from determining with complete accuracy the number of investigations of different U.S. persons and different non-U.S. persons during which the FBI issued NSLs for financial records and NSLs for toll billing/electronic communication transactional records. (U)

IV. National Security Letter Requests From 2003 Through 2005 (U)

In this section, we describe the FBI's use of NSLs from 2003 through 2005 as documented in the OGC database. As discussed above, the data in the OGC database is not fully accurate or complete and, overall, significantly understates the number of FBI NSL requests. However, it is the only database that compiles information on the FBI's use of NSLs. Moreover, the data indicates the general levels and trends in the FBI's use of this investigative tool. (U)

From 2003 through 2005, the FBI issued a total of 143,074 NSL requests (see Chart 4.1, next page).[74] Of that number, 141,367 requests (or 99 percent) were made pursuant to the three NSL statutes that are included in the Department's semiannual classified reports to Congress (RFPA, ECPA, and FCRAu). In addition, although the data was not required to be reported to Congress, the OGC database showed that the FBI issued [redacted] NSL requests for consumer full credit reports (FCRAv) during the same period. FBI records show that [redacted] (S)

b1
b3
Per FBI
(S)

As shown in Chart 4.1, the number of ECPA NSL requests increased in CY 2004, and then decreased in CY 2005. We determined that the spike in CY 2004 occurred because of the issuance of 9 NSLs in one investigation that contained requests for subscriber information on a total of 11,100 separate telephone numbers. If those nine NSLs are excluded from CY 2004, the number of NSL requests would show a moderate, but steady increase over the three years.[75] The overwhelming majority of the NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute. The [redacted] used NSL requests, accounting for approximately [redacted] percent of the total, sought

b1
b3
Per FBI
(S)

---

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

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

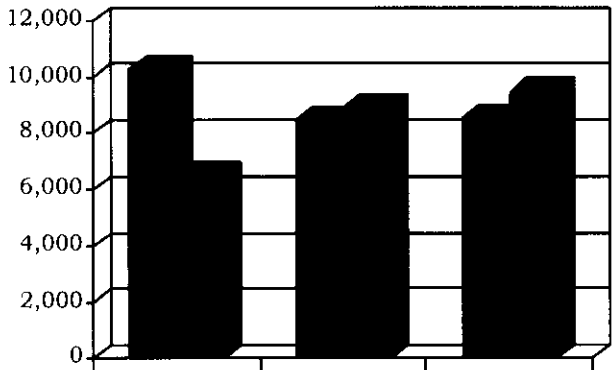
b1
b3
Per FBI
(S)

U.S. persons increased by almost 3,000 from 2003 to 2005, while the number of requests generated from investigations of non-U.S. persons decreased by about 1,700. As a result, the percentage of NSL requests generated from investigations of U.S. persons increased from about 39 percent of all NSL requests in CY 2003 to about 53 percent of all NSL requests in CY 2005.[77] (U)

CHART 4.2 (U)

NSL Requests Reported to Congress Relating to U.S. Persons and non-U.S. Persons (2003 through 2005) (U)

[The chart below is unclassified]



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

Source: DOJ semiannual classified NSL reports to Congress (U)

NSL Requests Issued During Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations: The following charts present the number of NSL requests issued from 2003 through 2005 for different types of investigations. (U)

---

[77] Chart 4.2 does not contain the same totals as Chart 4.1 because not all NSL requests reported to Congress identified whether they related to an investigation of a U.S. person or a non-U.S. person. Of the 141,367 NSL requests reported in the Department's semiannual classified reports to Congress for CY 2003 through CY 2005 (which included the ECPA, RFPA and FCRAu requests), 52,199 NSL requests identified whether the request for information related to a U.S. person or a non-U.S. person. The remaining 89,168 NSL requests were for the ECPA NSLs seeking subscriber information for telephone numbers and Internet e-mail accounts and did not identify the subject's status as a U.S. person or non-U.S. person. ~~(S)~~

49 briefings to members of Congress and their staff. Hayden told us that during the many PSP briefings to members of Congress, no one ever suggested that the NSA should stop the program. Hayden emphasized that he did more than just "flip through slides" during the briefings, which lasted as long as attendees had questions.

(U) Foreign Intelligence Surveillance Court Briefings on the Program

~~(TS//SI//OC/NF)~~ On 31 January 2002, the FISC Presiding Judge Royce Lamberth became the first member of the court to be read into the PSP. He was briefed on the program after James Baker, the head of DoJ's Office of Intelligence Policy and Review (OIPR) raised concerns with the White House over PSP-derived information being included in FISA applications. White House officials initially rejected the idea of reading in members of the FISC. Lamberth's briefing was conducted at the DoJ and was attended by Ashcroft, Hayden, Mueller, Yoo, and Baker.

~~(TS//SI//OC/NF)~~ Ashcroft provided Lamberth a brief summary of the President's decision to create the PSP, and Ashcroft stated that he had determined, based upon the advice of John Yoo, an attorney in DoJ's Office of Legal Counsel (OLC), that the President's actions were lawful under the Constitution. Ashcroft also emphasized to Lamberth that the FISC was not being asked to approve the program. Following Ashcroft's summary, Hayden described for Lamberth how the program functioned operationally, Yoo discussed legal aspects of the program, and Baker proposed procedures for handling international terrorism FISA applications that contained PSP-derived information. For the next four months, until the end of his term in May 2002, Lamberth was the only FISC judge read into the PSP.

~~(TS//SI//OC/NF)~~ Judge Colleen Kollar-Kotelly succeeded Lamberth as the FISC Presiding Judge and was briefed on the PSP on 17 May 2002. The briefing was similar in form and substance to that provided to Lamberth. In response to several questions from Kollar-Kotelly about the scope of the President's authority to conduct warrantless surveillance, DoJ prepared a letter to Kollar-Kotelly, signed by Yoo, that, according to Kollar-Kotelly, "set out a broad overview of the legal authority for conducting [the PSP], but did not analyze the specifics of the [PSP] program." The letter, which Kollar-Kotelly reviewed at the White House but was not permitted to retain, essentially replicated Yoo's 2 November 2001 memorandum regarding the legality of the PSP. Kollar-Kotelly was the only sitting FISC judge read into the PSP until January 2006, when the other FISC judges were read in.

~~(TS//SI//OC/NF)~~ Baker was read into the PSP only after he came upon "strange, unattributed" language in a FISA application that suggested the existence of a compartmented program. Baker advised that the FISC needed to be read into the program, but the White House initially resisted this idea. As noted, eventually Lamberth, and later his successor, Kollar-Kotelly, were read in. The DoJ IG believes that not having OIPR officials and members of the FISC read into the PSP, while program-derived information was being disseminated as investigative leads to the FBI and finding its way into FISA

documents, data, and other materials "if the item is within the government's possession, custody, or control" and the item is material to preparing the defense; the government intends to use the item in its case-in-chief at trial; or the item was obtained from or belongs to the defendant. (U)

Under Rule 16, a defendant's statements carry a "near presumption of relevance," and "the production of a defendant's statements has become 'practically a matter of right even without a showing of materiality.'" *United States v. Yunis*, 867 F.2d 617, 621-22, 625 & n.10 (D.C. Circuit 1989).[404] (U)

