulk orders between 2007 and 2009.

We found that the increase in business records orders for ECTRs was primarily due to a significant change in the use of NSLs. In late 2009, Internet providers began refusing to provide transactional information for e-mail [REDACTED] [REDACTED] accounts in response to an NSL, requiring the FBI to use business records orders to obtain the same information.⁴⁹ Consequently, the number of business records orders went up "exponentially."

Interviews with FBI and Department personnel supported this conclusion. One NSLB attorney described business records orders as a [REDACTED] used to obtain transactional records that were previously obtained through NSLs. Several agents told us that a business records order was their only option once providers refused to accept NSLs for transactional information. Many agents expressed frustration at having to utilize the business records process instead of NSLs, because an NSL requires only field office approval and takes a few weeks to obtain rather than the several months that can be required for a business records order.

However, the number of non-ECTR business records orders also increased significantly compared to the previous review period. There were [REDACTED] business records orders for non-ECTR information during our current review period, as opposed to [REDACTED] between 2007 and 2009. We asked FBI and NSD personnel about the reasons for the increase in non-ECTR business records orders. Some witnesses attributed the increase to agents' growing awareness of and comfort

⁴⁸ Business records orders requesting ECTRs included requests for [REDACTED] [REDACTED] business records orders ([REDACTED]) requested e-mail account information and [REDACTED].

⁴⁹ As described in the OIG's August 2014 report on the FBI's Use of National Security Letters, Internet providers began refusing to produce ECTRs in response to NSLs around November 2009. The FBI historically had relied on Section 2709(b) of the Electronic Communications Privacy Act (ECPA) for authority to obtain ECTRs using NSLs. In November 2008, however, the Department's Office of Legal Counsel (OLC) issued an opinion interpreting Section 2709(b) as authorizing communications providers to produce four exclusive categories of information in response to an NSL: subscriber name, address, length of service, and local and long distance toll billing records. Although the OLC opinion did not specifically focus on ECTRs, one Internet provider argued that Section 2709(b) did not give the FBI authority to compel e-mail transactional records using an NSL, and several other providers followed suit. [REDACTED]

with the business records process, while others were unable to provide an explanation for it.

An NSD Deputy Unit Chief noted that the number of business records orders reached its peak in 2012 and has declined annually since then, and that the number of ECTR requests has declined more than other types of requests. The Deputy Unit Chief said that the Snowden revelations have played a role in this decline, both in terms of the stigma attached to use of Section 215 and increased resistance from providers. The Deputy Unit Chief stated, "I think that it's possible that folks . . . have decided it's not worth pursuing [business records orders], you know, obviously things haven't been great with providers since Snowden either."

In comments provided to the OIG after reviewing a draft of this report, NSD stated that the degree to which the Snowden disclosures affected the number of business records applications was speculative, and attributed the FBI's increasing use of taskings under Section 702 as likely a "notable cause" in the decrease in business records requests. NSD stated that during the relevant period (and continuing today) it suggested that FBI withdraw business records requests for accounts used by non-U.S. persons located overseas that can instead be tasked under Section 702.⁵⁰

4. Timeliness of the Business Records Process

Lastly, we examined the median length of time it took for business records orders to move through the approval process, including the overall length of time from initiation of a FISAMS request to FISA Court approval and the amount of time spent in each phase of the business records process. As we describe in more detail below, we did not identify a particular phase of the business records approval process that was responsible for delays.⁵¹

Our review also evaluated whether particular characteristics of business records orders affected the time it took for a business records order to move

⁵⁰ Section 702 of the FISA Amendments Act allows the government to acquire foreign intelligence by targeting non-U.S. persons reasonably believed to be outside the United States. Under Section 702, the government is not required to obtain individual surveillance orders from the FISA Court. Instead, the FISA Court approves targeting procedures to ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States, and minimization procedures to guard against the inadvertent collection, retention, and dissemination of U.S. person information.

⁵¹ In comments provided to the OIG after reviewing a draft of this report, NSD highlighted the importance of the expedite process for business records applications. NSD stated that it had worked closely with FBI over the years to establish an expedite process through which FBI management can request that a FISA request, including a business records request, be processed immediately. According to NSD, this has resulted in some applications being processed in a single day. We agree that the expedite process is an important procedure that allows NSD and FBI to move applications quickly when operationally necessary. However, given the infrequency with which the expedite process is used for business records requests, we do not believe it impacts our overall analysis of the timeliness of the business records process. As noted below in footnote 54, only [REDACTED] business records requests we examined followed an expedited or amended approval process.

through the approval process. To do this, we first examined the median amount of time it took for a business records order to be approved from the time the request was initiated in FISAMS, to the time the order was sent to the FISA Court for approval. We then aggregated the business records orders by the following characteristics: type of records requested, type of underlying investigation, whether the subject of the investigation was a U.S. person, and by originating field office. We compared the aggregated median number of days for each of these characteristics to determine whether any orders sharing a similar characteristic took longer to be approved. Based on this analysis, we concluded that these factors had no appreciable effect on timeliness.

a. Overall Length of Time for Business Records Orders Approval, 2012-2014

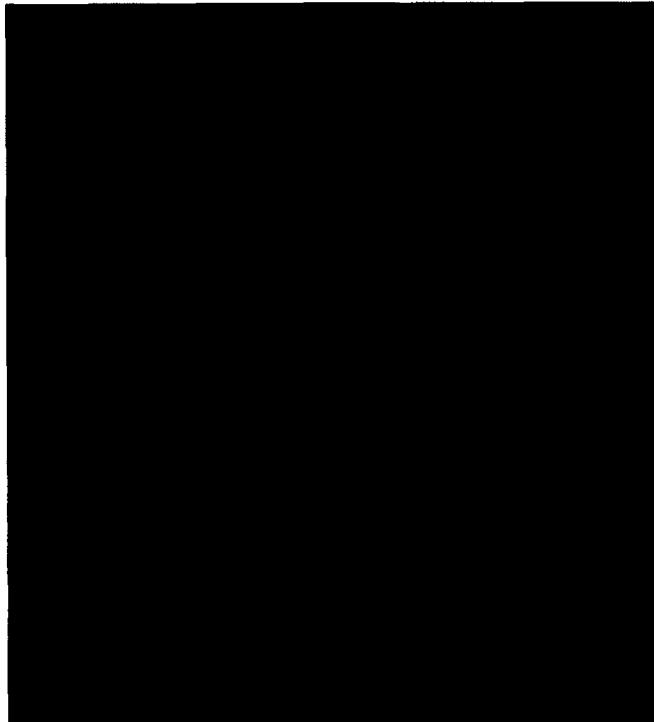
First, we examined the overall length of time it took for business records orders to go from initiation in the Foreign Intelligence Surveillance Act Management System (FISAMS) to approval by the FISA Court.⁵² We found that it took a median of 115 days (almost 4 months) for a business records order to move through the approval process during our review period.⁵³ [REDACTED] of the business records orders ([REDACTED] orders) were processed in 4 months or less during our review period.⁵⁴ Figure 6 illustrates the amount of time business records took to move through the business records orders approval process.