Disclosure of a defendant's statements is usually made by the government after receiving a request pursuant to Rule 16. However, even without making a Rule 16 request, a defendant has an independent right to discovery of his statements and certain other relevant information under *Brady v. Maryland*, 373 U.S. 83 (1963). *Brady* requires the government to disclose evidence in its possession favorable to the defendant and material to either guilt or punishment. Material evidence must be disclosed if it is exculpatory or if it could be used to impeach a government witness. (U)

According to an Office of Intelligence Policy and Review (OIPR) memorandum on the government's Rule 16 and *Brady* obligations, "[p]rudent prosecutors err heavily on the side of disclosure to avoid unnecessary discovery litigation or charges of prosecutorial misconduct." The memorandum noted that most courts and the Justice Department's Office of Professional Responsibility view an intentional failure to disclose *Brady* material as prosecutorial misconduct.[405] (U)

However, according to the memorandum, when production of the defendant's statements or other information would reveal classified information, the government may assert a national security privilege, sometimes known as the state secrets privilege.[406] If the government asserts a colorable claim in a legal proceeding that classified information is privileged, the defendant must show that the information is not only

---

[404] See also *United States v. Scarpa*, 913 F.2d 993, 1011 (2nd Cir. 1990), citing *United States v. McElroy*, 697 F.2d 459, 464 (2nd Cir. 1982)("Rule 16 does not cover oral statements unrelated to the crime charged or completely separate from the government's trial evidence."). (U)

[405] Counsel for Intelligence Policy James Baker told us the memorandum was drafted at his request by an Assistant U.S. Attorney who had been detailed to OIPR. Baker said he requested the memorandum to refresh his understanding of the government's discovery obligations in criminal prosecutions. (U//~~FOUO~~)

[406] The state secrets privilege is a common law doctrine asserted by the United States government to protect classified information. See generally, *United States v. Reynolds*, 345 U.S. 1 (1952). (U)

measures that were in place to keep Stellar Wind-derived information out of the criminal prosecution process. He stated that the FBI had "walled off" any evidence it collected from inclusion in criminal cases by tipping out Stellar Wind-derived information under [redacted] with a caveat that the information in the tipper was "for lead purposes only." Rowan noted that OIPR also had in place a scrubbing process to delete program-derived information from FISA applications. Rowan expressed confidence that these mechanisms ensured that no program information was used in international terrorism prosecutions.[416] Finally, Rowan stated that the FBI is "very quick to get FISAs up," thereby minimizing the likelihood that the NSA's Stellar Wind database would be the sole repository of *Brady* material. ~~(TS//STLW//SI//OC/NF)~~

B. May 2005 Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~

At the direction of Assistant Attorney General Wray, Rowan memorialized his research regarding these discovery issues in a memorandum entitled "Discovery Issues Raised by Stellar Wind." He completed the memorandum on May 4, 2005, shortly before Wray left the Department. Rowan said he worked on the memorandum largely alone, consulting occasionally with Wray. Rowan said it was very difficult to work on the matter because of the secrecy surrounding the program and the other demands of his job.[417] ~~(TS//STLW//SI//OC/NF)~~

In his May 2005 memorandum, [redacted]

[redacted]

[redacted]

[416] As discussed in Chapter Six, the caveats were intended to exclude at the outset any Stellar Wind-derived information from FISA applications and other criminal pleadings. The scrubbing process acts as a second check against including this information in FISA applications. However, neither the caveats nor the scrubbing process relieved the government of its obligations under *Brady* to disclose evidence in the government's possession favorable to the defendant and material to either guilt or punishment. ~~(TS//STLW//SI//OC/NF)~~

[417] The memorandum noted, "Because there were no additional attorneys within the Criminal Division who were read into the program (and very few in the Department generally), we have been unable to assign work to others or to fully consult with others within the Division." ~~(TS//SI//NF)~~

possesses potential *Brady* or other discovery material; or, (2) in the absence of such knowledge, where "there nonetheless exists any reliable indication suggesting" that the Intelligence Community possesses such material. USAM, Criminal Resources Manual § 2052 (2002). The USAM stated that, as a general rule, a prosecutor should not seek access to Intelligence Community files unless there is an affirmative obligation to do so. However, it noted that certain types of cases, including terrorism prosecutions, fall outside this general rule. In such cases, the USAM advised that the prosecutor should conduct a "prudential search." Id. ~~(TS//STLW//SI//OC/NF)~~

Rowan wrote that the practice in several sections within the Criminal Division was to "generally go beyond both the legal obligations outlined [in his memorandum] and the general rule outlined in the USAM, initiating searches out of prudence, rather than a legal obligation." For instance, Rowan reported that the practice of the Criminal Division's Counterespionage Section (CES) was to search Intelligence Community files in almost every case, even in instances in which the Intelligence Community had no involvement in the investigation or prosecution [redacted].[420] (TS//STLW//SI//OC/NF)

[redacted][421] In cases involving the NSA, the typical practice

[420] The OIG interviewed John Dion, the Chief of CES, which became part of the National Security Division in 2006. Dion stated that CES had no fixed policy for conducting prudential searches of Intelligence Community files, but rather approached the subject on a case-by-case basis. Dion stated that such searches are conducted in cases in which there is likely to be intelligence collection concerning the defendant as "suggested by the facts of the matter." He added that the searches were requested for a variety of reasons, including for purposes of meeting discovery obligations. Dion said that searches also were requested to determine whether the defendant has a "relationship" with an intelligence agency. He noted that CES does not request prudential searches as a matter of course to avoid making spurious requests. ~~(S//NF)~~

[421] [redacted] Dion said CES was a proponent of the position that line prosecutors with whom CES co-prosecutes cases should have the same knowledge as CES concerning the "national security equities" involved in each case. Dion said this arrangement also allows for the AUSA, who is often the prosecutor most familiar with the case and the jurisdictional practices, to review any Intelligence Community material for Rule 16 and *Brady* purposes. Dion acknowledged the limitations to this arrangement concerning strictly compartmented programs such as Stellar Wind, where the NSA understandably would be reluctant to read in line prosecutors for the limited purpose of screening defense discovery requests. ~~(TS//STLW//SI//OC/NF)~~

C. Office of Legal Counsel and Discovery Issue (U)

Shortly before Rowan finished his memorandum in May 2005, OLC Principal Deputy Assistant Attorney General Steve Bradbury became the acting head of OLC. Bradbury told us that he recalled having some discussion with Rowan about how discovery matters should be handled in connection with the Stellar Wind program. Bradbury said that John Eisenberg, later a Deputy in OLC, also may have discussed the matter with Rowan. Bradbury stated that he did not believe that OLC followed up on Rowan's request that it continue researching these issues. ~~(TS//STLW//SI//OC/NF)~~