⁵² As discussed in Section II.B, the process to obtain a Section 215 order generally involves FBI field office initiation and review, FBI Headquarters review by NSLB and the Counterterrorism or Counterintelligence substantive desk, NSD review, and review and approval by the FISC.

⁵³ A median was used instead of an average in this case because the datasets had several number outliers artificially inflating the average.

⁵⁴ For purposes of our timeliness analysis, we excluded [REDACTED] records in our dataset because those records followed expedited or amended approval processes. Because these investigations were not entered into FISAMS, we do not have information as to how long they took to process.

FIGURE 6
Business Records Orders Approval Time, 2012-2014



Source: FBI.

b. Length of Time in Each Phase of the Approval Process, 2012-2014

We also examined the length of time business records orders spent in each phase of the approval process (field office, NSLB, NSD, and final approval) during our review period. We found that business records orders spent the least amount of time in the field office phase of the approval process – a median of 16 days.⁵⁵ Despite testimony from witnesses attributing delays in the process to various bottlenecks at FBI Headquarters, in NSD, or in obtaining final signatures, we were unable to identify a particular phase of the process that was responsible for delays. Orders spent a median of 40 days with NSLB and a median of 33 days in the NSD phase of the approval process.⁵⁶ We found that the FBI took a median of 2 weeks to obtain final approval signatures from NSLB and the FBI Deputy General Counsel.

⁵⁵ As described above, the field office phase of the approval process usually includes the initiation of a business records request by case agent in FISAMS, and approval from the following supervisors: Supervisory Special Agent, Chief Division Counsel, and the Assistant Special Agent in Charge.

⁵⁶ In comments provided to the OIG after reviewing a draft of this report, NSD noted that a substantial amount of the time between NSD's receipt of a business records request and the finalization of the application involves a back and forth with FBI personnel who review the draft and provide answers to questions from NSD.

As described above, FISA Court rules provide for submission of a "read" copy no later than 7 days before the government seeks to have the matter entertained by the Court. Our analysis included the time that applications and proposed orders were with the FISA Court to provide the most accurate measurement of the time needed for the FBI to obtain business records orders. While we do not have complete data regarding the FISA Court's processing of business records applications, we were informed that "read" copies generally are provided the week before, and the orders signed within a day or two of submission of the final application. No witnesses cited delays with the FISA Court as an issue.

c. Overall Timeliness

In interviews with the OIG, agents expressed concern with the timeliness of the business records orders approval process. Many agents we interviewed told us that the process for obtaining a business records order was lengthy, citing the amount of detail required, the multiple layers of approval, and the need to work with attorneys to draft the application.

Various agents told the OIG that the process was a deterrent to seeking another business records order. One counterterrorism agent stated, "To be candid with you, I don't think I ever will [seek another business records order]." He explained that he could be "waiting for months" before the order is approved and served, and that "once a case is over, it's not really over," because he has to go through internal FBI inspections, as well as possible inspections from other entities, including the OIG. By contrast, where there is a parallel criminal case, he can consult with the Assistant United States Attorney (AUSA) to confirm that there is enough information to obtain a grand jury subpoena, and receive the records much more quickly.

Agents expressed particular concerns about the impact of these delays in cyber cases. One agent said that the 2 to 3 months it took to obtain his business records order was "ridiculous." He explained that information moves quickly in the cyber realm, stating:

[REDACTED]

Another cyber agent agreed, stating, [REDACTED]

He said [REDACTED]

[REDACTED]. He told the OIG that it has been common practice to use the FISA process and NSLs in cyber cases, but that given providers' resistance to NSLs and delays in obtaining FISA orders,

some cyber squads have begun opening parallel criminal cases on foreign actors and finding ways to develop probable cause to obtain criminal legal process, allowing them to get data more quickly and with less oversight. These views are consistent with the [REDACTED], as discussed above.

NSD and NSLB personnel we interviewed were aware of agents' frustrations and said that their divisions have taken steps to improve the business records process. While several NSD witnesses said that the volume of requests did not significantly impact their processing of business records orders, one NSD attorney acknowledged to us that there had been delays in the process "because things get backed up." An NSD Deputy Unit Chief told the OIG that NSD has implemented "TurboFISA" to provide standardized language and streamline the drafting process for business records requests. NSD also places business records applications on a 14-day schedule, requiring attorneys to attend a meeting with supervisors to explain the reasons for any delays. An NSLB attorney told the OIG that he was "embarrassed" at how long the business records process takes, stating, "We are asking for less [than a full FISA], and it's taking twice as long." He told the OIG that, although NSLB does not measure the timeliness of the business records process, he thought that NSLB has streamlined the way it handles ECTR requests. Another NSLB attorney told the OIG that he thought ECTRs were being drafted and received by the FISA Court in a much more expeditious manner than other types of requests because they were so common.

As described above, we examined whether the type of records requested affected the timeliness of the process and identified no difference between ECTR and non-ECTR applications. We also did not see improvements in the timeliness of ECTR requests over the 3-year period: [REDACTED]. We did not obtain or analyze 2015 data.

Based on agents' concerns about timeliness, we recommend in Section VI that the FBI and the Department continue to pursue ways to make the business records process more efficient, particularly for applications related to cyber cases.

V. SELECTED SECTION 215 ORDERS OBTAINED BETWEEN 2012 AND 2014

In this section we describe selected Section 215 applications and orders obtained by the FBI between 2012 and 2014. We chose these matters to illustrate various uses of Section 215 authority. For each selected use, we summarize the underlying investigation and describe the material requested and any notable issues regarding the application and order. We then describe, where applicable, the material produced in response to the order, how it was used, and any compliance incidents.

In addition, in this section we discuss three compliance incidents that affected numerous business records orders during our review period. These

consisted of overproductions of full and partial subject lines (*i.e.*, content) by [REDACTED], the production of e-mail [REDACTED] by [REDACTED], and the FBI's release of un-minimized data from quarantined areas of DWS before agents conducted their initial review.

Finally, we provide a brief overview [REDACTED] following passage of the USA Freedom Act.