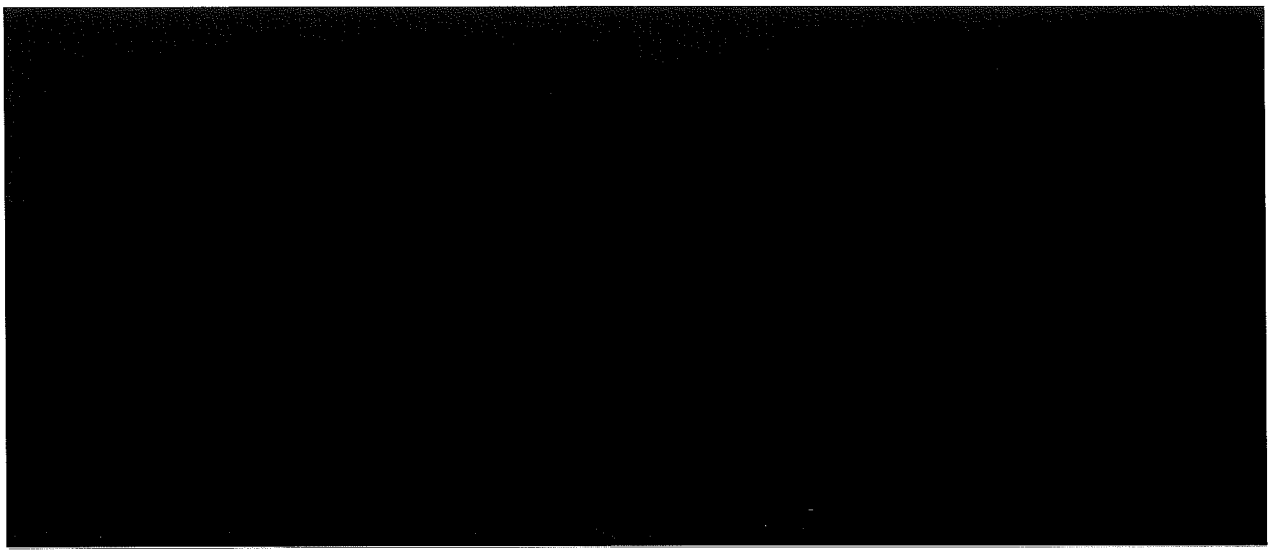
Eisenberg told us that he discussed the Rule 16 issue with Rowan at some point, but did not recall whether they discussed the *Brady* issue. He recalled discussing Yoo's [redacted] memorandum with Rowan and said he believes the Justice Department took the position that the Yoo memorandum was correct, at least with respect to Yoo's legal analysis in [redacted] (TS//STLW//SI//OC/NF) b1, b3, b6, b7C, b7E

When we showed Eisenberg a copy of Rowan's May 4, 2005, memorandum, Eisenberg stated that he had not previously seen it. Eisenberg told us that OLC would not typically be responsible for addressing the discovery issues presented in Rowan's memorandum and that he was not aware of any OLC opinion on the subject other than Yoo's memorandum. Eisenberg also said he was not aware of any formal procedures for handling Rule 16 disclosure requests or the government's affirmative *Brady* obligations other than the *ex parte* in camera motions practice pursued by the National Security Division, discussed below. ~~(TS//STLW//SI//OC/NF)~~

CES Chief Dion agreed that OLC would not be the appropriate entity to review discovery procedures in the context of Stellar Wind, in part because OLC attorneys generally do not have criminal litigation expertise. Dion suggested that if the Department were to develop procedures for handling discovery of Intelligence Community files, it should be done by the Department's National Security Division in coordination with United States Attorneys' Offices, and it should be binding only on those two entities. Rowan, while generally agreeing with Dion, told the OIG that he believed the OLC appropriately could have analyzed the legal issue of what impact a

---

National Security Division in 2006. [redacted] The results of these searches were produced to the courts *ex parte*, in camera, pursuant to CIPA. ~~(TS//STLW//SI//OC/NF)~~



V. OIG ANALYSIS (U)

We found that the Department made little effort to understand and comply with its discovery obligations in connection with Stellar Wind-derived information for the first several years of the program. The Department's limited initial effort was also hampered by the limited number of attorneys who were read into the program. As a result, OLC attorney John Yoo alone initially analyzed the government's discovery obligations in one early case, and he produced a legal analysis that was based on an incorrect understanding of the facts of the case to which it applied. When other attorneys from the Department's Criminal Division eventually were read into the program, their review of these discovery issues implicitly rejected Yoo's analysis. At that point, the Department eventually took steps to address, on a case-by-case basis, its discovery obligations. However, in our view, those steps are not complete and do not fully ensure that the government has met its discovery obligations regarding information obtained through the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

As described in this chapter, in 2002 the Department first recognized that the Stellar Wind program could have implications for discovery obligations in terrorism cases. OIPR Counsel Baker raised with Department

through electronic surveillance and physical search. Section 702(g) requires the Attorney General and the Director of National Intelligence to file written certifications with the FISA Court attesting to the fact that appropriate targeting and minimization procedures are in place, with copies of the procedures attached.[7] These certifications are subject to judicial review and provide the primary mechanism by which the FISA Court conducts its judicial oversight of the implementation of Section 702.

B1
B3
B7E

(TS)

(U//FOUO) Section 702 also requires extensive reporting and oversight concerning activities authorized under the statute. Section 707(b)(1) requires the Attorney General to provide Congress with a Section 702 Semiannual Report that includes:

- (U//FOUO) all certifications submitted during the reporting period;
- (U//FOUO) the reasons for the exercise of any exigent circumstances authority under Section 702(c)(2);
- (U//FOUO) any directives issued during the reporting period and a description of any action taken to enforce them;
- (U//FOUO) a description of any judicial review of the certifications and any targeting and minimization procedures during the reporting period;
- (U//FOUO) copies of any compliance review conducted by the Attorney General;
- (U//FOUO) copies of any procedures implementing Section 702; and
- (U//FOUO) a description of any incidents of noncompliance by the Intelligence Community or by the providers.

---

[7] (U//FOUO) Unlike traditional FISA applications seeking authority to conduct electronic surveillance within the United States, the certifications are "not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted." Section 702(g)(4).

Section 702(*l*)(1) requires the Attorney General and the Director of National Intelligence to conduct semiannual assessments of the FBI's compliance with its targeting and minimization procedures. Section 702(*l*)(2)(B) and (C) requires the Inspector General to review certain FBI activities related to U.S. persons. Section 702(*l*)(3)(A) requires the Director of the FBI to also conduct annual reviews of certain FBI activities concerning U.S. persons.

B. ~~(S//NF)~~ Roles of the FBI, the NSA, and the CIA in the 702 Program

~~(S//NF)~~ The FBI and the NSA are the only agencies authorized to acquire foreign intelligence information under Section 702. The Central Intelligence Agency (CIA) participates in Section 702 targeting activities by submitting its targeting requests to the NSA. The NSA is the lead agency in the 702 Program and during the OIG's review period was the only agency with the formal authority to initiate electronic surveillance [redacted] under FISA Court-approved FAA procedures. Thus, during our review period, the NSA initiated all such electronic surveillance [redacted] searches, although sometimes the NSA did so on behalf of the CIA or at the request of the FBI. B1 B3 B7E (S)

(~~S//NF~~) The basic roles and division of responsibilities among the FBI, the NSA, and the CIA are set forth in a Memorandum of Understanding that the three agencies entered into in April 2008, after the PAA expired and before the FAA was enacted.

~~(S//NF)~~ The FBI conducts two general activities under Section 702. First, it approves the NSA's requests to acquire [redacted] Before approving the NSA's requests, the FBI must review information about the foreignness of the presumed user of the designated account to ensure that the targeted user is a non-U.S. person reasonably believed to be located outside the United States. When the NSA seeks to acquire the [redacted] communications of designated targets, the FBI provides technical assistance only, and plays no role in approving the NSA's targeting decisions. Second, the FBI acquires both [redacted] from the participating providers and routes the raw unminimized data to the NSA and, at the NSA's direction, to the CIA and to the FBI's [redacted] (S) B1 B3 B7E

---

[8] ~~(S//NF)~~ As noted, a "selector" is either a telephone number or an identifier used for Internet communications, such as an e-mail account. Because the FBI's targeting activities under the 702 Program are limited to acquiring [redacted] from domestic electronic communications service providers (usually Internet service providers), the term "selector," as used throughout this report, refers to an identifier for Internet communications, such as an e-mail address. (S) B1 B3 B7E

(S) [redacted] The FBI retains a portion of the raw data for analysis and dissemination as finished intelligence products. B1 B3 B7E

~~(S//NF)~~ These two basic activities, which are discussed below and in detail in Chapters Three and Four of the OIG's report, are carried out by personnel in the Counterterrorism Division's [redacted] These personnel are drawn primarily from the [redacted] wo of five units within [redacted] We refer to these personnel as the 702 Team. The 702 Team is supported by the FBI's [redacted] and the [redacted] The 702 Team also works closely with attorneys from the FBI Office of General Counsel (OGC), including attorneys we refer to in this report as the Operations Attorney and the Policy Attorney.