A. Selected Uses of Section 215 Authority

1. Business Records Orders in [REDACTED] Related FBI Counterterrorism Investigations

In 2012 and 2013, an FBI agent obtained [REDACTED] business records orders and submitted one application that was withdrawn after submission to NSLB. These were obtained in [REDACTED] related counterterrorism investigations [REDACTED]

[REDACTED]. As a result of this information, the FBI opened a full investigation [REDACTED].

[REDACTED]. The agent stated that the FBI was concerned that these [REDACTED] individuals wittingly or unwittingly may have been tied to a foreign power, so they initiated preliminary investigations on each of them.⁵⁷

[REDACTED] of the business records orders obtained in these cases were for electronic communication transactional records, while the other [REDACTED] business records orders and the withdrawn application were for [REDACTED]. Below we describe these orders and the withdrawn application, the handling of the information received in response to the approved orders, how the information was used to further the investigation, and any compliance incidents.

⁵⁷ Under the FBI's Domestic Investigation and Operations Guide (DIOG), there are two levels of predicated national security investigations: a preliminary investigation, which requires information or an allegation of a possible threat to national security, and a full investigation, which requires an articulable factual basis of a possible threat to national security.

a. **█████ Requests for Electronic Communications Transactional Records from █████ (Section 215 Orders Issued December 2012)**

Between April and August 2012, the agent initiated █████ business records requests for electronic communications transactional records from █████. The requests sought transactional data for █████ in an effort to gather information about these individuals and determine whether they had been in contact with a foreign power. NSLB approved the requests in October 2012, and the FISA Court issued █████ separate orders in December 2012.

Each of these orders requested “[a]ll tangible things, but not the ‘contents’ of any communications as defined by 18 U.S.C. § 2510(8), *e.g.*, electronic mail or subject line, associated with the [targeted account] . . . from the inception of the targeted account to the date of production.” In standardized language used in every request for e-mail transactional records, the orders listed the following items as examples of “tangible things” being sought for the identified e-mail addresses:

- █████;
- █████;
- █████;
- █████;
- █████;
- █████;
- █████;
- █████;
- █████;
- █████; and
- █████.

For [REDACTED] of the orders, the FISA Court issued standard Supplemental Orders requiring submission of written reports describing the FBI's implementation of the Interim Procedures to U.S. person information received from the providers. For the [REDACTED] order, which included a request for transactional data from [REDACTED], the FISA Court issued a Supplemental Order requiring the Department to report on its minimization of U.S. person information, and on whether the records received from the providers included the "content" of any communications. NSD and the FBI filed the required Supplemental Reports.

For each of these orders, the providers delivered the records in electronic format. The records included [REDACTED]

[REDACTED]. DITU received the records from the providers and uploaded them into DWS, where they were stored as unpublished products. The records were viewable only to relevant FBI personnel until the agent or co-case agent completed his initial review, minimized nonpublic U.S. person information, and "published" the information. Except as described below, the agent or his co-case agent reviewed the records and determined that they were within the scope of the orders.

After receiving these returns, the agent requested analysis of the information by a Staff Operations Specialist (SOS) in the field office. The SOS used the [REDACTED] to search three FBI databases – Clearwater, Sentinel/ACS, and DIVS.⁵⁸ [REDACTED]

[REDACTED], in general they returned no information indicating connections to or support for a foreign terrorist organization. The SOS documented these analyses in ECs widely available to FBI personnel through Sentinel.

The agent told the OIG that he pursued the business records orders only after taking other investigative steps, [REDACTED], coordinating with local law enforcement, obtaining NSLs for financial and e-mail subscriber data, and conducting searches of FBI and other government databases. The agent explained that a number of providers recently had stopped providing e-mail transactional records in response to NSLs, and that a business records order was the only available tool given the classification of the derogatory information in his cases. The agent stated that the business records process took considerably longer than an NSL. Nonetheless, he said that the information he obtained was

58 [REDACTED]

Automated Case System (ACS) and its successor, Sentinel, are the FBI's case management systems. As described above, DIVS operates as a search engine for a collection of FBI and non-FBI databases to which the FBI has access.

critical in allowing him to conclude [REDACTED].

There were compliance incidents related to two of these business records orders. The first order sought transactional records from [REDACTED] for an e-mail address used [REDACTED].

[REDACTED]. In response to the order, [REDACTED] produced [REDACTED], virtually all of which [REDACTED].

Although the co-case agent reviewed the records in DWS and identified no overproduction, DITU later determined that some of [REDACTED] and were part of a systemic overproduction of content by [REDACTED]. As described in more detail below, DITU purged overproduced records from DWS, and the overproductions were reported to the FISA Court and to the IOB in 2013 and 2014 as part of a larger report about [REDACTED] systemic overproductions.

The [REDACTED] order requested transactional records from [REDACTED] for [REDACTED] e-mail addresses used by another associate, [REDACTED]. In response to this order, [REDACTED] produced responsive records in electronic format, which the FBI uploaded into DWS on two separate dates. On [REDACTED], the FBI uploaded [REDACTED] consisting of transactional information for [REDACTED] and [REDACTED], as well as [REDACTED]. Three days later, on [REDACTED], the FBI uploaded an additional [REDACTED] records, which primarily were e-mail header information. The agent and co-case agent reviewed the returns and determined that the records were within the scope of the FISA Court order and did not include content. However, the agent and co-case agent mistakenly attributed the second batch of [REDACTED] records to [REDACTED]. The co-case agent documented these as separate returns from [REDACTED] in the case file, and the FBI subsequently closed the preliminary investigation for this individual on [REDACTED]. The FBI also disclosed these as [REDACTED] returns to the FISA Court in a Supplemental Report filed on [REDACTED].

[REDACTED] did not complete its production of responsive records until [REDACTED], almost 6 months after the investigation was closed. [REDACTED] produced approximately [REDACTED] records consisting of [REDACTED], which were uploaded electronically into DWS. Upon initial receipt of the records from [REDACTED], DITU identified full or partial e-mail subject lines in the production, sent the entire production back to [REDACTED], deleted the materials from its systems, and asked for the information to be produced without the subject lines. [REDACTED] subsequently re-produced the records, which were then uploaded into DWS.

The agent told the OIG that he did not learn about the [REDACTED] production until several months later, when he logged on to DWS and noticed that he had returns for review. According to e-mails dated [REDACTED], the agent subsequently contacted attorneys in NSLB and NSD, who helped him determine that the [REDACTED] records were within the date range in the order and thus were not an overproduction, even though the investigation had been closed

Two weeks later, on [REDACTED], [REDACTED] responsive documents directly to the agent in hard copy. The records contained telephone numbers and e-mail addresses [REDACTED]. According to the Supplemental Reports filed with the FISA Court, the agent reviewed the hard copy documents and determined that the information related exclusively to the targeted individuals. The agent then had an SOS analyze the information by using the identifiers to conduct database checks and create a telephone link chart, which were documented in ECs and uploaded into Sentinel. The agent also uploaded scanned documents of the original returns into the case file in Sentinel. NSD reviewed the returns for these business records orders in its 2014 Minimization and Accuracy Review and identified no errors.

[REDACTED]. Based on this and other information, the FBI found no nexus to terrorism and closed the preliminary investigations in [REDACTED].

The FBI closed the full investigation [REDACTED] in [REDACTED]. According to the closing EC, [REDACTED]. Although he had had contact with a person who was associated with the foreign terrorist organization, there was no evidence that he supported or was a member of the organization himself. The FBI also determined [REDACTED]. As a result, the FBI concluded [REDACTED] posed no threat to national security warranting further investigation.

The FBI disseminated information about these [REDACTED] investigations to members of the [REDACTED] in a briefing at a conference in June 2015.⁶¹ In a joint presentation, the FBI and Defense Intelligence Agency briefed conference attendees on efforts by [REDACTED].

2. Multiple Business Records Orders in an FBI Counterintelligence Investigation

Between 2012 and 2014, an FBI agent obtained [REDACTED] business records orders and submitted [REDACTED] business records application that was withdrawn after submission of a "read copy" to the FISA Court. The business records [REDACTED].

⁶¹ [REDACTED]

[REDACTED]. In a related case, another FBI agent obtained a business records order for information about [REDACTED]. Below we describe the business records orders and the withdrawn application, the FBI's handling of the information received in response to the approved orders, how the information was used to further the investigation, and any compliance incidents that occurred in connection with these matters.

a. Request for [REDACTED] (Section 215 Order Issued February 2012)

In [REDACTED], the FBI agent initiated a business records request for [REDACTED]

⁶² According to the agent, several of the subject's [REDACTED], which revealed [REDACTED]

[REDACTED] to determine whether it had been used to access [REDACTED]. She said that there was no other authority available to obtain this data given the classification and sensitivity of the case.

The business records request was submitted to NSD in early [REDACTED], and subsequently was approved by the FISA Court on [REDACTED]. Because the order pre-dated the Final Procedures, the FISA Court issued a Supplemental Order requiring submission of a written report describing the FBI's minimization of U.S. person information received in response to the order.

According to the Supplemental Report filed with the FISA Court, the [REDACTED] on [REDACTED], and received responsive materials between [REDACTED]. The providers produced [REDACTED]. The agent told us that the records were important because they gave the FBI a window into the subject's communications habits, [REDACTED].

⁶² [REDACTED]

The agent placed the information in the FBI's official case file, which is maintained in a secure area of the FBI field office and restricted to personnel involved in the case, and did not upload it into the FBI's electronic case management database. The OIG reviewed the records and confirmed that they did not include any identifying or account information.

b. Request for [REDACTED] (Section 215 Order Issued February 2012)

In [REDACTED], the agent initiated a business records request for the subject's [REDACTED], including account records for his [REDACTED]. According to the application, [REDACTED]. The application stated that the FBI wanted to obtain this information [REDACTED].

The business records request was sent to NSD in [REDACTED], and the FISA Court signed the order on [REDACTED]. The FISA Court again issued a Supplemental Order requiring submission of a written report describing the FBI's minimization of U.S. person information received in response to the order. The FBI served the FISA Court order on [REDACTED].

According to the Supplemental Report filed with the FISA Court, the FBI [REDACTED]. The case agent reviewed the materials and determined that they were within the scope of the order and contained only information relating to the subject. We reviewed the documents received in response to this business records order and confirmed that they contained only the subject's information. The information remained in hard copy, and was not uploaded into the FBI's electronic case management database or disseminated.

c. Request for [REDACTED] (Section 215 Order Issued March 2012)

In [REDACTED], the agent initiated a business records request for the subject's [REDACTED] information. The draft request sought various information related to the subject, his e-mail addresses, [REDACTED].

⁶³ The request was submitted to NSD on [REDACTED], and subsequently was revised several times. One draft requested "all tangible things" relating to the subject including [REDACTED] for the subject, [REDACTED]. The final application revised this request to "all tangible things including . . . records" for the subject, [REDACTED], but noted for reasons discussed below in a footnote, [REDACTED]

The order was approved by the FISA Court on [REDACTED]. The FISA Court issued its standard Supplemental Order requiring submission of a written report describing the FBI's minimization of U.S. person information received in response to the order. According to the Supplemental Report submitted to the FISA Court, the FBI served the order [REDACTED].⁶⁴ In response, [REDACTED]

[REDACTED]. Although not explicitly addressed in the Supplemental report, [REDACTED], for reasons discussed below.

The agent told the OIG that she reviewed the information and [REDACTED]. According to the agent, the records established [REDACTED], and were not uploaded to the FBI's electronic case management database or otherwise disseminated.

Although the FBI ultimately obtained [REDACTED], the OIG asked why the request included [REDACTED]. Under current FBI policy, [REDACTED]

⁶³ [REDACTED]

⁶⁴ The Supplemental Report for this order and the 2012 orders [REDACTED] were not filed until early 2015. According to contemporaneous e-mails, these Supplemental Reports "got lost in [NSD's] administrative shuffle when the matters were handed off between attorneys," and the delay was not the agent's fault. The NSD attorney who filed the Supplemental Reports in 2015 explained the reason for the delay in his cover letters to the FISA Court.

metadata obtained with a business records order can include [REDACTED]

[REDACTED]. The NSD attorney who drafted the application said [REDACTED]. The agent told the OIG that [REDACTED]

[REDACTED]. A Deputy Unit Chief in NSD said that they subsequently began limiting business records requests to [REDACTED]

In addition, our review of [REDACTED] revealed that [REDACTED] information included [REDACTED]. This information was within the scope of the order, which authorized the production of all records associated with [REDACTED]. As described in more detail below in connection with the discussion of the FBI's dispute [REDACTED], the FBI and NSD believe that Section 215 authorizes the government to [REDACTED] using business records orders, but nonetheless began excluding [REDACTED].

d. Request for [REDACTED] (Section 215 Order Issued November 2012)

The agent submitted a business records request for [REDACTED] in [REDACTED], seeking "all tangible things" related to the subject, including [REDACTED]. The agent told us that she requested these [REDACTED].