III. (U) The FBI's Targeting Activities Under Section 702

(S//NF) The FBI's primary role in the 702 Program is to acquire the (S) [redacted] This process begins with the NSA's determination, based on intelligence from other agencies and its own analysis of signals intelligence already collected, that the [redacted] of a selector (typically an e-mail address) may yield foreign intelligence information. The NSA applies its FISA Court-approved targeting procedures to determine that the account is used by a non-U.S. person reasonably believed to be located outside the United States. B1 B3 B7E

~~(TS//SI//NF)~~ The NSA may apply its targeting procedures to target a selector for electronic surveillance, nominate a selector to the FBI [redacted] (TS) When the NSA targets a selector for electronic surveillance, the FBI, through [redacted], provides technical assistance only. When the NSA nominates a selector [redacted] the 702 Team must first apply the FBI's own targeting procedures before conducting the [redacted] B1 B3 B7E

~~(S//NF)~~ The NSA [redacted] nominations are forwarded to the 702 Team in two ways: (1) by "selector sheets" that are e-mailed to the 702 Team each day, and (2) through an FBI system called PRISM, [redacted] (The CIA receives PRISM information [redacted].) [redacted] (S) B1 B3 B7E

information." In view of these provisions, the 702 Team approaches its targeting responsibilities with considerable deference to the NSA's targeting judgments.

(U//FOUO) We concluded that overall the FBI's 702 Team has implemented its targeting procedures with commendable deliberation, thoroughness, and professionalism. Our more specific findings regarding the FBI's targeting activities are summarized below.

1. ~~(S//NF)~~ Findings and Recommendations Relating to the FBI's Review and Evaluation of the Sufficiency of the NSA's Foreignness Determinations

~~(S//NF)~~ The FBI's review and evaluation of the sufficiency of NSA's foreignness determinations is a critical step in the FBI's [redacted] approval process because for approximately two-thirds of all NSA nominations in the OIG's review period, the FBI uncovered no information [redacted] (S) [redacted] about the account or its presumed user, and thus approved NSA nominations based solely on the NSA's foreignness determinations. B1 B3 B7E

[redacted] (S) B1 B3 B7E

a. ~~(S//NF)~~ The [redacted] Factor (S)

~~(TS//SI//NF)~~ The OIG determined that approximately 8 percent of nominations submitted to the FBI during the OIG's review period were based on the [redacted] factor, which is defined in the FBI's SOPs as follows: [redacted] (TS) B1 B3 B7E

[9] ~~(S//NF)~~ After reviewing a draft of this report, the NSA objected to this characterization of the FBI's [redacted] authority to the extent it suggests that the NSA lacks the fundamental authority to acquired [redacted] pursuant to Section 702.

Officer raised concerns that the [redacted]

~~(S//NF)~~ To address these concerns, the FBI implemented a special review process for nominations involving targeted users who have [redacted] B1 B3 B7E (S)

During the OIG's review period, the FBI's OGC consulted with attorneys in the NSD when conducting these reviews.

~~(TS//SI//NF)~~ The OIG identified approximately [redacted] that had been subject to some level of FBI analysis for [redacted] our review period. We determined that the FBI never rejected a nominated selector based explicitly on [redacted] concerns during the review period. We also conducted a careful review of selector files and concluded that although the OGC collected all the information relevant to making a [redacted] determination for each selector it reviewed, there did not appear to be a discernable set of principles guiding the FBI OGC's analysis of [redacted] However, we believe that the FBI's [redacted] process was not a meaningless exercise. The NSA withdrew several selectors after learning that the FBI had found recent [redacted] by the target and would be submitting the nomination to the FBI OGC for review. (TS) B1 B3 B7E

~~(TS//SI//NF)~~ The OIG also analyzed nominations for [redacted] involving targets who had [redacted] (TS) B1 B3 B7E

information shows that the user of the targeted selector was in the United States on the day the user's [redacted] were acquired. For other acquisitions, the data contains a strong indication that the user was likely in the United States on the day the user's communications were acquired, but the information available to the OIG was not sufficient to determine with certainty that each of the incidents in fact met the FBI's statutory reporting criteria. We believe that the FBI's expertise in analyzing presumed users' [redacted] in the targeting context can be applied to determine whether a user was in the United States at the time an acquisition occurred, and therefore ineligible for coverage under Section 702. B1 B3 B7E (TS)

~~(S//NF)~~ In July 2011, the OIG met with senior FBI Counterterrorism Division, OGC, and Inspection Division officials to present our preliminary findings and the methodology we used to reach them. The FBI officials stated at that time that the FBI was still exploring how to compile the requisite information for its 2010 reporting period. They also expressed concern about being required to report on acquisitions for particular selectors that may also be the subject of separate reporting by the NSA, resulting in what they characterized as [redacted] B1 B3 B7E (S)

~~(S//NF)~~ The OIG does not believe there is any merit to this concern. First, the statute unambiguously requires this accounting from "the head of each element of the intelligence community conducting an acquisition under [Section 702(a)]." See Section 702(*l*)(3). The FBI and the NSA both conduct acquisitions under Section 702, and therefore both agencies are required to submit these reports. [redacted] (S)

[redacted] B1 B3 B7E these distinctions, it is understandable that Congress would want to assess these acquisitions separately. Third, to the extent there are reportable acquisitions for both agencies arising from the conduct of electronic surveillance [redacted] for the same selector, that fact can be noted in the FBI's annual reports.

(U//FOUO) The OIG recommends that the FBI amend its 2009 annual report and ensure that it fulfills its reporting obligations under Section 702(*l*)(3)(A)(iii) without delay.

~~(S//SI//NF)~~ [redacted] B1 B3 B7E (S)

October 2009, none of the Section 702 data that the FBI acquired for the NSA was dual routed to and retained by the FBI.

~~(S//NF)~~ Section 702 data that is dual routed to the FBI is maintained in the [redacted] along with other FISA-acquired (S) information. [redacted] administered by the [redacted] The FBI is required to acquire, retain and disseminate Section 702 information in accordance with its FISA Court-approved Standard Minimization Procedures (SMPs). B1 B3 B7E

A. (U//FOUO) The FBI's Standard Minimization Procedures

~~(S//NF)~~ As required by the FISA statute, the FBI's SMPs are "specific procedures that are reasonably designed in light of the purpose and technique of the particular surveillance or physical search to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. §§ 1801(h) & 1821(4). Though initially designed to apply to information of or concerning a United States person that was collected under traditional FISA, the SMPs were adapted to Section 702 through Attorney General-approved language that conforms relevant provisions to Section 702. The FBI has also developed various internal guidance documents to explain how 702-acquired data must be handled by FBI personnel.

~~(S//NF)~~ The SMPs provide that the FBI may only acquire 702 information in accordance with its targeting procedures, and must purge from its systems any communication it has acquired and retained that is inconsistent with the targeting and acquisition limitations set forth in Section 702(b).

~~(S//NF)~~ The retention provisions of the SMPs restrict access to 702-acquired information to authorized users who have been trained on the requirements of the SMPs and Section 702. The SMPs provide that authorized users may access raw FISA-acquired information on a continuing basis only as necessary to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime (the SMP minimization standards). Once information has been assessed as meeting SMP minimization standards, it may be disseminated – that is, made more broadly available outside of [redacted] However, if the information is "of or concerning" a United States person, the FBI's SMP Policy Implementation Guidelines (SMP

Guidelines) require that the information first be electronically "marked" [redacted] as having met SMP minimization standards before it may be disseminated.[13] B1 B3 B7E (S)

~~(S//NF)~~ Under the FBI's SMP Guidelines, only case coordinators in [redacted] (where the 702 Team is located) are authorized to mark 702-acquired information in [redacted]. In practice, however, the burden is on the operators in the field to apply SMP minimization standards to the information they wish to have marked. Thus, the 702 Team case coordinators defer considerably to the knowledge and judgment of the requesting agents and analysts concerning which marking to apply and why the marking is justified.

B. ~~(S//NF)~~ FBI Retention of Section 702-Acquired Information

~~(S//NF)~~ For the FBI to retain 702-acquired data for its own analysis, it must first request the NSA to allow the data to be "dual routed" to the FBI. The OIG examined the evolution of the FBI's Section 702 dual routing and retention policies and practices through April 2010, as well as how the data is maintained in and purged from FBI systems.

1. ~~(S//NF)~~ Findings Relating to Early Dual Routing and Retention Issues

~~(S//NF)~~ The FBI did not begin to request dual routing of 702 data until October 14, 2009, [redacted] B1 B3 B7E (S)

[redacted] B1 B3 B7E (S)

[13] (U//FOUO) If the information of or concerning a U.S. person does not meet the SMP minimization standards, the FBI must "strike or substitute a characterization" for the person's identity before the information may be disseminated. SMPs, Section III.C.

and (ii). As noted above, the FBI submitted one annual report that covered the period of September 1, 2008, through August 31, 2009 (the 2009 reporting period). Because the FBI did not begin retaining 702-acquired data until after the 2009 reporting period, it reported that it "did not disseminate any intelligence reports containing a reference to a United States-person identity derived from acquisitions conducted under [Section 702(a)]" during that period. For the same reason, the FBI also reported that it did not disseminate any U.S. person identities that were not referred to by name or title in original reporting.

~~(S//NF)~~ In conducting its statutorily mandated review, the OIG reviewed the [redacted] intelligence reports that the FBI disseminated between December 2009 and April 2010. These reports would fall within the FBI's annual reporting period for September 1, 2009, through August 31, 2010. However, as of February 2012, the FBI had not conducted this statutorily required annual review.[17] B1 B3 (S) B7E

~~(S//NF)~~ The OIG read its mandatory review provision broadly to include any reference to a U.S. person identity in a disseminated intelligence report that was materially related to a Section 702 acquisition – even if the reference to the U.S. person's identity was not directly acquired under authority of Section 702. [redacted] Even though the communications or identities of these U.S. persons were not acquired directly under Section 702, we believe that the references were "with respect to" 702 acquisitions within the meaning of the reporting provisions of Section 702. B1 B3 B7E (S)

~~(S//NF)~~ [redacted] b1 b3 b7E (S)

[17] ~~(S//NF)~~ The FBI submitted its annual reports for September 1, 2009, through August 31, 2010, and September 1, 2010, through August 31, 2011, on May 22, 2012.

[redacted] (S)

b1
b3
b7E

(U//FOUO) The OIG determined that the FBI did not develop a strategy for meeting its annual reporting requirement to provide "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." In fact, beyond generally acknowledging that this reporting requirement applies to a broader spectrum of information than the SMPs and minimization guidance apply to, it appeared to the OIG that FBI personnel gave very little thought to this important statutory obligation. Several witnesses, including the Operations Attorney, told the OIG that guidance was needed to provide direction on how to comply with the reporting requirements of Section 702(*l*)(3)(A)(i) and (ii).

~~(S//NF)~~ The OIG recommends that the FBI OGC promptly issue guidance for meeting its annual reporting requirements under Section 702(*l*)(3)(A)(i) and (ii). In drafting this guidance, the FBI should develop a reasonable interpretation of that section's "with respect to" language that ensures that the FBI's reports to Congress fully and accurately convey the information Congress seeks, keeping the following principles in mind. The guidance should explain that that the reporting criteria extends broadly to disseminated intelligence reports containing a reference to a U.S. person identity that is "with respect to" to a Section 702 acquisition, and may therefore include reports in which the U.S. person is identified through a source other than the 702-acquired material.[18] The guidance should also explain that a "reference to a United States-person identity" for statutory reporting purposes is broader than the application of the SMPs to "nonpublicly available information concerning unconsenting United States persons," and that a reference to a U.S. person identity also may appear in metadata, such as in an e-mail address.[19] Lastly, we believe that the FBI should create a system

---

[18] [redacted] (S)

b1
b3
b7E
Per FBI

[19] [redacted] (S) (Cont'd.)

b1
b3
b7E
Per FBI

for tracking intelligence reports that meet the reporting criteria as the reports are disseminated (or as the FBI disseminates U.S. person identities previously not identified in such reports) so that its annual accountings can be issued in a timely manner.

V. (U) Conclusion

~~(S//NF)~~ The OIG believes that in general the FBI responsibly implemented its Section 702 targeting procedures during our review period.

[redacted]

b1
b3
b7E
Per FBI

(S)

~~(S//NF)~~ The OIG found that the FBI generally conducted its post-targeting activities responsibly as well, and approached its authority to retain and disseminate 702-acquired data with deliberation and foresight from the standpoint of ensuring compliance with the requirements and limitations of Section 702. [redacted]

b1
b3
b7E
Per FBI

(S)

[redacted]

(S)

b1
b3
b7E
Per FBI

(U//FOUO) Section 702, which is the focus of this report, allows the Attorney General and the Director of National Intelligence to jointly authorize, for up to 1 year, the targeting of non-U.S. persons reasonably believed to be located outside the United States. To exercise this authority, the Attorney General and the Director of National Intelligence must adopt targeting and minimization procedures that govern how targets are determined to be non-U.S. persons outside the United States and how the information acquired may be retained and disseminated. The statute places limitations on the government's targeting authority by prohibiting the intentional targeting of persons known to be in the United States at the time of acquisition, and the targeting of persons outside the United States where the purpose of the acquisition is to obtain the communications of "a particular, known person reasonably believed to be in the United States" (a practice known as "reverse targeting"). The targeting and minimization procedures adopted by the Attorney General and the Director of National Intelligence are subject to FISA Court review and approval.

~~(S//NF)~~ Section 702 also requires the government to certify that "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider." Under Section 702, foreign intelligence is obtained from these U.S.-based electronic communications service providers (U.S. providers) either by conducting electronic surveillance of communications as they are transmitted, or by conducting a search of communications that are in electronic storage after they have been transmitted.

~~(S//NF)~~ The Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) are the only agencies authorized to acquire foreign intelligence information under Section 702. The NSA is the lead agency in the 702 Program and, during the OIG's review period, was the only agency with the formal authority to initiate electronic surveillance [redacted] under FISA Court-approved targeting procedures. Thus, during our review period, the NSA initiated all such electronic surveillance [redacted] although sometimes the NSA did so on behalf of the Central Intelligence Agency (CIA), or at the request of the FBI. B1 B3 B7E (S)

~~(S//NF)~~ [redacted] B1 B3 B7E (S)

authorized the NSA, [redacted] to intercept the content of communications into and out of the United States where there was a reasonable basis to conclude that at least one of the communicants was a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.

~~(TS//SI//NF)~~ The TSP and the other intelligence activities authorized by the President under the PSP were legally controversial because these activities traditionally were viewed to be governed by the FISA statute.[26] Subject to certain statutory exceptions, and until it was amended in 2007 by the PAA, FISA generally required the approval of the FISA Court whenever the government sought to acquire, for foreign intelligence purposes, "the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." For the FISA Court to grant authority to conduct electronic surveillance, the government would first have to establish probable cause to believe that the target of the surveillance is a "foreign power" or an "agent of a foreign power," and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used" by the target. FISA imposed similar legal requirements to conduct a physical search, including of stored electronic communications.

(U//FOUO) When FISA was enacted in 1978, most international telephone calls were carried by satellite. Under FISA, the interception of such calls constituted "electronic surveillance" only if the acquisition intentionally targeted a U.S. person in the United States, or if all participants to the communication were located in the United States. Thus, government surveillance of satellite communications that targeted foreign persons outside the United States generally was not considered electronic surveillance, and the government was not required to obtain a FISA Court order authorizing the surveillance, even if one of the parties to the communication was in the United States.

~~(TS//SI//NF)~~ In the mid-1980s, however, fiber optic technology began to replace satellites as the primary means for transmitting international (and domestic) communications. Because many of these communications were now "wire communications" routed through and acquired inside the United States,

---

[26] (U//FOUO) Proponents of this view cite 18 U.S.C. § 2511(2)(f), which states, in relevant part, that the

> (U) procedures in [chapter 119 and 11 of title18] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(U//FOUO) In addition to addressing targeting and minimization requirements in the certification, the Attorney General and the Director of National Intelligence also were required to certify that the acquisition involved obtaining the foreign intelligence information from or with the assistance of a communications service provider having access to the communications, either as the communications were transmitted or while they were stored, and that a "significant purpose of the acquisition is to obtain foreign intelligence information[.]"

(U//FOUO) The PAA left unchanged the procedures for acquiring foreign intelligence information by targeting foreign powers or agents of foreign powers in the United States, as well as the procedures under Executive Order 12,333 (E.O. 12,333) Section 2.5, to obtain Attorney General approval before acquiring foreign intelligence information against a U.S. person outside the United States.

~~(S//NF)~~ The first PAA certification was filed with the FISA Court on August 9, 2007. [redacted] (S) were filed with the FISA Court under the PAA. The FISA Court reviewed these certifications and approved them, allowing the government to continue the activities authorized by the Attorney General and the Director of National Intelligence to acquire foreign intelligence information concerning persons reasonably believed to be outside the United States without individualized FISA Court approval for up to one year. These acquisitions were conducted by the NSA. As of January 31, 2008, the PAA certifications also authorized the FBI to acquire [redacted] on behalf of the NSA. After the PAA expired on (S) February 16, 2008, the government's foreign intelligence acquisition authority under the statute gradually lapsed as the individual certifications expired. The final PAA certification expired in April 2009.

B1
B3
B7E

[redacted]

B1
B3
B7E

(S)

The respective roles of the NSA, the CIA, and the FBI under the PAA

were formalized in a Memorandum of Understanding (MOU) signed in April 2008.[31]

~~(S//SI//NF)~~ The FBI's role under the PAA thus became virtually identical to its current role under the Section 702 of the FAA – to acquire, on behalf of the NSA (and the CIA through the NSA), [redacted] persons reasonably believed to be located outside the United States, and to provide technical assistance to the NSA in acquiring the in-transit communications of persons reasonably believed to be outside the United States. (S) B1 B3 B7E

(U//FOUO) Although the Department viewed the PAA as an adequate temporary fix to those provisions of FISA seen as outdated because of changes in telecommunications technology, Department and other Intelligence Community officials continued to press Congress for more permanent modernization legislation. The result of these efforts was the FISA Amendments Act of 2008.

II. (U) The FISA Amendments Act of 2008

(U//FOUO) The FISA Amendments Act of 2008 (FAA) was signed into law as Public Law 110-261 on July 10, 2008. According to the FAA's legislative history, Congress had two primary goals in passing the FAA. First, Congress wanted to provide a sound statutory framework, consistent with the Constitution, enabling the targeting of persons reasonably believed to be located outside of the United States for the acquisitions of foreign intelligence information, while simultaneously affording additional protections to United States persons whose communications are targeted for collection or collected incidentally. In striking this balance, Congress discarded the PAA's redefinition of the term "electronic surveillance," which had excluded from FISA's individualized order requirement *all* persons outside the United States, including U.S. persons, and instead promulgated a specific authorization for the acquisition of communications from *non*-U.S. persons located outside the United States without an individualized order. The result was a sharply narrowed statute under which U.S. persons overseas could no longer be

[31] ~~(S//NF)~~ According to an attorney in the FBI's Office of General Counsel who participated in drafting the Memorandum of Understanding (MOU), the document took a long time to negotiate, and was not finalized until after the PAA expired. However, the attorney stated that the MOU remained in effect after the PAA expired because certifications issued under the PAA were valid for one year, and thus the use of PAA authority extended beyond the PAA's expiration. This attorney also stated that the MOU remains in effect under the FAA to the extent it is relevant to the FAA's provisions. Thus, provisions in the MOU concerning targeting the accounts of U.S. persons, which is prohibited under the FAA, are considered void.

b. (U//FOUO) Procedural Requirements of Section 702

(U//FOUO) Section 702(c) requires that acquisitions authorized pursuant to Section 702(a) shall conform to "the targeting and minimization procedures adopted in accordance with subsections (d) and (e)," and "upon submission of a certification in accordance with subsection (g), such certification," as explained below. FAA, Section 702(c)(1).

(U//FOUO) Section 702(d) requires the Attorney General, in consultation with the Director of National Intelligence, to adopt targeting procedures that are reasonably designed to ensure that the acquisition of foreign intelligence information pursuant to Section 702 complies with the limitations in subsections (a) and (b). Specifically, Section 702(d)(1)(A) requires that the procedures "ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States," and Section 702(d)(2)(B) requires that the procedures "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." These targeting procedures are subject to judicial review.[36]

~~(U//FOUO)~~ Section 702(e) requires the Attorney General, again in consultation with the Director of National Intelligence, to adopt minimization procedures governing the retention and dissemination of information acquired under Section 702(a) that meet the statutory rules in FISA that are otherwise applicable to data acquired through electronic surveillance and physical searches. Those provisions of FISA provide that the minimization procedures must be designed to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." The minimization procedures adopted under the FAA are subject to judicial review.[37]

(U//FOUO) In addition to specific targeting and minimization procedures, Section 702(f) requires the Attorney General, in consultation with

---

[36] ~~(S//NF)~~ At present, only the NSA and the FBI conduct acquisitions under Section 702, and thus are required to submit their targeting procedures to the FISA Court for review. The CIA nominates selectors for electronic surveillance to the NSA, [redacted] through the NSA to the FBI, and therefore does not submit targeting procedures to the FISA Court. The NSA's and FBI's targeting procedures are discussed in Chapter Three. B1 B3 (S) B7E

[37] ~~(S//NF)~~ The CIA, NSA, and FBI each receives raw Section 702-acquired data and is required to retain and disseminate such data in accordance with its own minimization procedures. Therefore, the FISA Court must review the minimization procedures of all three agencies. The FBI's minimization procedures are discussed in Chapter Four.

[redacted]

[redacted] B1 B3 B7E (S)

(U//FOUO) NSA Targeting Procedures at 4.

~~(TS//SI//NF)~~ The NSA targeting procedures also govern the NSA's assessment of the foreign intelligence purpose of the targeting, which is an assessment of "whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory."

[redacted]

~~(TS//SI//NF)~~ When the NSA's post-targeting analysis reveals that a target has entered the United States or is a United States person, the targeting

---

which the target is referred to in the content of a communication. Electronic communications "about" a 702 target are only collected "upstream" of U.S. providers, and the NSA has represented to the FISA Court that "no about communications will be obtained by acquisitions conducted by the FBI."

(S//NF) CHAPTER FOUR
THE FBI'S POST-TARGETING ACTIVITIES: ACQUISITION, ROUTING, RETENTION, MINIMIZATION, AND DISSEMINATION OF SECTION 702 INFORMATION

~~(S//NF)~~ In this chapter we examine the FBI's post-targeting activities under Section 702 from September 2008 through the end of April 2010. Unlike the activities discussed in Chapter Three concerning the FBI's [redacted] (S) [redacted] many of its post-targeting activities did not commence until over a year after the FAA was enacted; most significantly, the FBI did not begin retaining Section 702-acquired data or disseminating it in intelligence reports until October 2009. B1 B3 B7E

~~(S//NF)~~ In Section I we provide an overview of the FBI's FISA Court-approved Standard Minimization Procedures for FISA electronic surveillance and physical search, as adapted to Section 702. In Section II we summarize how the FBI acquires 702 communications from participating providers and routes the communications within the Intelligence Community. In Section III we discuss 702 data retention issues, including a description of the FBI's dual routing policies and practices and how unminimized 702 data is retained. In Section IV we focus on the dissemination process for 702-acquired information. In Section V we describe our review of the number of disseminated intelligence reports containing a reference to a U.S. person identity, as required under Section 702(*l*)(2)(B). In Section VI we provide the OIG's analysis of the FBI's post-targeting activities under Section 702 during our review period.

I. (U//FOUO) FBI's Standard Minimization Procedures

(U//FOUO) "Minimization" is a process designed to ensure the appropriate acquisition, retention, and dissemination of information concerning U.S. persons that is acquired under Section 702 and other surveillance authorities. Minimization is necessary in part because targeting processes may result in the acquisition of communications that are irrelevant to the purpose of the surveillance. Authorized personnel are responsible for reviewing the communications to assess whether they meet the agency's standards for retention and dissemination, and for memorializing these assessments by annotating or "marking" the acquired communications before they can be made more broadly available. This assessment process generally is referred to as "minimization."

(U//FOUO) Under Section 702(e) of the FAA, the Attorney General, in consultation with the Director of National Intelligence, must adopt minimization procedures for acquisitions authorized under Section 702(a). The minimization procedures adopted under 702 must meet the minimization

standards for electronic surveillance and physical search as defined in the FISA statute. As such, the FBI's minimization procedures must be reasonably designed in light of the purpose and technique of the particular electronic surveillance or physical search, to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. §§ 1801(h) & 1821(4).

(U//FOUO) The FBI's minimization procedures are reviewed and approved by the FISA Court as part of the government's Section 702 certifications and serve as the primary authority governing the FBI's handling of raw 702-acquired information.[95] The FBI's minimization procedures in effect during the period covered by this review are entitled "Standard Minimization Procedures for Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act" (SMPs). Though designed to apply to information collected under traditional FISA, the SMPs were adapted to Section 702 through Attorney General-approved language that conforms relevant provisions to Section 702.[96]

~~(S//NF)~~ Among other changes, the 702 conforming language requires the FBI to remove from FBI's systems the communications of "a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or is subsequently determined to be a United States person." This amendment was necessary because the specific foreignness requirement of Section 702(a) (reasonable belief that a target is a non-U.S. person located outside the United States) is not an element of traditional FISA.

~~(S//NF)~~ The Attorney General adopted the SMPs after concluding that they meet the requirements of the FISA statute.

~~(S//NF)~~ The FBI's SMPs for all [redacted] in place from October 14, 2009, when the FBI began retaining Section 702-acquired information and thus was first required to apply its minimization procedures, through April 30, 2010, the end of our review period, are identical. The SMPs are organized (S) B1 B3 B7E

---

[95] (~~S//NF~~) The CIA, NSA, and FBI each receives raw Section 702-acquired information and is required to retain and disseminate such information in accordance with its own minimization procedures. The FISA Court must review and approve the minimization procedures of all three agencies. The FISA Court was not required to review and approve each agency's minimization procedures under the PAA. See PAA, Section 105C.

[96] (U//FOUO) This Attorney General-approved language is referred to in this report as the "702 conforming language." Unless otherwise indicated, references in this report to the SMPs in effect during our review period incorporate the 702 conforming language.

around three basic phases of the minimization process: acquisition, retention, and dissemination. Below we summarize key provisions of the FBI's SMPs, as adapted to Section 702, and as interpreted by the FBI in relevant guidance.

A. (U//FOUO) Acquisition

~~(S//NF)~~ The SMPs govern the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons that the FBI obtains under traditional FISA and Section 702. The SMPs provide that "information acquired from electronic surveillance or physical search conducted under FISA concerning United States persons may be used and disclosed by Federal officers and employees without the consent of the United States persons" only in accordance with the SMPs. SMPs, Section I.B. The SMPs do not apply to publicly available information about United States persons or to information "acquired, retained, or disseminated with a United States person's consent." In addition, with limited exceptions not applicable to this report, the SMPs do not apply to information concerning non-United States persons. Id.

(U//FOUO) The SMPs adopt the FISA definition of "United States person," which is:

> (U) a citizen of the United States, an alien lawfully admitted for permanent residence [as defined in 8 U.S.C. § 1101(a)(20)], an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power as defined [in 50 U.S.C. § 1801(a)(1), (2), or (3)]

(U) 50 U.S.C. § 1801(i).

~~(S//NF)~~ The SMPs also include presumptions about United States person status for purposes of implementing the SMPs. These presumptions, set forth below, are important because the SMPs require references to United States person identities to be stricken in disseminated material unless the information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime:

> ~~(S//NF)~~ [I]f an individual is known to be located in the United States, or if it is not known whether the individual is located in or outside of the United States, he or she should be presumed to be a United States person unless the individual is identified as an alien who has not been admitted for permanent residence or circumstances give rise to the reasonable belief that the individual

> is not a United States person. If an individual is known or believed to be located outside the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or circumstances give rise to the reasonable belief that the individual is a United States person. In an on-line operation, if it is not known whether an individual is located in or outside of the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or circumstances give rise to the reasonable belief that the individual is a United States person.

(U//FOUO) SMP General Provisions, ¶ C.

~~(S//NF)~~ The SMPs provide that the FBI may acquire [redacted] (S) [redacted] under Section 702 only in accordance with the FBI's targeting procedures, as adopted by the Attorney General, in consultation with the Director of National Intelligence, under Section 702(d). B1 B3 B7E

~~(S//NF)~~ The SMPs also require the FBI to "remove from FBI systems upon recognition" any communication acquired through targeting a person reasonably believed to be outside the United States or a non-U.S. person at the time of targeting, but who is in fact inside the United States or a U.S. person at the time of acquisition." The FBI is allowed to retain such communication only if the Director or Deputy Director determines in writing that the communication "is reasonably believed to contain significant foreign intelligence information, evidence of a crime that has been, is being, or is about to be committed, or information retained for cryptanalytic, traffic analytic, or signal exploitation purposes."

~~(S//NF)~~ Finally, the FBI is required to purge from its systems any communication it has acquired and retained that is inconsistent with the targeting and acquisition limitations set forth in Section 702(b).[97] This purging

---

[97] (U//FOUO) As described in Chapter Two, Subsection 702(b) provides that "[a]n aquisition authorized under subsection (a)—"

> (U) (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (U) (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (U) (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (U) (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(Cont'd.)

requirement extends to all copies of the acquired communication that are accessible to any "end user electronically or in hard copy."[redacted] (S)

[redacted] B1 B3 B7E

B. (U//FOUO) Retention

(~~S//NF~~) The retention provisions of the SMPs govern the storage of, access to, and use of FISA-acquired information within the FBI's data storage systems. The SMPs define "FISA-acquired information" to mean "all information, communications, material, or property that the FBI acquires from electronic surveillance or physical search conducted pursuant to FISA."[98]

~~(S//NF)~~ The SMPs restrict access to this information to "authorized users." Authorized users are personnel who have been trained on the

---

(U) (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(U) FAA Section 702(b).

[98] (~~TS//SI//NF~~) The SMPs also define "Raw FISA-acquired information" to mean:

"information that (a) is in the same or substantially same format as when the FBI acquired it, or (b) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime."

SMPs, Section III.A. Pursuant to a FISA Court Order dated July 22, 2002, and made permanent by an order dated May 19, 2004, the FBI has been allowed to share raw, or "unminimized," FISA-acquired data related to international terrorism with the CIA and the NSA for further analysis, retention, and dissemination in accordance with their own FISA Court-approved minimization procedures. The series of filings that led to these information-sharing procedures are generally known as the "Raw Take Motion" and the "Raw Take Order." Prior to the Raw Take Order, the CIA and the NSA received FISA data collected by the FBI related to international terrorism "only if and when" it was disseminated pursuant to the FBI's SMPs. Motion for Amended Orders Permitting Modified Minimization Procedures, filed with the FISA Court on May 10, 2002, under multiple docket numbers.

requirements of the SMPs and Section 702, [redacted] B1
[redacted] The SMPs also require the FBI to maintain records of all B3
personnel who have been granted access to this information and who have (S) B7E
accessed the information. [redacted]

~~(S//NF)~~ The SMPs provide that authorized users may access raw FISA-acquired information on a continuing basis only as necessary to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime (the SMP minimization standards). SMPs, Section III.B. Once raw FISA-acquired information has been assessed as meeting the SMP minimization standards, the FBI may retain the information for further investigation and analysis, and may disseminate it in accordance with other SMP requirements described below.

~~(S//NF)~~ [redacted] (S)
B1
B3
B7E

~~(S//NF)~~ [redacted] B1
B3
(S) B7E

~~(S//NF)~~ [redacted] B1
B3
(S) B7E

[99] (U) As of May 2011, the FBI had approximately 35,437 employees, including 13,963 special agents and 21,474 support personnel. See http://www.fbi.gov/about-us/quick-facts.

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

C. (U//FOUO) Dissemination

~~(S//NF)~~ Lastly, the SMPs govern the dissemination of FISA-acquired information "of or concerning United States persons," both domestically and to foreign governments. The FBI may disseminate FISA-acquired information concerning United States persons that reasonably appears to be foreign intelligence information to federal, state, local, and tribal officials and agencies. The FBI also may disseminate, for law enforcement purposes, FISA-acquired information concerning United States persons that reasonably appears to be evidence of a crime but not foreign intelligence information, but must do so consistent with the rules governing access to FISA-acquired information in connection with criminal investigations and proceedings. The dissemination must also include a statement that such disclosure may only be used in a criminal proceeding with the advance authorization of the Attorney General. (S)

[redacted] B1 B3 B7E

~~(S//NF)~~ Disseminations of FISA-acquired information concerning United States persons to the governments of the United Kingdom, Canada, Australia, or New Zealand require approval of the Director of the FBI or a designee. Disseminations of this information to other foreign governments also require the approval of the Director or a designee not lower than Section Chief, and must be made in coordination with the FBI OGC. The SMPs require the FBI to maintain a record of all disseminations to foreign governments concerning United States persons and to report this information to the Attorney General or a designee on a quarterly basis. SMPs, Section IV.C. FBI officials told the OIG that there were no disseminations to foreign governments concerning United States persons during the OIG's review period.

~~(S//NF)~~ Section II below describes how the FBI physically acquires 702 data from participating providers and routes the data into [redacted] (S) B1 B3 B7E

[redacted] (S)

B1
B3
B7E

3. [redacted] (S)

[redacted] (S)

B1
B3
B7E

[redacted] (S)

B1
B3
B7E

[redacted] (S)

B1
B3
B7E

b. ~~(S//NF)~~ Purging 702 Data from [redacted] FBI Systems (S)

B1
B3
B7E

~~(S//NF)~~ The FBI's SMPs require that "[a]ny communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or is subsequently determined to be a United States person will be removed from FBI systems upon recognition . . . ."

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

~~(S//NF)~~ The SMPs define "FISA-acquired information" to mean "all information, communications, material, or property that the FBI acquires from electronic surveillance or physical search conducted pursuant to FISA." SMPs, Section III.A. This definition is made applicable to Section 702 by the 702 conforming language.

~~(S//NF)~~ According to both the Operations Attorney and NSD officials, "FISA-acquired information" includes both the content and metadata of electronic communications acquired under FISA.

4. (U//FOUO) U.S. Person

~~(S//NF)~~ The SMPs adopt the definition of "United States person" used in the FISA statute, which provides that a "United States person" is "a citizen of the United States, an alien lawfully admitted for permanent residence [as defined in 8 U.S.C. § 1101(a)(20)], an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power as defined [in 50 U.S.C. § 1801(a)(1), (2), or (3)]." 50 U.S.C. § 1801(i). The SMPs also contain certain presumptions about U.S. person status (see Section I.A. of this chapter), which are reiterated in the SMP Guidelines.

~~(S//NF)~~ The Operations Attorney stated that the definition of U.S. person supplied in the FISA statute should also apply for purposes of the reporting provisions of Section 702(*l*)(2) and (3).

B. ~~(S//NF)~~ Role of the 702 Team in Disseminations of 702-Acquired Information

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

[redacted] (S) B1 B3 B7E

122

---

120 (U//FOUO) The version of this report that has been distributed outside the Department of Justice contains redactions in this sentence based on the Department's assertion of the attorney-client privilege.

121 (U//FOUO) The FBI may issue National Security Letters to obtain transactional data and subscriber information for electronic communications upon the FBI Director or his designee's certification that the "information sought is relevant to an authorized investigation 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 of the United States." 18 U.S.C. § 2709(b).

[redacted] (S) B1 B3 B7E