The FISA Court approved the Section 215 order on [REDACTED], and issued a standard Supplemental Order requiring reporting on the minimization of responsive U.S. person information. The FBI served the FISA Court order on [REDACTED], and the recipient company produced responsive records on [REDACTED]. The agent then reviewed the records and determined that they were within the scope of the order. The agent told us [REDACTED]. The agent retained the records in hard copy in the FBI's restricted case file.

The FBI shared the [REDACTED]. The agent told us [REDACTED] went through minimization training

and received only a hard copy of the [REDACTED]. She explained that the process of disseminating records to [REDACTED] to directly view the minimized data.⁶⁵ The FBI disclosed this dissemination to the FISA Court in a Supplemental Report filed on [REDACTED].

As this investigation is ongoing, [REDACTED]. However, the case agent told the OIG [REDACTED].⁶⁶

e. [REDACTED] (Section 215 Order Issued January 2013)

In [REDACTED], the FBI opened a spin-off investigation [REDACTED]. Based on information [REDACTED], the agent leading the spin-off case initiated a business records request for [REDACTED]. The application sought "all tangible things" related to the [REDACTED] including [REDACTED].

The FISA Court approved the application on [REDACTED], and issued its standard Supplemental Order requiring reporting on the amount of U.S. person information received and how it was retained and disseminated. The FBI served the business records orders [REDACTED] on [REDACTED].

According to the Supplemental Report filed with the FISA Court, [REDACTED]. The FBI determined that the printed summary fell within the scope of the order, but that [REDACTED] did not because they either preceded the start date of the order or related to different names than the [REDACTED].

⁶⁵ This business records order was governed by the Interim Procedures, which allowed the FBI to [REDACTED]

[REDACTED]. The Final Procedures allow the FBI to [REDACTED]

⁶⁶ As noted above, the FBI told us that [REDACTED].

[REDACTED]. The FBI purged the [REDACTED] overproduced records and retained the remaining [REDACTED] records in its physical investigative file. The [REDACTED] produced [REDACTED], all of which fell within the scope of the order and were retained in the FBI's physical investigative file. The FBI did not disseminate or upload the records into its databases.

The case agent told us [REDACTED]

[REDACTED]. The investigation of the [REDACTED] was ultimately closed in late [REDACTED].

**f. Request for E-mail Transactional Records
(Section 215 Order Issued December 2013)**

In [REDACTED], the agent initiated a business records request for transactional records from [REDACTED] for [REDACTED]. The application stated [REDACTED]

[REDACTED]. According to the agent, [REDACTED]

The FISA Court approved the application on [REDACTED], and issued a Supplemental Order requiring the government to file a report stating whether the items received include the contents of any communication. The FBI served the order on [REDACTED] on [REDACTED]. [REDACTED] produced responsive records the following day. According to the Supplemental Report filed with the FISA Court, [REDACTED] produced [REDACTED], which were uploaded and stored in a restricted area of the FBI's DWS. The Supplemental Report stated [REDACTED]

The agent told the OIG that she marked the records in DWS by whether they met the FISA Standard, and did not release them to the FBI's case management database. The OIG reviewed the records and confirmed that they were visible only to the agent.

The agent told the OIG that the [REDACTED], and there was no other way to obtain this information in a counterintelligence investigation. However, she indicated [REDACTED]

[REDACTED]. According to the agent, the latter information would have been helpful because [REDACTED]

g. Request for Additional [REDACTED] Records (Section 215 Order Issued June 2014)

In [REDACTED], the agent initiated another business records request for transactional records from [REDACTED]. Rather than identifying specific [REDACTED]

[REDACTED] According to the agent, during interviews with the U.S. government, [REDACTED]

[REDACTED]. The agent obtained emergency authorization for electronic surveillance and physical search [REDACTED]

. The agent said that she sought information from [REDACTED] about [REDACTED]

The agent told us that the

██████████. She said that although the information was helpful, she was unable ██████████. She said that there were no overproductions in the returns. The OIG reviewed the ██████████ production and confirmed that it was stored in the restricted case file.

h. Withdrawn Request for

In [REDACTED], NSD and the FBI began discussing using a business records order [REDACTED]. The agent told the OIG [REDACTED]

The initial draft request sought “all tangible things related to [the subject]

In early [REDACTED], [REDACTED]

NSD subsequently finalized the business records application. The final draft request sought "all tangible things related to [the subject] [REDACTED]

[REDACTED] " In the final application, NSD argued [REDACTED]

[REDACTED]. According to the application, Congress had ratified this interpretation of the business records provision in its 2011 reauthorization.

[REDACTED]

The final application also included the same supplemental minimization procedures as the initial draft, noting that these were used in the [REDACTED].

The EAD signed the final application, and NSD filed a "read copy" with the FISA Court in [REDACTED].

[REDACTED], the FISA court judge informed NSD that he was [REDACTED].

[REDACTED]. In discussions with NSD in [REDACTED], a legal advisor on the FISA Court staff stated that he thought [REDACTED].

NSD and NSLB then proposed [REDACTED]. In an e-mail dated [REDACTED], an NSLB attorney informed the agent [REDACTED].

[REDACTED]. The agent said that she became extremely frustrated with the process and [REDACTED].

[REDACTED] in [REDACTED] - 3 years after she initiated the business records request. The agent told the OIG [REDACTED].

[REDACTED]

The FISA Court approved the order on [REDACTED], and issued its standard Supplemental Order under the Interim Procedures. According to the Supplemental Report filed with the FISA Court, [REDACTED]

[REDACTED]. The field office stored the raw data on a computer system accessible only to cyber squad members. The agent reviewed the records, [REDACTED], minimized the U.S. person information, summarized his analysis in an EC, and uploaded the EC into the FBI's case management system.

Based on the information produced [REDACTED]
[REDACTED]. After receiving the information [REDACTED]
[REDACTED].⁷⁰ While some of these searches resolved [REDACTED], requiring the agent to use an NSL [REDACTED].⁷¹ After [REDACTED].

The agent told the OIG [REDACTED] was very important to his investigation and [REDACTED]. However, he expressed concern about how long the business records process took (approximately 106 days from initiation to order in this instance). [REDACTED]

69 [REDACTED]

70 [REDACTED]

71 [REDACTED]

and contained only information relating to the subject, requested that the records be uploaded into DWS.⁷² We reviewed the records received in response to the business records order and confirmed that they contained only the subject's information. Additionally, we found that [REDACTED] in response to the order. The case agent told the OIG that the records [REDACTED] and were not of investigative value. No analytical products were created using the records obtained. The investigation was closed in [REDACTED] after the subject departed the United States.

5. Request for [REDACTED] (Section 215 Orders Issued October 2013)

On [REDACTED], an FBI agent initiated a business records request for records [REDACTED]. According to the primary case agent, the underlying counterintelligence investigation was initiated in [REDACTED] to [REDACTED].

The business records request was submitted to NSD on [REDACTED], and was subsequently approved by the FISA Court on [REDACTED]. The Court ordered [REDACTED].

The case agent described the business records process to be uneventful in this case. He stated that he answered a few factual questions for the NSD attorney assigned to the business records application, but that no concerns or problems were identified with the application. The case agent described the overall business records process positively, but noted that the amount of time it takes to obtain a business records order was "frustrating" and can slow down an investigation.

The FBI served the FISA Court orders [REDACTED] on [REDACTED]. [REDACTED] the FBI with records responsive to the business records order on [REDACTED], and [REDACTED] responsive records on [REDACTED].

⁷² In [REDACTED], the FBI identified an error in DWS that resulted in the [REDACTED]. We describe this compliance issue in more detail below.

[REDACTED]. The case agent conducted an initial review of the records and determined that the records were responsive and contained no overproduced information.

Around this time, in [REDACTED], the FBI decided to transfer management of this case from the [REDACTED]. The case agent told the OIG that this decision was based on resource considerations. Due to this, the case agent forwarded the business records to the new case agent in FBI's [REDACTED]. The new case agent told the OIG that the FBI reached out to an individual identified in the business records and [REDACTED]. According to the new case agent, [REDACTED]

[REDACTED]. The new case agent stated that the FBI would not have identified [REDACTED] if not for these business records. Because of that, the agent described the business records request as "one of the key steps" in the ongoing investigation.

6. Multiple Business Records Orders in an FBI Counterintelligence Investigation

In 2013 and 2014, FBI agents obtained [REDACTED] business records orders in a counterintelligence investigation involving [REDACTED]. The subjects of the investigation [REDACTED]

[REDACTED]. The FBI believed that the subjects, [REDACTED]

[REDACTED]. Below we describe the [REDACTED] business records orders obtained in this investigation.

a. Request for [REDACTED] (Section 215 Order Issued August 2013)

On [REDACTED], an FBI co-case agent initiated a business records request [REDACTED]. First, the agent requested [REDACTED].

Second, the agent requested [REDACTED].

[REDACTED]. The FBI agent told the OIG [REDACTED]

[REDACTED]. The FBI hoped that the results of this business records request would allow the FBI [REDACTED].

The business records request was submitted to NSD on [REDACTED], and was subsequently approved by the FISA Court on [REDACTED]. The Court

ordered [REDACTED] the requested records for the period from inception of service to the date of production of the records.

The FBI served the FISA Court order [REDACTED] on [REDACTED]. The FBI received [REDACTED] on [REDACTED]. The [REDACTED] FBI agents assigned to the investigation conducted an initial review of the records and determined that they were responsive to the request. The FBI agent who requested the records told the OIG that the records confirmed [REDACTED].

**b. Requests for [REDACTED]
(Section 215 Orders Issued August 2013 and
March 2014)**

On [REDACTED], the FBI co-case agent also initiated a business records request [REDACTED] for [REDACTED] relating to the subjects. FBI investigation had determined that [REDACTED].

The business records request was submitted to NSD on [REDACTED], and was subsequently approved by the FISA Court on [REDACTED]. The Court ordered [REDACTED]. At the government's request, the FISA Court's order explicitly stated should not produce [REDACTED].

The FBI attempted to serve the order [REDACTED] informed the FBI [REDACTED] was misidentified in the order and refused to accept service of the order. As a result, no records were obtained in response to this order and, as we discuss below, the FBI obtained a new order for these records.⁷³

On [REDACTED], the FBI case agent initiated a second business records request for these records. In addition to the records previously requested, the second request [REDACTED]

⁷³ NSD told us that [REDACTED].

[REDACTED]

The business records request was submitted to NSD on [REDACTED], and was subsequently approved by the FISA Court on [REDACTED]. The Court's order again contained language [REDACTED] should not produce [REDACTED].

The FBI served the order [REDACTED]. The FBI received [REDACTED] with the responsive records on [REDACTED]. The case agent told us that she conducted an initial review of the materials upon receipt and found the records responsive to the request. The case agent also told us the records were useful to the investigation and that some of the records were disseminated [REDACTED]. The case file indicated [REDACTED]. The investigation into the subjects is ongoing, and the case agent told the OIG [REDACTED].

B. Compliance Incidents

The OIG reviewed three compliance incidents that affected numerous business records orders between 2012 and 2014. The first involved the overproduction of full and partial e-mail subject lines by two providers, [REDACTED], which the OIG determined affected [REDACTED] business records orders. [REDACTED] similarly overproduced [REDACTED]. NSD and FBI witnesses told the OIG that the vast majority of compliance incidents relating to business records orders between 2012 and 2014 were the result of overproductions by providers.

A third compliance incident was the result of a technical problem in an FBI database, rather than provider error. In March 2015, the FBI [REDACTED].

We describe each of these compliance incidents below.

1. Full and Partial Subject Lines from [REDACTED]

On November 16, 2012, DITU notified NSD that it had discovered that [REDACTED] had overproduced full or partial subject lines in response to [REDACTED] business records orders requesting e-mail transactional records. Upon discovery of the overproduction, the FBI contacted [REDACTED] and stopped serving business records orders on it. NSD filed a preliminary notice with the FISA Court on November 21, 2012, disclosing the [REDACTED] overproduction and stating that the FBI was investigating the issue further. On December 19, 2012, [REDACTED] advised the FBI that it had identified the cause of the overproduction and rectified the error, and the FBI then resumed serving business records orders on [REDACTED].

However, DITU's review of subsequent productions revealed that [REDACTED] continued to produce full and partial subject line information in response to business records orders after December 2012. DITU determined that the overproduction was caused by a mistake in [REDACTED] production logic, and that [REDACTED] earlier fix was flawed. DITU then sequestered all business records productions from [REDACTED] so that they were available only to limited technical personnel. When DITU discovered overproduced information, it purged the entire production prior to uploading and requested that the provider reproduce it without the subject line information.

By April 6, 2013, [REDACTED] represented that it had corrected its production methodology to include only authorized e-mail fields. Nonetheless, DITU continued to manually review [REDACTED] business records productions and discovered additional full or partial subject lines in July, August, and October 2013. According to a Rule 13(b) notice filed with the FISA Court on December 26, 2013, DITU did not identify additional overproductions by [REDACTED] after November 8, 2013, and stopped manually reviewing business records productions from [REDACTED] on November 18, 2013.

While investigating [REDACTED] systemic overproduction of subject lines, DITU identified similar overproductions by [REDACTED]. DITU followed the same procedures as it had with [REDACTED], sequestering and purging the [REDACTED] productions to ensure that no information had been transferred to other FBI systems. DITU continued to review all [REDACTED] returns until November 12, 2013, when it determined that [REDACTED] had corrected the problem. In July 2015, however, NSD reported that [REDACTED] had overproduced subject line information in response to two business records orders issued in 2014. A subsequent FBI investigation concluded that these overproductions were an isolated issue and not a systemic problem. The OIG did not identify additional overproductions by [REDACTED] in 2014.

Although NSLB concluded that DITU followed proper procedures by sequestering the overproductions and did not compound the errors by uploading the materials into FBI databases, the FBI reported these as IOB violations based on the systemic nature of the technical problems by the providers and the large number of FISA Court dockets affected. The Department also reported the systemic overproductions to Congress in the Attorney General's 2013 Annual Report on the use of the business records provision and in the Semi-Annual Report for January 1 to June 30, 2013.

2. [REDACTED]

On June 27, 2013, the FISA Court approved an application for transactional records from [REDACTED]

[REDACTED]. The Deputy Section Chief explained that this distinction was not always readily discernible and required case-by-case analysis. She stated that when the error in this instance was initially discovered, the FBI determined that DITU could not automatically screen [REDACTED] productions to identify [REDACTED] data that constituted content. She said that the FISA Court was aware that NSLB issued guidance instructing agents to be on the lookout for [REDACTED] data in future [REDACTED] productions.

The Department also reported the production of [REDACTED] data to Congress in the Attorney General's Semi-Annual Report for January 1 to June 30, 2014.

3. DWS Release of Quarantined Records

As described above, the FBI's typical practice is to store business records returns produced in electronic format in an access-restricted area of DWS. The agent is required to conduct an initial review of the records to identify overproductions and minimize nonpublic U.S. person information before "releasing" the records in DWS.

In March 2015, the FBI identified an error that caused DWS to release some business records returns prior to initial review, making the un-minimized raw data available FBI-wide. The FBI determined that the error potentially affected [REDACTED] business records orders between January 2014 and March 2015.⁷⁶ The FBI informed the FISA Court of the error on June 30, 2015. According to the Rule 13(b) notice filed with the FISA Court, the FBI corrected the error in DWS and restricted access to the materials produced in response to the affected business records orders. The FBI then notified the agents responsible for those orders to allow them to conduct initial reviews of their returns. An NSD Deputy Section Chief told us that NSD and FBI are still investigating the incident, specifically they are confirming that all initial reviews have been completed and attempting to determine whether any of the un-minimized raw data was exported from DWS prior to the initial review being conducted.

C. Current Status of Bulk Collection under Section 215

Our May 2015 report described in detail the Section 215 applications submitted by the FBI [REDACTED]

⁷⁶ This error affected [REDACTED] business records orders in 2014, including [REDACTED] orders selected for review by the OIG.

As noted previously, the USA Freedom Act effectively ended bulk collection by the government under Section 215 by requiring the government to limit the scope of its requests "to the greatest extent reasonably practicable," and by requiring that applications for business records include a "specific selection term," such as a specific individual, telephone number, or e-mail address. This addition to the business records statute was significant because the FISA Court [REDACTED]

[REDACTED] on the theory that all of the data was relevant because it was necessary to create a data archive from which to identify known and unknown terrorists that may be in the United States or in contact with U.S. persons. The new provision of the USA Freedom Act became effective on November 29, 2015, 180 days after the date of the statute's enactment; [REDACTED]

[REDACTED] bulk collection [REDACTED] expired on November 28, 2015. After that date, [REDACTED]

A Deputy Section Chief from NSD told us that the government no longer collects information in bulk under Section 215.⁷⁷

[REDACTED] authorization from the FISA Court to retain and use data previously produced under the FISA Court orders that authorized the [REDACTED]. According to filings with the FISA Court, the NSA requested authority to retain previously produced data for two reasons. First, the NSA requested 90 days of technical access to previously produced data so that authorized technical personnel could use that data to verify the completeness and accuracy of call detail records produced under the new targeted production orders authorized by the USA Freedom Act. Second, the NSA requested authority to retain previously produced data in order to remain in compliance with civil litigation preservation obligations imposed by federal district courts until the NSA was relieved of those obligations. [REDACTED]

[REDACTED]

The FISA Court appointed amicus curiae under the new provisions of the USA Freedom Act and ordered the amicus and the government to brief the issue [REDACTED]. In memoranda to the FISA Court, the amicus concluded that the USA Freedom Act did not prohibit the government's retention and requested use of the bulk data, and that it was within the discretion of the FISA Court to determine [REDACTED]

⁷⁷ As noted in Section II of this report, the USA Freedom Act created a new mechanism that allows the government to obtain call detail records from providers within two "hops" of the specific selection term on an ongoing basis for 180 days from the date of the FISA Court order. See 50 U.S.C. § 1861(b)(2)(C).

[REDACTED]. The amicus stated that given the significant privacy interests of U.S. persons that were at issue, the FISA Court should exercise its oversight authority to ensure that the government was retaining and using the previously collected information in a manner consistent with applicable minimization procedures. Following a hearing on the matter, the FISA Court granted the [REDACTED]. According to the [REDACTED], the FISA Court found [REDACTED],

[REDACTED] comported with the statutory definition of minimization procedures set forth in the FISA statute. See 50 U.S.C. § 1861(g). [REDACTED]

[REDACTED] the FISA Court found that the government's access to and use of the bulk telephony metadata was appropriately tailored to ensure that the successor program established by the USA Freedom Act was functioning effectively and to ensure compliance with the government's litigation-related obligations.

VI. CONCLUSION

As required by the USA Freedom Act, we examined the FBI's use of Section 215 authority for calendar years 2012 through 2014 in this report. Our review determined that the FISA Court issued 561 business records orders during the review period, including 212 in 2012, 179 in 2013, and 170 in 2014. We found that the Section 215 applications during our review period sought a variety of "tangible things," including transactional records for e-mail [REDACTED]

We found that the number of business records orders obtained by the FBI increased significantly between 2007 and 2014, largely driven by the refusal of several communications providers to produce transactional records for e-mail [REDACTED] (ECTRs) in response to NSLs. Between 2007 and 2009, the FISA Court issued 51 total orders. Of these, [REDACTED] related to [REDACTED], and only [REDACTED] were requests for ECTRs, representing [REDACTED] of all non-bulk business records orders obtained during that period. By contrast, between 2012 and 2014, [REDACTED] of the orders related to [REDACTED], while [REDACTED] involved requests for ECTRs, constituting roughly [REDACTED] of the non-bulk orders obtained during our review period.

Even excepting requests for e-mail [REDACTED] transactional records, the number of business records orders obtained by the FBI between 2012 and 2014 was substantially higher than in the previous review period. There were [REDACTED] business records orders for non-ECTR, non-bulk information during our review period, as compared to [REDACTED] between 2007 and 2009. Some witnesses

attributed this increase to agents' growing awareness of and comfort with the business records process, while others were unable to provide an explanation for it.

We identified changes in the use of business records orders that took place within our review period. The number of business records orders reached its peak in 2012 with 212 orders and has declined annually since then. Witnesses told us that the number of ECTR requests has declined more than other types of requests. According to an NSD Deputy Unit Chief, revelations about the NSA's bulk telephony metadata program played a role in this decline, both in terms of the stigma attached to use of Section 215 and increased resistance from providers. In comments provided to the OIG after reviewing a draft of this report, NSD also attributed the FBI's increasing use of taskings under Section 702 of the FISA Amendments Act as likely a "notable cause" in the decrease in business records requests.

We found that business records orders were used most frequently in counterintelligence cases. Of the [REDACTED] total orders we analyzed, [REDACTED] were obtained in counterintelligence cases, [REDACTED] in counterterrorism cases, and [REDACTED] in cyber cases. Agents told us that business records orders frequently [REDACTED] [REDACTED] cyber cases in some instances can open a parallel criminal case and use the grand jury process to obtain the same information more quickly and with less oversight than a business records order. [REDACTED] [REDACTED], which is consistent with agents' explanations that those cases require particularly timely acquisition of information, as discussed below.

During our review, we analyzed the timeliness of the business records process, both generally and at each phase of the approval process. We determined that the median time needed to obtain business records orders during our review period was 115 days. Business records orders spent the least amount of time in the field office phase of the approval process, a median of 16 days. Orders spent a median of 40 days with NSLB and 33 days in the NSD phase of the approval process. We found that the FBI took a median of 2 weeks to obtain final approval signatures from NSLB and the FBI Deputy General Counsel.

Agents we interviewed described the entire process as lengthy and added that the delay in obtaining business records orders often had a negative impact on their investigations. Agents conducting cyber investigations particularly emphasized this point, [REDACTED] Agents told the OIG [REDACTED] [REDACTED]. As a result, timeliness is even more critical in cyber cases. While agents said that [REDACTED] [REDACTED] [REDACTED] NSD and NSLB attorneys

acknowledged the delays in the process and told the OIG that they have taken steps to improve it, including streamlining the drafting and review process for ECTRs.

We also selected [REDACTED] applications to illustrate the various uses of Section 215 authority and to conduct a more detailed review of the types of materials requested, the purposes of the requests, the materials produced, and the manner in which the materials were used. Although agents expressed concern about the length of the process to obtain a business records order, they told us consistently that these orders continued to be a valuable investigative tool. As with our previous reviews, the majority of agents we interviewed did not identify any major case developments that resulted from use of the records obtained in response to business records orders, but told us that the material produced was valuable as a building block of the investigation. However, in at least two cases, agents we interviewed told us that the business records obtained in their investigation provided valuable information that they would not otherwise have been able to obtain. In other instances, case agents told us that they used the information obtained under Section 215 to exculpate a subject and close the investigation.

We also reviewed the [REDACTED] FISA Court orders authorizing the bulk collection of certain data as part of counterterrorism [REDACTED]. Our third report on Section 215 authority described [REDACTED] at length, including the specialized minimization procedures that applied to [REDACTED], reported compliance incidents, and the status of [REDACTED] through May 2015. As described in this report, the USA Freedom Act effectively ended the government's collection of data in bulk under Section 215 by requiring the government to limit the scope of its requests "to the greatest extent reasonably practicable," and by requiring that applications seek records related to a "specific identifier," such as an individual, account, address, or personal device. On November 24, 2015, the FISA Court granted [REDACTED] the bulk data previously collected under prior FISA Court orders.

Finally, in addition to reviewing the FBI's use of Section 215 authority in calendar years 2012 through 2014, we examined the progress the Department and the FBI made in addressing three recommendations in the OIG's March 2008 and May 2015 reports. In the 2008 report, we recommended that the Department implement final minimization procedures, develop procedures for reviewing materials received in response to business records orders to identify overproduced information, and develop procedures for handling overproductions. In our May 2015 report, we recognized that the Department had adopted Final Procedures implementing the OIG's recommendations, but identified several terms used in the Final Procedures that we believed required clarification. Based on the information obtained in our current review, we concluded that the Department and the FBI have made these clarifications. We therefore have closed the recommendations.

Based on the information developed during our review, we concluded that the process used to obtain non-bulk business records orders between 2012 and

2014 contained safeguards that protected U.S. persons from the unauthorized collection, retention, and dissemination of nonpublic information about them. As described above, the business records process requires multiple layers of approval, including by attorneys in NSLB and NSD, and by the FBI EAD for certain sensitive records. Information we reviewed indicates that NSLB and NSD attorneys routinely question agents about business records applications. Rather than acting as a “rubber stamp,” documents that we reviewed reflect that the FISA Court engages in a dialogue with NSD and at times has informed NSD that it will not approve certain business records applications: we identified at least [REDACTED] applications that were withdrawn after submission of a “read copy” to the FISA Court during the period covered by this review.

In addition, since July 2013, the Final Procedures require agents to determine whether nonpublic U.S. person information meets the FISA Standard before retaining or disseminating it to other agencies. We found that the agents we interviewed had received training on the minimization procedures, were knowledgeable about them, and appeared to take them seriously. The steps that the FBI and NSD have taken to implement the OIG’s previous recommendations, combined with the level of oversight and reporting to monitor FBI compliance with the Final Procedures, reflect considerable progress in the FBI’s use of Section 215 authority.

However, based on the concerns expressed by agents about the time needed to obtain business records orders, we recommend that the FBI and the Department continue to pursue ways to make the business records process more efficient, particularly for applications related to cyber cases where agents

[REDACTED]. Potential measures include using FISAMS data to track the timeliness of Section 215 applications, using alerts within FISAMS to identify applications that have lingered past a certain period of time without review, and implementing a streamlined drafting and review process [REDACTED]

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.



Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig