(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: June 1, 2012 – November 30, 2012

August 2013

(U) As part of the government's response to recent unauthorized disclosures, the government is currently conducting a review of the information contained in this report to determine the appropriate level of classification. If, following that review, new classification determinations are made that affect how this report is marked for classification purposes, a revised version of this report will be issued with updated classification markings.

Classified By: 2282945
Derived From: MET T-06
Reason: 1.4(c)
Declassify On: 20380626

(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

August 2013

TABLE OF CONTENTS

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence

August 2013

Reporting Period: June 1, 2012 – November 30, 2012

(U) EXECUTIVE SUMMARY

(U) The FISA Amendments Act of 2008 (hereinafter "FAA") requires the Attorney General and the Director of National Intelligence to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended, (hereinafter "FISA" or "the Act") and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. This report sets forth the Department of Justice, National Security Division (NSD) and Office of Director of National Intelligence's (ODNI) ninth joint compliance assessment under Section 702, covering the period June 1, 2012, through November 30, 2012 (hereinafter the "reporting period"). This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was submitted as required by Section 707(b)(1) of FISA (hereinafter "the Section 707 Report") on March 11, 2013, and covers the same reporting period.

(U) Compliance assessment activities have been jointly conducted by NSD and ODNI. Specifically, the joint team consisted of members from NSD, ODNI's Civil Liberties and Privacy Office (CLPO), ODNI's Office of General Counsel (OGC), and ODNI's Office of the Deputy Director for Intelligence Integration/Mission Integration Division (DD/II/MID). NSD and ODNI have assessed the oversight process used since Section 702 was implemented in 2008, and have identified improvements in the Intelligence Community personnel's awareness of and compliance with the restrictions imposed by the statute, targeting procedures, minimization procedures and the Attorney General Guidelines.

~~(S//NF)~~ The joint team has found that a vast majority of compliance incidents reported in the Section 707 Reports have been self-identified by the agencies, sometimes as a result of preparation for the joint reviews. In discussing compliance incidents in this Semiannual Assessment (hereinafter also referred to as the Joint Assessment), the focus is on incidents that have the greatest potential to impact United States persons' privacy interests; intra- and interagency communications; the effect of human errors on the conduct of acquisition; and the effect of technical issues on the conduct of acquisition.

(U//~~FOUO~~) This Joint Assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities

and to impose internal controls for compliance and verification purposes. The compliance incidents which occurred during the reporting period represent a very small percentage of the overall collection activity, which has increased from the last Joint Assessment. Individual incidents, however, can have broader implications, as further discussed herein and in the Section 707 Report. Based upon a review of these compliance incidents, the joint team believes that none of these incidents represent an intentional attempt to circumvent or violate the Act, the targeting or minimization procedures, or the Attorney General's Acquisition Guidelines.

(U) SECTION 1: INTRODUCTION

(U) The FISA Amendments Act of 2008, relevant portions of which are codified at 50 U.S.C. §1881 – 1881g (hereinafter "FAA"), requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq*., as amended (hereinafter "FISA" or "the Act"), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter "Section 702") have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI's ninth joint compliance assessment under Section 702, covering the period June 1, 2012, through November 30, 2012 (hereinafter the "reporting period").[1]

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting and minimization procedures, as well as guidelines. A primary purpose of the guidelines is to ensure compliance with the limitations set forth in subsection (b) of Section 702, which are as follows:

> An acquisition authorized under subsection (a)—
>
> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
> (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;
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
> (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

[1] (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on March 11, 2013, as required by Section 707(b)(1) of FISA, and covers the same reporting period.

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

These guidelines, the Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "the Attorney General's Acquisition Guidelines"), were adopted by the Attorney General in consultation with the DNI on August 5, 2008.

~~(TS//SI//NF)~~ During the reporting period, the Attorney General and DNI reauthorized [redacted] Section 702(g) certifications, all of which reauthorized previous certifications. On [redacted] 2012, the FISC approved these reauthorization certifications. [redacted] Each reauthorization certification was submitted with targeting and minimization procedures, which featured modifications from the targeting and minimization procedures used in previous certifications. The Attorney General's Acquisition Guidelines applicable for each certification remained unchanged. On [redacted] 2012, the FISC held that the targeting and minimization procedures met all statutory and Constitutional requirements. These [redacted] certifications, and all associated documents were previously provided to the congressional committees on September 28, 2012, and as attachments to the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of FISA, March 2013, submitted as required by Section 707(b)(1) of FISA (hereinafter the "Section 707 Report") filed on March 11, 2013.

~~(S//NF)~~ Three agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA).[2] An overview of how these agencies implement the authority appears in Appendix A of this assessment.

[2] ~~(S//NF)~~ The other agency involved in implementing Section 702 is the National Counterterrorism Center (NCTC), which has a limited role, as reflected in the recently approved "Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended." Under these limited minimization procedures, NCTC is not authorized to receive unminimized Section 702 data. Rather, these procedures recognize that, in light of NCTC's statutory counterterrorism role and mission, NCTC has been provided access to certain FBI systems containing *minimized* Section 702 information, and prescribe how NCTC is to treat that information. For example, because NCTC is not a law enforcement agency, it may not receive disseminations of Section 702 information that is evidence of a crime, but which has no foreign intelligence value; accordingly, NCTC's minimization procedures require in situations in which NCTC personnel discover purely law enforcement information with no foreign intelligence value in the course of reviewing minimized foreign intelligence information that the NCTC personnel either purge that information (if the information has been ingested into NCTC systems) or not use, retain, or disseminate the information (if the information has been viewed in FBI systems). No incidents of noncompliance with

(U//~~FOUO~~) Section Two of this Joint Assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting and minimization procedures, as well as the Attorney General's Acquisition Guidelines. Section Three compiles and presents data acquired from the joint oversight team's compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the Section 707 Report. As with the prior Joint Assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent recurrences.

(U//~~FOUO~~) In summary, the joint team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period. As in the prior Joint Assessments, the joint team has not found indications in the compliance incidents that have been reported or otherwise identified of any intentional or willful attempts to violate or circumvent the requirements of the Act. The number of compliance incidents remains small, particularly when compared with the total amount of targeting and collection activity. To reduce the number of future compliance incidents, the Government will continue to focus on measures to improve communications, training, and monitoring of collection systems, as well as monitor purge practices and withdrawal of disseminated reports as may be required.[3] Further, the joint oversight team will also monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report.

(U) SECTION 2: OVERSIGHT OF THE IMPLEMENTATION OF SECTION 702

~~(S//NF)~~ The implementation of Section 702 is a multi-agency effort. As described in detail in Appendix A, NSA and FBI each acquire certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, and CIA [redacted] each handle Section 702-acquired data in accordance with their own minimization procedures. There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies from using preexisting systems to implement Section 702

---

the NCTC minimization procedures were identified during this reporting period. The joint oversight team will be assessing NCTC's compliance with its minimization procedures in the next reporting period.

[3] (U//~~FOUO~~) In November 2012, during final review of the prior Assessment, the NSA Office of Inspector General shared with NSD and ODNI the results of its study of NSA's management controls of its Section 702 program. The Office of the Inspector General subsequently revised its study in March 2013. NSD and ODNI are currently reviewing these results and will incorporate any relevant additional information resulting from the review in the next Joint Assessment.

authorities. Because of these differences in practice and procedure, there are corresponding differences in both the internal compliance programs each agency has developed and in the external oversight programs conducted by NSD and ODNI.

(U) A joint team has been assembled to conduct compliance assessment activities, consisting of members from NSD's Office of Intelligence (OI), ODNI's Civil Liberties and Privacy Office (CLPO), ODNI's Office of General Counsel (ODNI OGC), and ODNI's Office of the Deputy Director for Intelligence Integration/Mission Integration Division (ODNI DD/II/MID). The team members play complementary roles in the review process. The following describes the oversight activities of the joint team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this Joint Assessment.

~~(S//NF)~~ I. Joint Oversight of NSA

~~(S//NF)~~ Under the process established by the Attorney General and Director of National Intelligence's certifications, all Section 702 targeting is initiated pursuant to the NSA's targeting procedures. Additionally, NSA is responsible for conducting post-tasking technical checks of all Section 702-tasked communication facilities[4] once collection begins. NSA must also minimize its collection in accordance with its minimization procedures. Each of these responsibilities is detailed in Appendix A. Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities. NSA's internal oversight and compliance mechanisms are further described in Appendix A.

~~(TS//SI//NF)~~ NSD and ODNI's joint oversight of NSA's implementation of Section 702 consists of periodic compliance reviews, which NSA's targeting procedures [redacted] as well as the investigation and reporting of specific compliance incidents. During this reporting period, NSD and ODNI conducted the following onsite reviews at NSA:

Figure 1: ~~(S)~~ NSA Reviews

Date of Review	Applicable Certifications	Taskings/Minimization Reviewed
August 14, 2012	[redacted]	June 1, 2012 – July 31, 2012
October 12, 2012	[redacted]	August 1, 2012 – September 30, 2012
December 11, 2012	[redacted]	October 1, 2012 – November 30, 2012

[4] ~~(S)~~ Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities (also referred to herein as "selectors"), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. A fuller description of the Section 702 targeting process may be found in the Appendix.

Reports for each of these reviews, which document the relevant time period of the review, the number and types of selectors, the types of information that NSA relied upon, and a detailed summary of the findings for that review period, have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

~~(S//NF)~~ The review process for NSA targeting begins well before the onsite review. Prior to each review, NSA electronically sends the tasking record (known as a tasking sheet) for each selector tasked during the review period to NSD and ODNI. Members of the joint oversight team review tasking sheets and then NSD prepares a detailed report of the findings, which they share with the ODNI members of the review team. During this initial review, NSD attorneys determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that, without further review of the cited documentation, did not provide sufficient information, and either sets forth its questions for each selector or requests that NSA provide the cited documentation for review.

~~(S//NF)~~ During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets, together with NSA Signals Intelligence Directorate (SID) Oversight and Compliance personnel, NSA attorneys, and other NSA personnel as required, to ask questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of e-mail and telephonic exchanges to answer questions and clarify issues.

~~(S//NF)~~ The joint oversight team also reviews NSA's minimization of Section 702-acquired data. The team reviews a large sample of the serialized reports that NSA has disseminated and identified as containing Section 702-acquired United States person information. NSD and ODNI also review a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English. In addition to the dissemination review, NSD and ODNI also review NSA's querying of unminimized Section 702-acquired communications using United States person identifiers.

~~(S//NF)~~ The joint oversight team also investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be compliance incidents (e.g., NSA must report any instance in which a targeted individual is found to be located in the United States, a circumstance which is only a compliance incident if NSA knew or should have known the target was in the United States during the collection period), but the report of which may lead to the discovery of an underlying compliance incident. Investigations of all of these incidents often result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report, and to the FISC through quarterly reports or individualized notices.

~~(S//NF)~~ II. Joint Oversight of CIA

~~(S//NF)~~ As further described in detail in Appendix A, although CIA does not directly engage in targeting, it does nominate potential Section 702 targets to NSA. [redacted] the joint oversight review team conducts onsite visits at CIA [redacted] the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. [redacted]

~~(S//NF)~~ NSD and ODNI also conduct periodic compliance reviews of CIA's application of its minimization procedures approximately once every two months. For this reporting period, NSD and ODNI conducted the following onsite reviews at CIA:

Figure 2: ~~(S//NF)~~ CIA Reviews

Date of Visit	Minimization Reviewed
August 22, 2012	June 1, 2012 – July 31, 2012
October 24, 2012	August 1, 2012 – September 30, 2012
December 19, 2012	October 1, 2012 – November 31, 2012

Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

~~(S//NF)~~ As a part of the onsite reviews, the joint oversight team examines documents related to CIA's retention, dissemination, and querying of Section 702-acquired data. The team reviews a sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with the analyst issues involving the proper application of the minimization procedures. The team also reviews all disseminations of information acquired under Section 702 that CIA identified as potentially containing United States person information. NSD and ODNI also review CIA's written justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.

~~(S//NF)~~ In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with the CIA minimization procedures and/or the Attorney General Acquisition Guidelines. [redacted] Investigations are coordinated through the CIA FISA Program

Office and CIA OGC, and when necessary, may involve requests for further information, meetings with CIA legal, analytical, and/or technical personnel, or the review of source documentation. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report, and to the FISC through quarterly reports or individualized notices.

~~(S//NF)~~ III. Joint Oversight of FBI

~~(S//NF)~~ FBI fulfills three separate roles in the implementation of Section 702. First, FBI is authorized under the certifications to acquire foreign intelligence [redacted] for such acquisition (hereinafter "Designated Accounts"). The acquisitions of communications must be conducted pursuant to FBI's targeting procedures. Second, [redacted] – for processing in accordance with the [redacted] FISC-approved minimization procedures. Similarly, FBI also provides [redacted] Third, FBI may receive [redacted] unminimized Section 702 acquired communications. Such communications must be minimized pursuant to FBI's Section 702 minimization procedures. [redacted] FBI's internal compliance program and NSD and ODNI's oversight program are designed to ensure FBI's compliance with statutory and procedural requirements for each of these three roles. Each of the roles discussed above, as well as the FBI's internal compliance program, are set forth in further detail in Appendix A.

(S//NF) FBI's targeting procedures require that [redacted] Because the review of FBI's targeting is a manual process, NSD and ODNI generally conduct monthly reviews. For this reporting period, onsite reviews were conducted on the following dates:

[redacted]

Figure 3: ~~(S)~~ FBI Reviews

Date of Visit	Applicable Certifications	Tasking and Minimization Reviewed
August 23, 2012	[redacted]	June 2012 taskings
September 27, 2012		July 2012 taskings; June 2012 – July 2012 minimization
October 25, 2012	[redacted]	August 2012 taskings
November 27, 2012		September 2012 taskings; August 2012 – September 2012 minimization
January 10, 2013	[redacted]	October 2012 taskings
January 23, 2013		November 2012 taskings; October 2012 – November 2012 minimization

Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

~~(S//NF)~~ In conducting the targeting review, the joint oversight team reviews the targeting checklist completed by the FBI analysts and supervisory personnel involved in the process, together with [redacted] supporting documentation. The joint oversight team reviews every file identified by FBI for which [redacted] The joint oversight team also reviews a sample of [redacted] files to identify any other potential compliance issues. FBI analysts and supervisory personnel are available to answer questions, and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

~~(S//NF)~~ With respect to minimization, the joint oversight team reviews [redacted] documents related to FBI's application of its minimization procedures. The team reviews a sample of communications that FBI [redacted] The team also reviews all disseminations of information acquired under Section 702 that FBI [redacted] In addition, during [redacted] reviews at FBI field offices, NSD looks at FBI's use of [redacted], including Section 702-acquired data.

~~(S//NF)~~ The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting and minimization procedures, the Attorney General's Acquisition Guidelines, or other agencies' procedures in which FBI is involved. These investigations are coordinated with FBI OGC and may involve requests for further information, meetings with FBI legal, analytical, and/or technical personnel, or review of source documentation. All compliance incidents identified

[6] ~~(S//NF)~~ Subsequent to the reporting period for this assessment, NSD expanded it minimization reviews in FBI review offices to also examine retention and dissemination decisions made by FBI field office personnel. A full description of these new oversight reviews and the results of such reviews will be included in the next Joint Assessment.

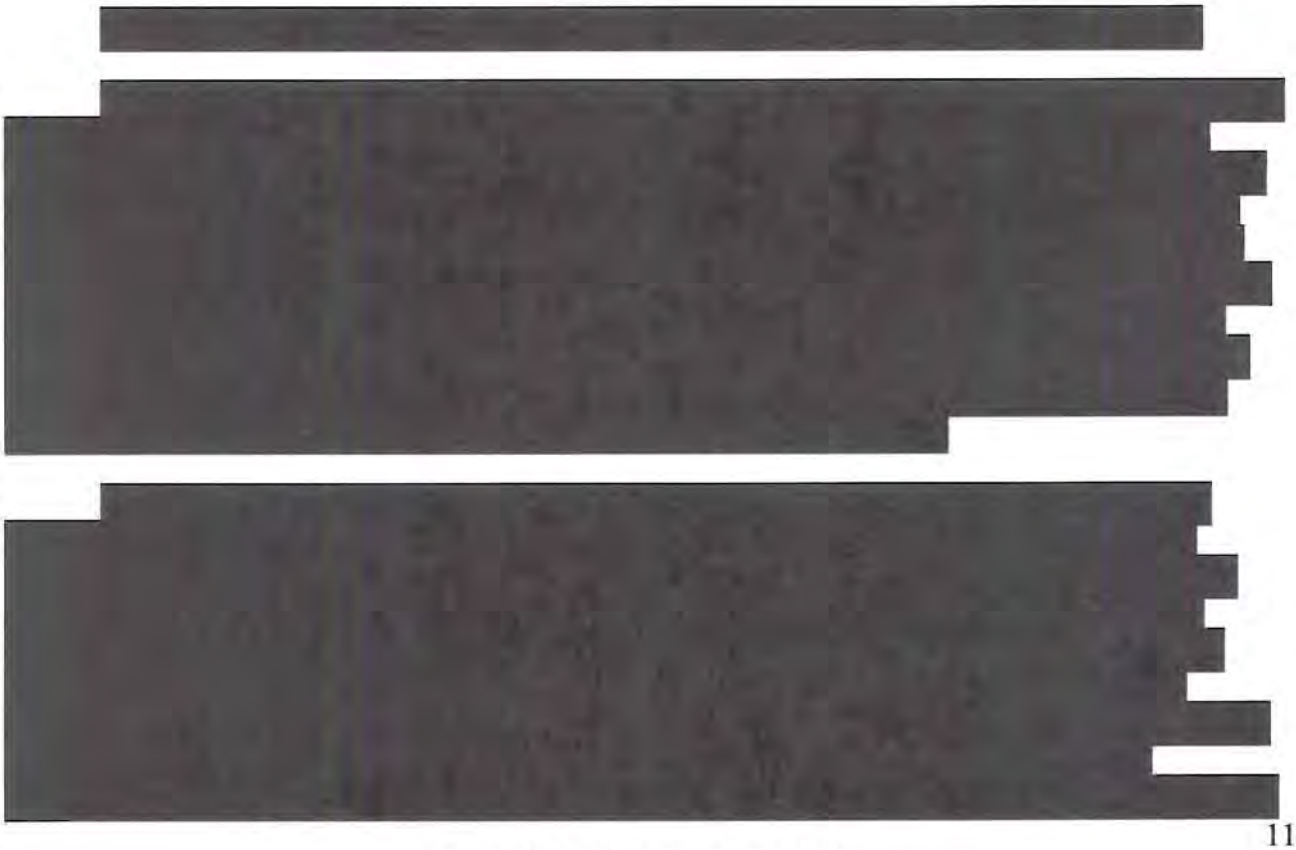
by these investigations are reported to the congressional committees in the Section 707 Report, and to the FISC through quarterly reports or individualized notices.

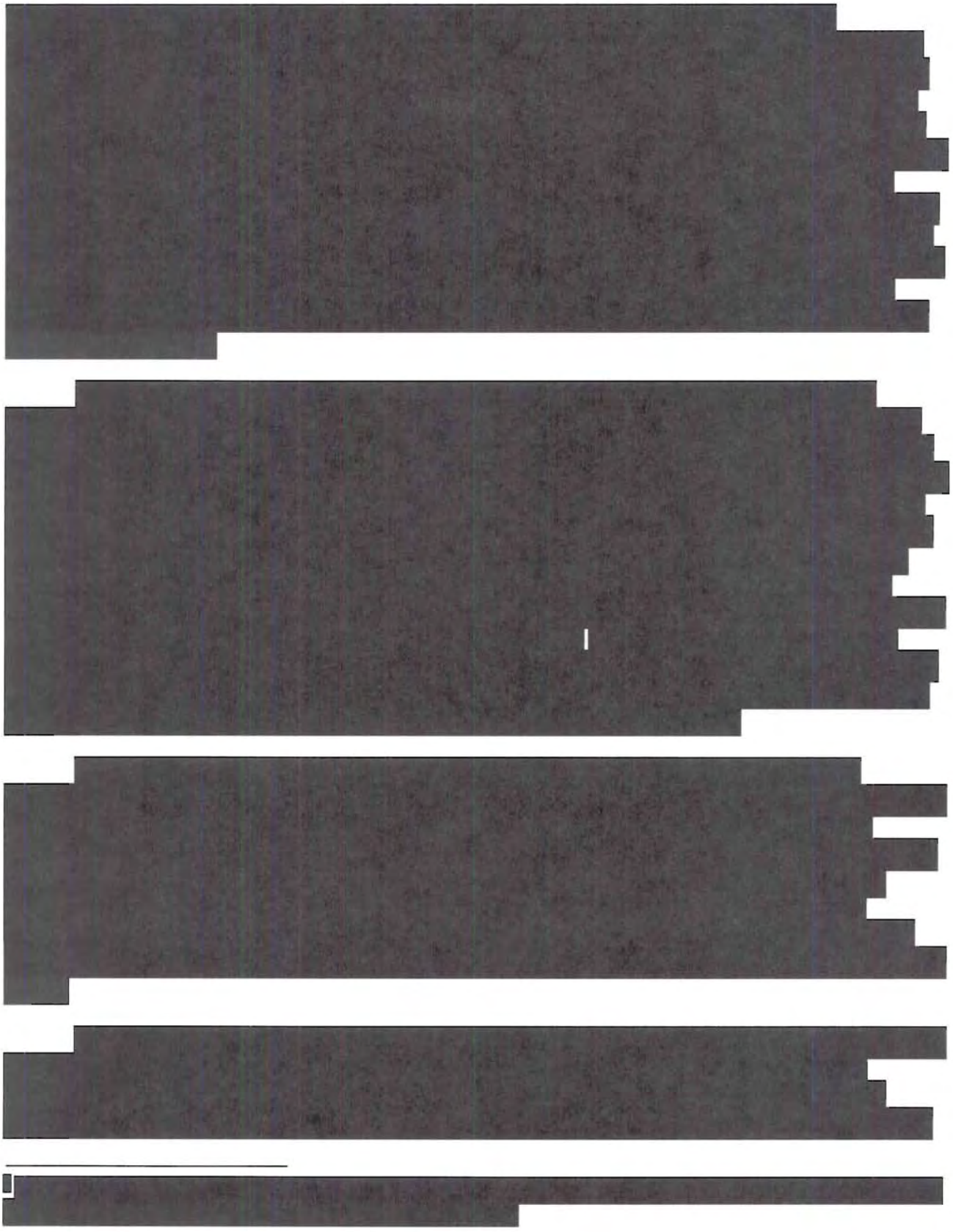
~~(S//NF)~~ IV. Interagency/Programmatic Oversight

~~(S//NF)~~ Because the implementation and oversight of the Government's Section 702 authorities is a multi-agency effort, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence, and comply with all legal requirements. For these reasons, NSD and ODNI conduct bimonthly meetings with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures.

~~(S//NF)~~ NSD and ODNI's programmatic oversight also involves efforts to proactively minimize the number of incidents of noncompliance. For example, NSD and ODNI have required agencies to demonstrate to the joint oversight team new or substantially revised systems involved in Section 702 targeting or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review, and where appropriate seek modifications of, their targeting and minimization procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance.

(U) V. Other Compliance Efforts





[redacted]

~~(TS//SI//NF)~~ B. Query Processes Using United States Person Identifiers

~~(TS//SI//NF)~~ As reported in the last semiannual assessment, NSA minimization procedures now permit NSA to query its databases containing telephony and non-upstream electronic communications using United States person identifiers in a manner designed to find foreign intelligence information. Similarly, CIA's minimization procedures have been modified to make explicit that CIA may also query its databases using United States person identifiers to yield foreign intelligence information.[8] As discussed above in the descriptions of the joint oversight team's efforts at each agency, the joint oversight team conducts reviews of each agency's use of its ability to query using United States person identifiers. To date, this review has not identified any incidents of noncompliance with respect to the use of United States person identifiers; as discussed in Section 4, the agencies' internal oversight programs have, however, identified isolated instances in which Section 702 queries were inadvertently conducted using United States person identifiers.

[redacted]

(U) D. Training

~~(S//NF)~~ In addition to specific instructions to personnel directly involved in the incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have also been engaged in broader training efforts to ensure compliance with the targeting and minimization procedures. NSA is currently updating its compliance training course and consolidating its online training materials. CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. CIA has also revised its initial training for its other personnel to better explain how to apply the legal standards to real world situations. FBI, in conjunction with its broader roll-out of its formal Section 702 nomination program, has substantially expanded its training program during this reporting period. After consultation with NSD and ODNI, FBI implemented an online training program regarding nominations and the

[8] ~~(S//NF)~~ FBI's minimization procedures had already provided that agency the ability to use [redacted] In the course of its FBI field office reviews over the last several years, NSD has audited FBI's [redacted]

[redacted]

requirements of the [redacted]; FBI already had an online training regarding compliance with its Section 702 minimization procedures. NSD and FBI have also conducted numerous in-person trainings at FBI field offices.

(U//~~FOUO~~) SECTION 3: TRENDS IN SECTION 702 TARGETING AND MINIMIZATION

~~(S//NF)~~ In conducting the above-described oversight program, NSD, ODNI, and the agencies have collected a substantial amount of data regarding the implementation of Section 702. In this section, a comprehensive collection of this data has been compiled in order to identify overall trends in the agencies targeting, minimization, and compliance.

~~(S//NF)~~ I. Trends in NSA Targeting and Minimization

~~(TS//SI//NF)~~ NSA reports that, on average, approximately [redacted] selectors were under collection pursuant to Certifications [redacted] on any given day during the reporting period. This represents an [redacted] increase from the approximately [redacted] selectors under collection on any given day in the last reporting period. This [redacted] increase is comparable to the rate of increase in the prior reporting periods, which were [redacted] and [redacted] respectively. As Figure 4 demonstrates, with one exception, the average number of selectors under collection has increased every reporting period.

[redacted]

[redacted]

~~(TS//SI//NF)~~ It is anticipated that the average number of tasked selectors will continue to

increase. The rate of increase may accelerate now that FBI has made its nomination process more widely available to its field office personnel.

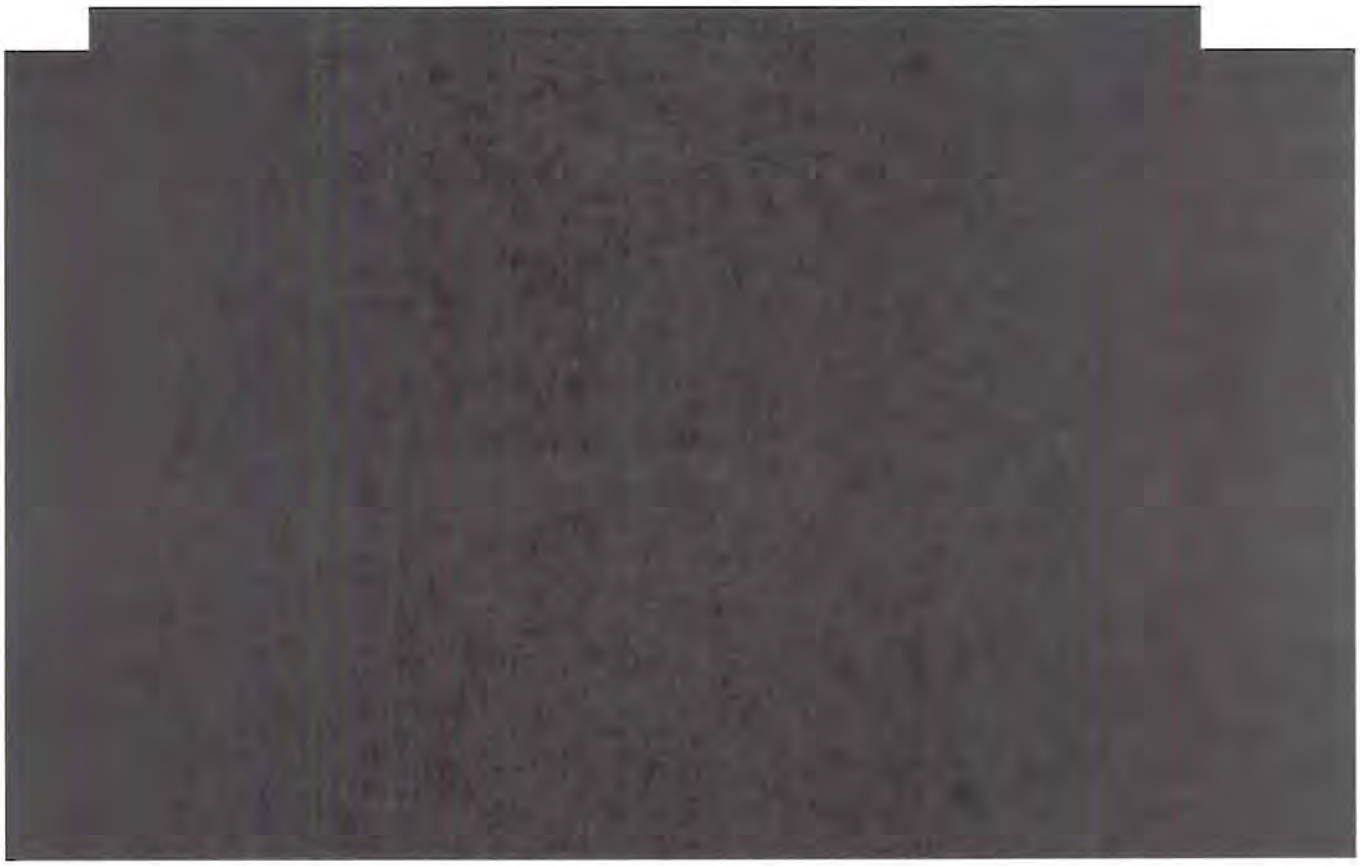
[redacted]

~~(TS//SI//NF)~~ The above statistics describe the average number of selectors under collection at any given time during the reporting period. The total number of newly tasked selectors during the reporting period provides another useful metric.[10] NSA provided documentation of [redacted] new taskings during the reporting period. This represents a [redacted] increase in new taskings from the previous reporting period. Additionally, [redacted] new taskings in the current reporting period were telephone numbers; the remaining [redacted] of the newly-tasked selectors were electronic communications accounts.

~~(TS//SI//NF)~~ Figure 5 charts the total monthly numbers of newly tasked facilities since collection pursuant to Section 702 began in September 2008.[11]

[10] ~~(S//NF)~~ The term newly tasked selectors refers to any selector that was added to collection under a certification. This term includes any selector added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked selectors are therefore selectors that had been previously tasked for collection, were detasked, and now have been retasked.

[11] ~~(S//NF)~~ For 2008 and 2009, the chart includes taskings under the last Protect America Act of 2007 (PAA) certification, Certification 08-01, which was not replaced by a Section 702(g) certification until early April 2009.



As the chart demonstrates, the number of newly tasked telephone numbers decreased after 2009, but began to increase again in 2012. The average number of telephone numbers tasked each month for the first 11 months of 2012 [redacted] As has been the case since the program was initiated, the average number of electronic communication accounts has continued to increase. The average number of electronic communications accounts tasked each month for the first 11 months of 2012 was [redacted] increase from the prior year.

~~(TS//SI//NF)~~ With respect to minimization, for this reporting period NSA identified to NSD and ODNI [redacted] serialized reports based upon minimized Section 702- or Protect America Act (PAA)-acquired data. This represents a [redacted] increase from the [redacted] such serialized reports NSA identified in the prior reporting period. As demonstrated by Figure 6, which reflects NSA reporting since late 2009, this increase represents a continuation of the overall increase in the number of reports based on Section 702- and PAA-acquired data since collection pursuant to these authorities began.

~~(TS//SI//NF)~~ During this reporting period, NSA identified serialized reports as containing United States person information derived from Section 702- or PAA-acquired data. NSD and ODNI's review revealed that in the vast majority of circumstances, the United States person information was at least initially masked.[12] The percentage of reports containing United States person information has remained low at for this reporting period, decreasing at a marginal rate of from the prior reporting period. Additionally, for the past three reporting periods the number of serialized reports issued by NSA without United States person information has grown at a far greater rate than the number of serialized reports issued containing United States person information.

~~(S//NF)~~ II. Trends in FBI Targeting and Minimization

~~(TS//SI//NF)~~ FBI reports that accounts for acquisition during the reporting period – an average of accounts designated per month. This is a increase from the accounts designated in the prior six-month reporting period. Of the electronic communications accounts for which Section 702 collection

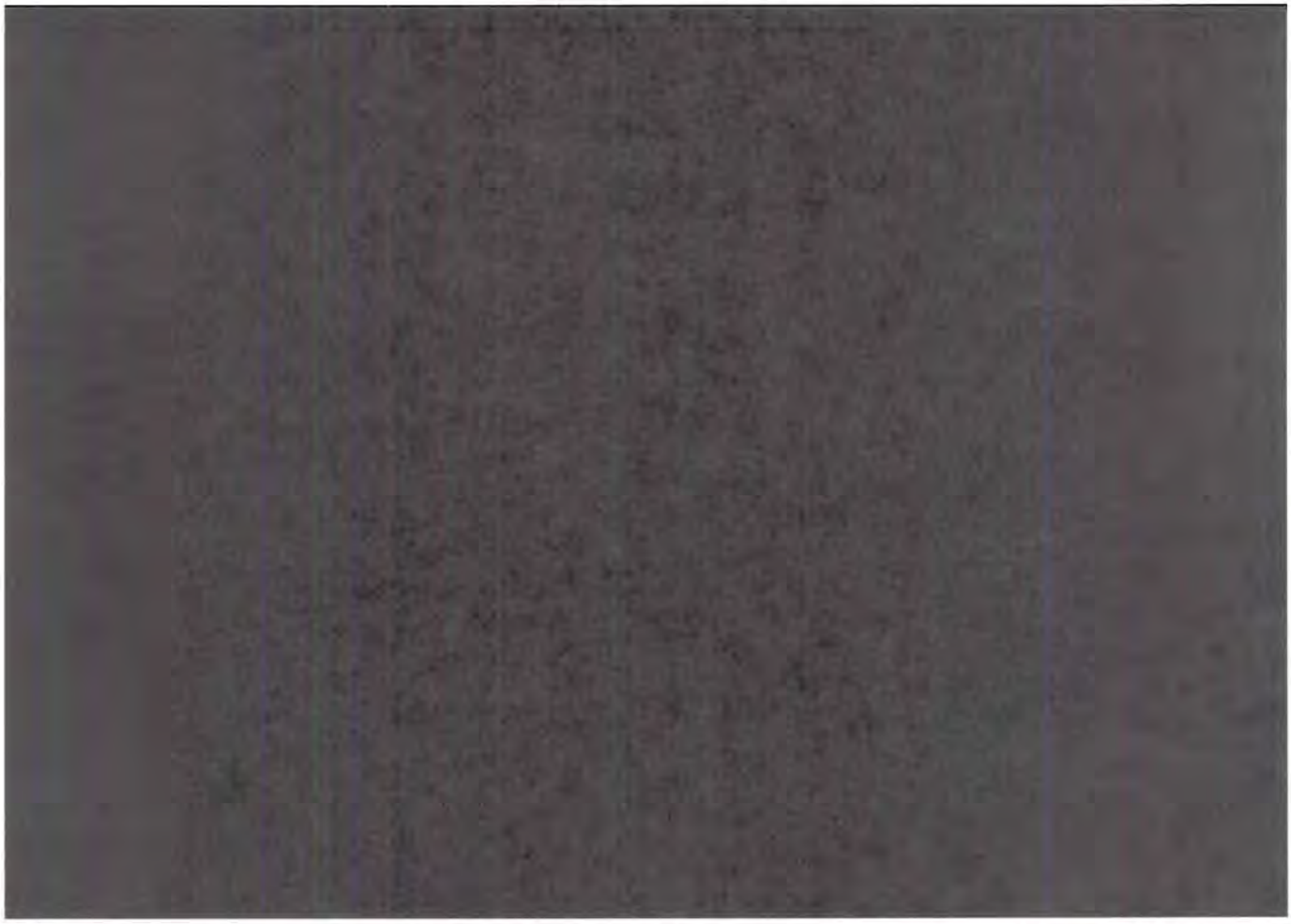
[12] ~~(S)~~ NSA generally "masks" United States person information by replacing the name or other identifying information of the United States person with a generic term, such as "United States person #1." Agencies may request that NSA "unmask" the United States person identity. Prior to such unmasking, NSA must determine that the United States person's identity is necessary to understand the foreign intelligence information.

during the reporting period, approximately [redacted] acquisitions. The prior Joint Assessment reported that [redacted]

~~(TS//SI//NF)~~ FBI approved [redacted] requests [redacted] during the reporting period. [redacted]

[redacted]

[13] ~~(S//NF)~~ Although FBI acquired [redacted] pursuant to Section 702 prior to April 2009, statistics are provided from April 2009 forward as NSD's practices for tracking selectors designated and approved changed as of this date. The "2009 Average" reflected in the table therefore reflects only the average number of accounts from April through December 2009.



~~(S//NF)~~ Figure 7 shows that the percentage of designated accounts approved for acquisition has been consistently high. FBI may not approve the acquisition [redacted] from a designated account for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the account are non-United States persons located outside the United States. Historically, the joint review team notes that for those accounts not approved by FBI [redacted], only a small portion were rejected on the basis that they were ineligible for Section 702 collection.

~~(S//NF)~~ In October 2009, FBI began to retain Section 702-acquired data in its systems. FBI identifies for the joint oversight team all disseminations of Section 702 data containing United States person information. Figure 8 below compiles the number of disseminated reports containing United States person information identified for these reviews for the last six review periods.

~~(TS//SI//NF)~~ A total of [redacted] reports that were based at least in part on Section 702-acquired United States person information were disseminated during this reporting period. This represents an [redacted] increase from the previous reporting period. During this reporting period, the Department of Justice Office of Inspector General issued a report in which it described certain disseminations of metadata made by the FBI. NSD and ODNI assess that some of these disseminations likely included disseminations of United States person information which were not previously identified to NSD and ODNI, and thus are not included in the above Figure. An update regarding this issue will be provided in the next Joint Assessment.

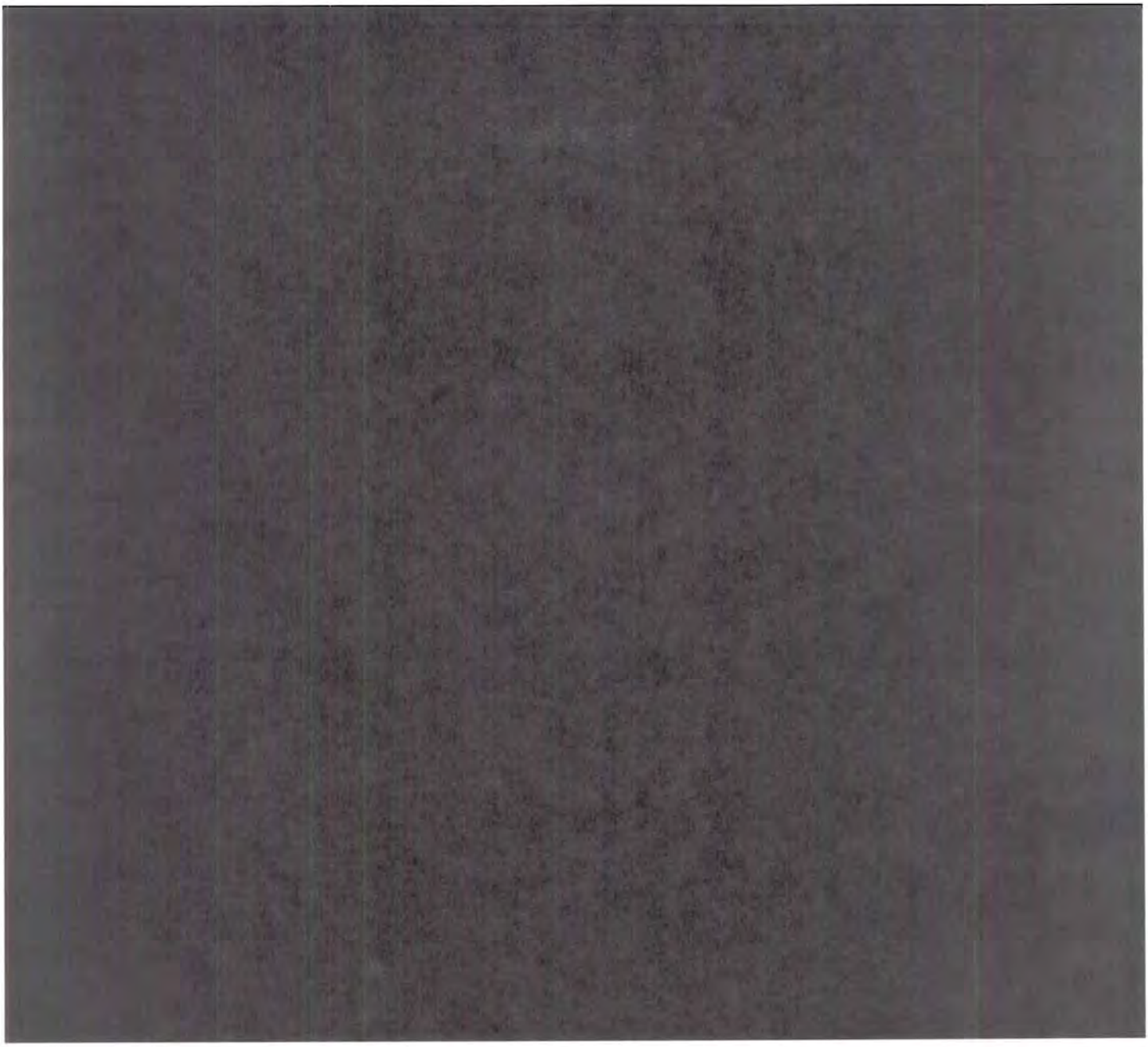
~~(S//NF)~~ III. Trends in CIA Minimization

~~(S//NF)~~ Like FBI, CIA only identifies for NSD and ODNI disseminations of Section 702 data containing United States person information. [redacted]

[redacted]

~~(S//NF)~~ During this reporting period, CIA identified [redacted] disseminations of Section 702-acquired data containing minimized United States person information. This is a [redacted] decrease from the [redacted] such disseminations CIA made in the prior reporting period. [redacted]

[redacted]



(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U//~~FOUO~~) The joint oversight team finds that during the reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to

implement these authorities and to impose internal controls for compliance and verification purposes.

~~(U//FOUO)~~ The compliance incidents during the reporting period represent a very small percentage of the overall collection activity. Based upon a review of the reported compliance incidents, the joint team does not believe that these incidents represent an intentional attempt to circumvent or violate the procedures required by the Act.

~~(S//NF)~~ As noted in prior reports, in the cooperative environment the implementing agencies have established, an action by one agency can result in an incident of noncompliance with another agency's procedures. It is also important to note that a single incident can have broader implications.

~~(U//FOUO)~~ The compliance incidents for the reporting period are described in detail in the Section 707 Report, and are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures.

(U) I. Compliance Incidents – General

(U) A. Compliance Incident Rate

~~(S//NF)~~ As noted in the Section 707 Report, there were a total of [redacted] compliance incidents that involved noncompliance with the NSA targeting or minimization procedures; [redacted] involving noncompliance with the CIA minimization procedures; and [redacted] involving noncompliance with FBI targeting and minimization procedures; for a total of [redacted] incidents involving NSA, CIA or FBI procedures.[14] Additionally, there were [redacted] incidents of noncompliance by electronic communication service providers issued a directive pursuant to Section 702(h) of FISA.

~~(TS//SI//NF)~~ The following tables put these compliance incidents in the context of the average number of selectors subject to acquisition on any given day during the reporting period:

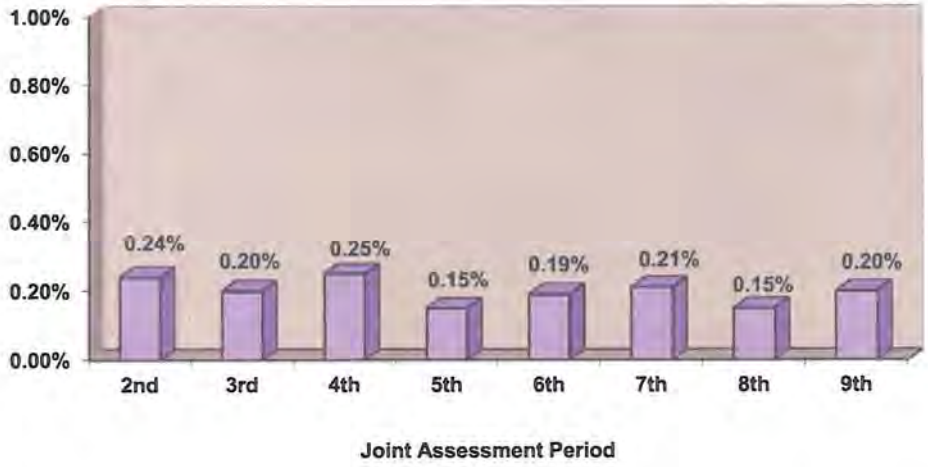
Compliance incidents during reporting period (June 1, 2012 – November 30, 2012) (including provider incidents)	[redacted]
Number of selectors on average subject to acquisition during the reporting period	[redacted]
Compliance incident rate as percentage of average selectors subject to acquisition	0.49%

[14] ~~(S//NF)~~ As is discussed in the Section 707 report and herein, some compliance incidents involve more than one element of the Intelligence Community. Incidents have therefore been grouped not by the agency "at fault," but instead by the set of procedures with which actions have been noncompliant.

~~(TS//SI//NF)~~ The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of [redacted] represents an increase from the [redacted] compliance incident rate in the prior reporting period.

~~(TS//SI//NF)~~ In [redacted] of the [redacted] incidents in this reporting period, however, the only incident of noncompliance was the failure to notify NSD and ODNI of certain facts within the timeframe provided in the NSA targeting procedures.[15] The median length of these reporting delays is one business day. The oversight team will continue to work with NSA to ensure that notifications are made to NSD and ODNI within the time frame specified in the relevant procedures. A better measure of substantive compliance with the applicable targeting and minimization procedures, therefore, is to compare the compliance incident rate excluding these notification delays. The following Figure shows this adjusted rate:

Figure 11: (U//~~FOUO~~) Compliance Incident Rate (as percentage of average selectors tasked), Not including Notification Delays



As Figure 11 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.20%, which is consistent with low compliance incident rates seen in prior reporting periods.

---

[15] ~~(S//NF)~~ Specifically, NSA's targeting procedures require:

[redacted]

NSA Targeting Procedures at [redacted]

(U) B. Categories of Compliance Incidents

~~(S//NF)~~ Most of the compliance incidents occurring during the reporting period involved non-compliance with the NSA's targeting or minimization procedures. This largely reflects the centrality of these sets of targeting and minimization procedures in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting or minimization procedures have generally fallen into the following categories:

- ~~(S//NF)~~ *Tasking Issues.* This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the selector.

- ~~(S//NF)~~ *Detasking Issues.* This category involves incidents in which the selector was properly tasked in accordance with the targeting procedures, but errors in the detasking of the selector caused noncompliance with the targeting procedures.

- ~~(S//NF)~~ *Notification Delays.* The category involves incidents in which a selector was properly tasked in accordance with the targeting procedures, but a notification requirement contained in the targeting procedures was not satisfied.

- ~~(S//NF)~~ *Documentation Issues.* This category involves incidents where the determination to target a selector was not properly documented as required by the targeting procedures.[16]

- ~~(S//NF)~~ *Overcollection.* This category involves incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked selectors, also acquired data regarding untasked selectors, resulting in "overcollection."

- ~~(S//NF)~~ *Minimization Issues.* The sixth category involves NSA's compliance with its minimization procedures.

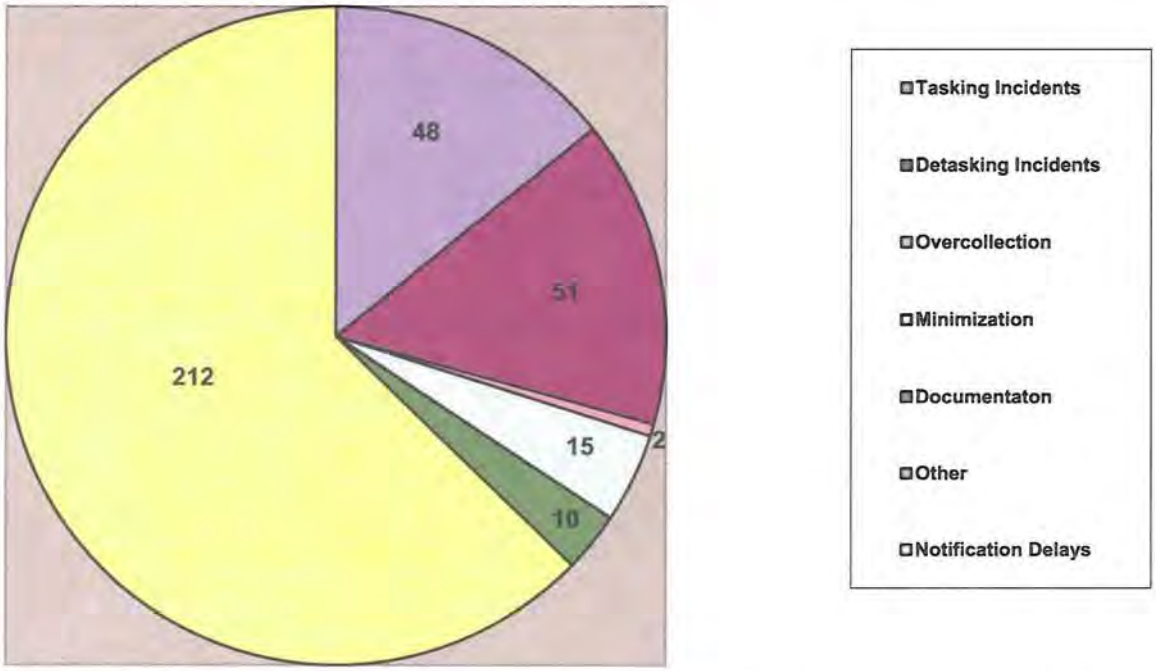
In some instances, an incident may involve more than one category of noncompliance.

~~(TS//SI//NF)~~ These categories are helpful for purposes of reporting and understanding the compliance incidents. The following chart depicts the numbers of compliance incidents in each category that occurred during this reporting period.

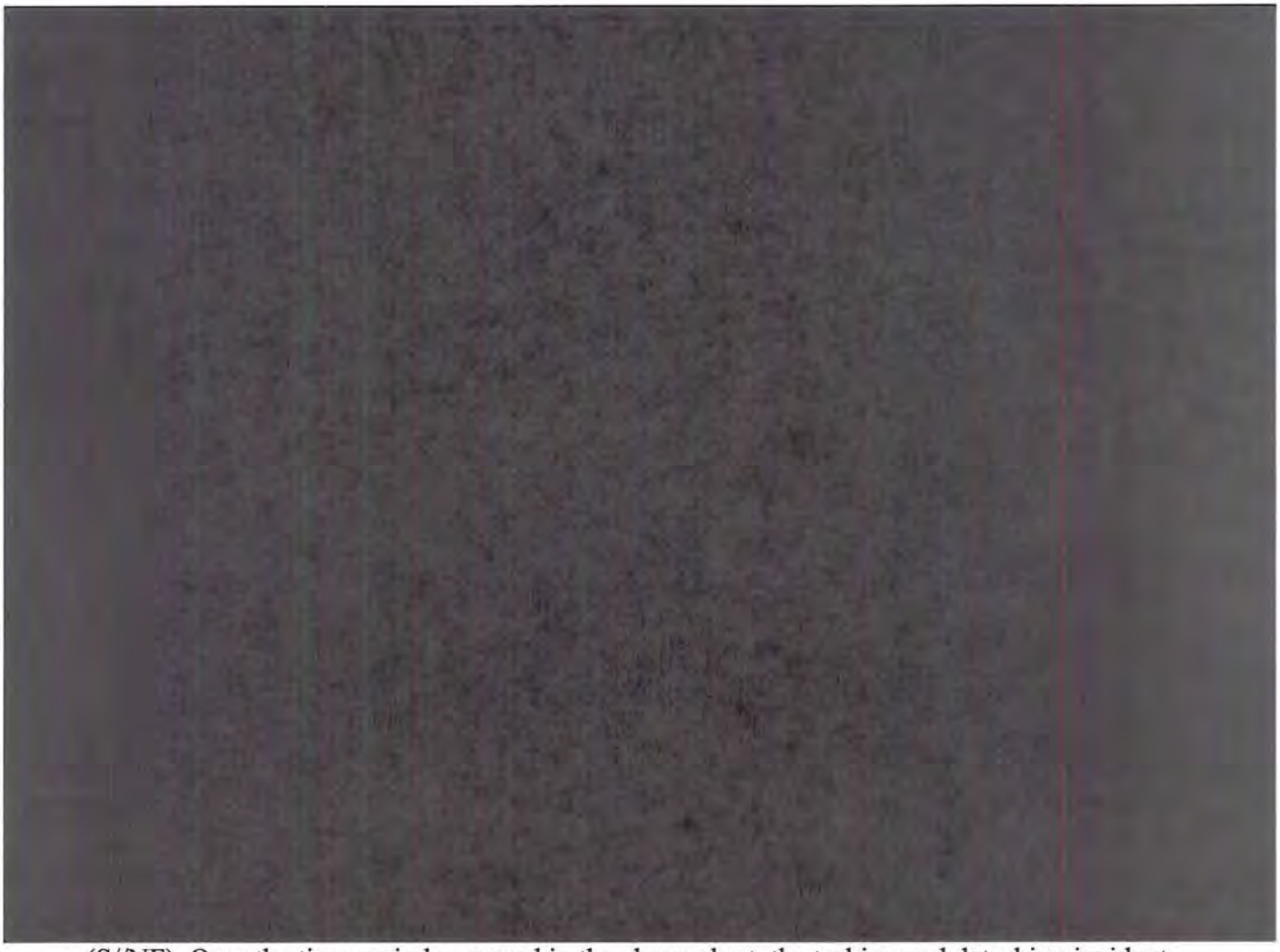
[16] ~~(S//NF)~~ As described in the Section 707 Report, not all documentation errors have been separately enumerated as compliance incidents.

[redacted]

June 1, 2012 - November 30, 2012



~~(S//NF)~~ As Figure 12 demonstrates, the vast majority of compliance incidents during the reporting period were notification delays. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a selector used by a United States person or an individual located in the United States. The following chart depicts the compliance incident rates, as compared to the average selectors on task, for tasking and detasking incidents over the previous reporting periods.



~~(S//NF)~~ Over the time periods covered in the above chart, the tasking and detasking incident compliance rate has varied by only fractions of a percentage point as compared to the average size of the collection. While tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account, detasking errors more often involve a selector used by a United States person or an individual located in the United States, who may or may not have been the intended target.[17] The percentage of compliance incidents involving such detasking incidents has remained consistently low.

~~(S//NF)~~ With respect to the other targeting and minimization procedures, [redacted] incidents of noncompliance with the FBI's procedures involved noncompliance with FBI's targeting procedures. As discussed below, each of these [redacted] targeting errors resulted from unintentional errors in the targeting process; [redacted] targeting errors involved a facility used by an individual located in the United States. These [redacted] FBI targeting incidents occurred in the course

[redacted]

of approving approximately [redacted] facilities for [redacted], and thus represented [redacted] of the total number of facilities tasked under FBI's targeting procedures during this reporting period. As discussed above, there were [redacted] incidents of noncompliance with CIA's minimization procedures. [redacted]

~~(S//NF)~~ II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures

~~(S//NF)~~ The Section 707 Report previously provided to Congress and the Court discussed in detail every incident of non-compliance that occurred during the reporting period. This Joint Assessment takes the broader approach and reports on the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The Assessment primarily focuses on incidents involving NSA's targeting and minimization procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA's targeting and minimization procedures. The first subsection examines compliance incidents that have the greatest potential to impact United States persons' privacy interests, a particular focus of the joint oversight team. Subsequent subsections discuss incidents caused by intra- and interagency communications (i.e., the ability of the agencies to communicate information between and among themselves in a timely manner to avoid compliance incidents), technical and system errors, incidents caused by human errors, and incidents involving the previously discussed [redacted]

(U) A. The Impact of Compliance Incidents on United States Persons

~~(S//NF)~~ A primary concern of the joint assessment team is the impact of certain compliance incidents on United States persons. The Section 707 Report discusses every incident of noncompliance with the targeting and minimization procedures. Most of these incidents did not involve United States persons, and instead involved matters such as typographical errors in tasking that resulted in no collection, detasking delays with respect to facilities used by non-United States persons who had entered the United States, or notification errors regarding similar detaskings that were not delayed.

~~(S//NF)~~ Several incidents, however, did involve United States persons during the recent reporting period. United States persons were primarily impacted by (1) tasking errors that led to the tasking of facilities used by United States persons, (2) delays in detasking facilities after NSA determined that the user of the selector was a United States person, and (3) the unintentional querying of Section 702 repositories using a United States person identifier. Due to their importance, these incidents are highlighted in this subsection.

~~(S//NF)~~ [redacted] of the tasking incidents described in the Section 707 report involved facilities where at the time of tasking the Government knew or should have known that one of the users of the selector was a United States person. For example, in NSA Incidents [redacted] and [redacted]

[redacted] In a separate incident, NSA Incident [redacted], NSA was informed by the Department of Homeland Security (DHS) that the target of a pending Section 702 tasking request was an LPR, but due to a lack of internal communication, NSA did not prevent the pending tasking request from being effectuated. In each of these incidents, all Section 702-acquired data was purged. Together, these [redacted] incidents represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occurred during the reporting period.

[redacted]

~~(TS//SI//NF)~~ The majority of detasking incidents involved non-United States persons who traveled to the United States. Only one of the [redacted] detasking delays that occurred during this reporting period, NSA Incident [redacted], is confirmed to have involved a United States person. In this incident, NSA determined that a targeted individual located outside the United States and previously assessed by NSA to be a non-United States person whom NSA had targeted pursuant to Section 702 and Executive Order 12333 was in fact a United States person. Based upon the revised assessment, NSA immediately detasked several selectors used by this individual, but due to a miscommunication within an NSA targeting office, did not detask one of this individual's telephone numbers that was tasked to Section 702 collection. The error was discovered three weeks later and the telephone number was detasked. No data was acquired as a result of this detasking delay. As is discussed in Subsection II.C below, NSD and ODNI assess that better records and additional detasking procedures could help prevent detasking delays such as this one.

~~(TS//SI//NF)~~ Several other detasking incidents reported in the Section 707 Report *may* also have involved United States person users of Section 702-tasked selectors, but this has not been confirmed. (b) (1) (A)

[redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted] incidents of non-compliance with the NSA's procedures during this reporting period involved the querying of Section 702 repositories using United States person identifiers [redacted] In its October 3, 2011, and November 30, 2011, orders regarding Certifications [redacted] the FISC approved modifications to NSA's minimization procedures that permitted NSA to query telephony and non-upstream acquired electronic communications Section 702 data using United States person identifiers. Such queries must be designed to yield foreign intelligence information and the query terms themselves are required to be approved pursuant to NSA internal procedures. In each of the [redacted] incidents, an NSA analyst either conducted a query without realizing that NSA had previously determined that the query term was an identifier of a United States person, or the NSA analyst conducted a federated query using a known United States person identifier, but forgot to filter out Section 702-acquired data while conducting the federated query.[19] None of the [redacted] incidents involved an intentional use of an unapproved United States person query term, nor did any of the incidents involve analysts being unaware that only approved United States person identifiers may be used to query Section 702-acquired data. As required by NSA's amended minimization procedures, the joint oversight team continues to conduct oversight of NSA's use of United States person identifiers in queries.

~~(S//NF)~~ B. Intra- and Interagency Communications

~~(S//NF)~~ As noted in the prior report, communications between and among the agencies have continued to improve, which enhances compliance. While communications issues continue to arise in the context of compliance incidents, the joint team assesses that these issues accounted for only a handful of compliance incidents during this reporting period.

~~(S//NF)~~ For example, as previously discussed, NSA Incident [redacted] involved internal communications issues at NSA, which contributed to the erroneous tasking of a selector used by an LPR. Similarly, NSA Incidents [redacted] involved internal miscommunications within NSA that resulted in delays in detasking all known selectors of a target. [redacted]

[19] ~~(TS//NF)~~ A federated query is a query using the same term or terms in multiple NSA databases.

[redacted]

~~(S//NF)~~ The joint oversight team has found that the agencies have established internal and external procedures to communicate information concerning a Section 702 user's travel to the United States or a change in the assessment of their citizenship status. The joint oversight team believes that agencies should continue their training efforts to ensure that these established protocols continue to be utilized. The joint oversight team will continue to work with NSA, CIA and FBI to ensure that the agencies develop and improve efficient and effective channels of communication.

~~(S//NF)~~ C. Effect of Technical Issues on Conduct of Acquisition

~~(S)~~ There were few compliance incidents resulting from technical issues during this reporting period, but technical issues can have larger implications than other incidents because they often involve more than one selector. As such, all agencies involved in the Section 702 program devote substantial resources towards the prevention, identification, and remedy of technical issues. Collection equipment and other related systems undergo substantial testing prior to deployment. The agencies also employ a variety of monitoring programs to detect anomalies in order prevent or limit the effect of technical issues on acquisition. Members of the joint oversight team participate in technical briefings at the various agencies to better understand how technical system development and modifications affect the collection and processing of information. As a result of these briefings, potential issues have been identified, the resolution of which prevented compliance incidents from happening and ensured the continued flow of foreign intelligence information to the agencies.

~~(TS//SI//NF)~~ Nonetheless, changes in the global electronic communications environment, unforeseen consequences of software modifications, and system design issues resulted in incidents that affected acquisition during the reporting period. For example, [redacted] of the compliance incidents during this reporting period resulted in NSA's systems overcollecting data beyond what was authorized under the Section 702 certifications. [redacted] NSA first identified this issue on [redacted], while conducting a regular review of its collection of overseas communications acquired pursuant to Executive Order 12333 and quickly realized that the same collection component had been utilized in its Section 702 collection since [redacted].

(b) (1) (A)

NSA developed, tested, and in (b) (1) (A) deployed a software fix to prevent further overcollection. (b) (1) (A)

(b) (1) (A)

~~(S//NF)~~ Two system errors during this reporting period resulted in delays in detasking facilities. In NSA Incident , an adjustment made in NSA's system during the transition between certifications resulted in detasking delays to facilities, of which resulted in the continued targeting of users located in the United States for up to three days.

~~(S//NF)~~ All of the technical issues discussed in this subsection were discovered by agency personnel and each demonstrates the importance of agencies continually monitoring their collection for abnormalities, particularly following configuration and other software changes made to collection and other related systems. The compliance incidents discussed in this subsection also highlight the complexity of the technical systems used to conduct Section 702 acquisition, as well as the rapid pace of change in communications architecture, that can result in technical and system-related incidents. The joint oversight team assesses that agencies' regular monitoring of relevant systems processing Section 702-acquired information has led to fewer technical tasking and detasking errors and the quicker identification and resolution of system errors that do occur.

~~(S//NF)~~ C. Effect of Human Errors on the Conduct of Acquisition

~~(S//NF)~~ As reported in previous Joint Assessments, human errors often cause many of the compliance incidents. Some of these errors are isolated events that do not lend themselves to categorization or development of standard processes.[21] Other errors, however, do present patterns that could be addressed with new training or procedures. As was in the case in the last several reporting periods, one of the most common errors in this reporting period involved situations where a target who used multiple selectors tasked to Section 702 or Executive Order 12333 collection was discovered to be in, or known to be traveling to, the United States, and some of the Section 702 selectors were missed in the detasking process. [redacted] detasking delays that occurred during this reporting period were the result of this fact pattern.[22] Most of these detasking delays were quickly identified and remedied, but in NSA Incident [redacted], an e-mail account remained on collection for approximately five weeks after its user was discovered to have traveled to the United States because the analyst had inadvertently detasked only some of the facilities known by NSA to be used by this individual.

~~(S//NF)~~ Ensuring that selectors are detasked when a target enters the United States requires not only that analysts be attentive, but also that they have access to accurate and up-to-date tasking records [redacted] tasked for a particular target, [redacted] The joint oversight team assesses that this linkage problem needs to be addressed to prevent future situations where some of a target's selectors are not promptly detasked, as required by the NSA targeting procedures. This is also one of the many instances in which good compliance practice is also good intelligence practice – ensuring that NSA has up-to-date, accessible, and accurate corporate records of all of the known communication facilities used by the targets of its acquisitions will also facilitate the analysis and production of foreign intelligence information. NSA has reported that it is examining how NSA targeting databases can be better used to centralize knowledge regarding all of a target's known facilities, which could have prevented some of the detasking delays. The joint oversight team assesses that improved linkage among the various NSA databases should be given high priority.

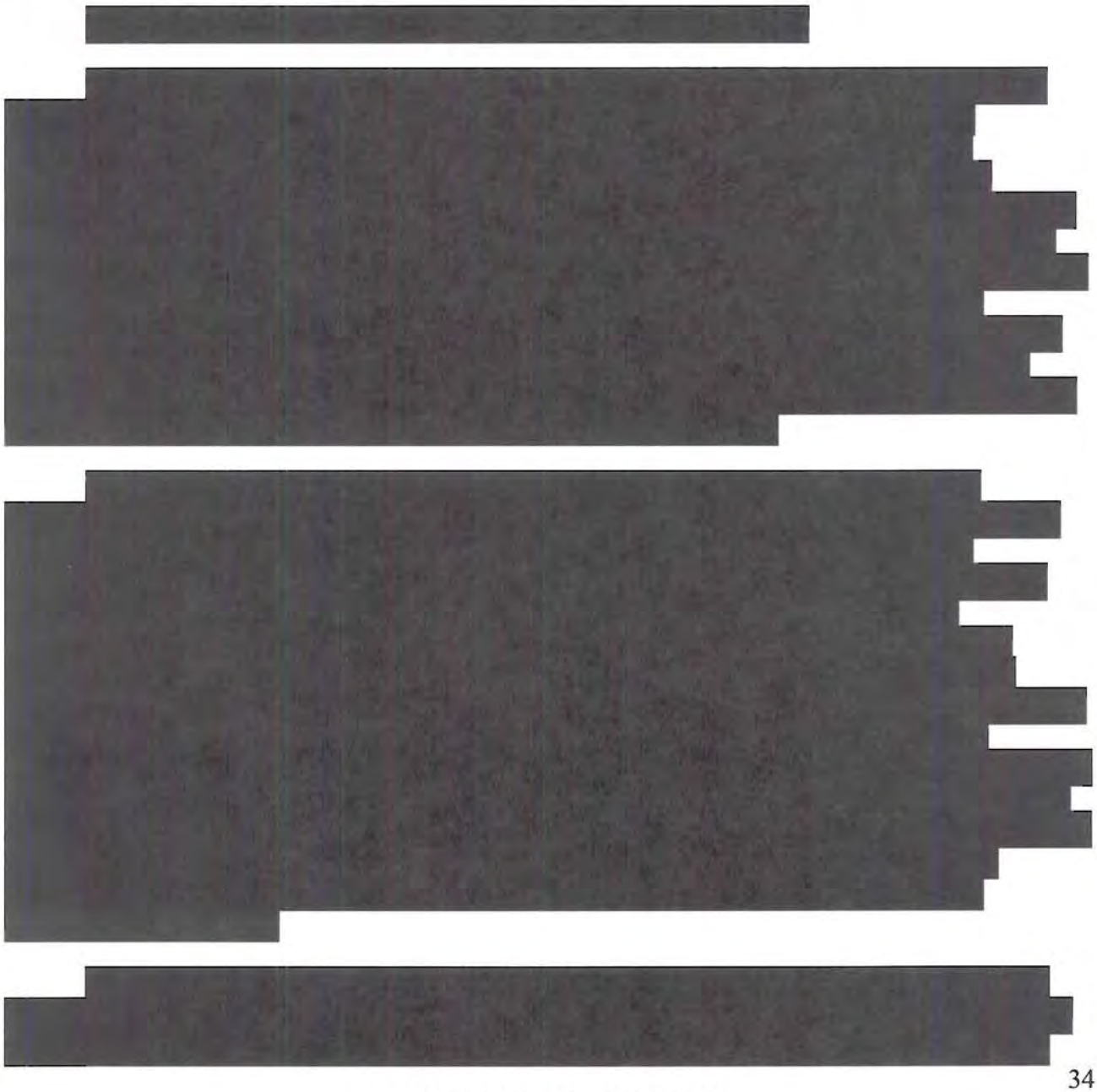
~~(S//NF)~~ There were other incidents involving human errors during this reporting period. For example, NSA Incidents [redacted]. This "retasking" issue is a familiar one at NSA and the joint team has seen a sharp decline in such incidents over time as a result of measures taken by NSA to address it.

---

[21] ~~(TS//SI//NF)~~ For example, NSA Incidents [redacted] are examples of typographical errors or similar errors that were committed when NSA was entering the selector name into the collection system or at some earlier time in the targeting process. The joint oversight team assesses that the overall rate of these types of errors is extremely low reflecting the great care analysts use to enter information and the effectiveness of the NSA pre-tasking review process in catching potential errors.

[22] ~~(S//NF)~~ See, e.g., NSA Incidents [redacted].

~~(S//NF)~~ Both the joint oversight team and the internal oversight programs have continued their attention on human errors that are susceptible to retraining. Though still relatively few in number, there was an increase of such incidents during this reporting period. [redacted] Other incidents resulting from confusion regarding legal or other requirements included several incidents regarding the necessity to promptly detask facilities where [redacted] (*see* NSA Incidents [redacted] and analysts not understanding the appropriate steps to take ensure a facility is detasked when a user of a Section 702 facility is determined to be located in the United States (*see* NSA Incidents [redacted]



[redacted]

[redacted]

~~(S//NF)~~ **III. Review of Compliance Incidents – CIA Minimization Procedures**

~~(S//NF)~~ During this reporting period, there were [redacted] incidents involving noncompliance with the CIA minimization procedures.

[redacted]

[redacted]

[redacted]

~~(S//NF)~~ **IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures**

~~(S//NF)~~ There were [redacted] incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period. In [redacted], it was determined that FBI had not been providing quarterly reports of foreign disseminations of Section 702-acquired United States person information to NSD, [redacted] FBI is now providing these reports.

~~(S//NF)~~ The other [redacted] incidents during this reporting period concerned errors in the processing of requests [redacted], one of which involved an individual located in the United States. With respect to the incident involving an individual located in the United States (FBI Incident [redacted]), FBI accidentally approved the [redacted] for an individual who had recently been found to be in the United States; FBI intended to reject that acquisition request, but the supervisory agent inadvertently selected the wrong option in FBI's targeting system and instead approved the request. FBI systems have a fail-safe to prevent the acquisition [redacted] under this scenario, but due to a system error, this fail-safe did not prevent the acquisition [redacted] in this case. The coding error in the fail-safe has since been corrected and the acquired communications were purged. In a second incident of note, FBI Incident [redacted], FBI personnel processing an FBI nomination [redacted] request relied upon an FBI agent's assessment that certain non-targeted individuals whom may have been located in the United States did not have access to an e-mail account nominated for Section 702 collection. After the acquisition was approved, it was determined that the FBI agent did not have a substantial basis for his assessment; queries run after the acquisition was approved, however, revealed no indication that these other non-targeted individuals were in fact located in the United States at the time of acquisition.

~~(S//NF)~~ The remaining [redacted] incidents involved instances where FBI did not properly [redacted] required by FBI's targeting procedures. In each case, [redacted] and in none of these cases was anything discovered that undermined FBI's targeting determination that the target was a non-United States person reasonably believed to be located outside the United States. Although these [redacted] incidents involve only [redacted] acquisitions FBI authorized during this reporting personnel, FBI personnel [redacted] have been reminded of the importance of properly [redacted]. The joint oversight team believes the protocols and training developed by FBI's Exploitation/Threat Section will continue to ensure that this error rate remains low.

~~(S)~~ **V. Review of Compliance Incidents – Provider Errors**

~~(S//NF)~~ During this reporting period, there were [redacted] incidents of noncompliance by an electronic communication service provider with a Section 702(h) directive. Each incident involved

an overproduction of data. [redacted] although in some cases the produced data was Court-authorized collection that was merely mislabeled. All agencies who received this data have completed their respective purges. [redacted].

~~(S//NF)~~ Although the causes were different, in all [redacted] of these incidents, overproductions were identified by agency personnel, either through automated systems or by agents and analysts properly reporting within their agencies that the acquired data did not correspond with the authorized scope of collection. The joint oversight team believes that this demonstrates a success in training and collection monitoring programs, and encourages agencies to maintain their vigilance in identifying possible overproductions. The joint oversight team also assesses that the overall number of overproductions during this reporting period, and over the course of the entire Section 702 program, has been relatively small. NSD and ODNI assess that this is due to the [redacted] resources and efforts all involved parties have devoted to ensuring that providers are producing only authorized data. NSD and ODNI will continue to assist the agencies in these efforts as collection activities expand and evolve.

(U) SECTION 5: CONCLUSION

(U//~~FOUO~~) During the reporting period, the joint team found that the agencies have continued to implement the procedures and to follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. As in previous reporting periods, the joint oversight team has identified no indications of any intentional or willful attempts to violate or circumvent the requirements of the Act in the compliance incidents assessed herein. Although the number of compliance incidents continued to remain small, particularly when compared with the total amount of collection activity, a continued focus is needed to address underlying causes of the incidents which did occur, including maintaining close monitoring of collection activities and finishing the implementation of personnel training enhancements. The joint oversight team will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.

APPENDIX A

APPENDIX A

(U) IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

~~(S//NF)~~ I. Overview - NSA

~~(TS//SI//NF)~~ The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).[1] As required by Section 702, those targets must be non-United States persons[2] reasonably believed to be located outside the United States. During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:

[redacted]

~~(S//NF)~~ As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the

---

[1] (U) Specifically, Section 701(b)(4) provides:

> The term 'electronic communication service provider' means -- (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

2 (U) Section 101(i) of FISA defines "United States person" as follows:

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section101(a)(20) of the Immigration and Nationality Act [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 subsection (a)(1), (2), or (3).

[redacted]

United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General's Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

~~(TS//SI//NF)~~ Under the Section 702 targeting process, NSA targets persons by tasking selectors used by those persons to communicate foreign intelligence information. A selector is a specific communications identifier or facility tasked to acquire information that is to, from, or about a target. A "selector" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address. [redacted] In order to acquire foreign intelligence information from or with the assistance of an electronic communication service provider, NSA uses as a starting point a selector to acquire the relevant communications, and, after applying the targeting procedures (further discussed below) and other internal reviews and approvals, "tasks" that selector in the relevant tasking system. The selectors are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

~~(S//SI//NF)~~ Once information is collected from these tasked selectors, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is initially routed to NSA. [redacted]

~~(S//NF)~~ NSA's targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably believed to be located outside the United States, the post-targeting analysis conducted on the selectors, and the documentation required.

[redacted]

[6] ~~(S//NF)~~ As noted in the Section 707 Report, with respect to and ongoing acquisitions from certain electronic communication service providers, [redacted] technical assistance in acquiring and transmitting raw, unminimized data [redacted]

(U) A. Pre-Tasking Location

~~(S//NF)~~ 1. Telephone Numbers

~~(S//SI//NF)~~ For telephone numbers, NSA analysts may [redacted]

~~(S//NF)~~ 2. Electronic Communications Identifiers

(S//~~SI//~~NF) For electronic communications identifiers, NSA analysts may [redacted]

[redacted]

[8] ~~(S//NF)~~ Analysts also check this system as part of the "post-targeting" analysis described below.

[redacted]

[redacted]

(U) B. Pre-Tasking Determination of United States Person Status

[redacted]

~~(S//NF)~~ C. Post-Tasking Checks

[redacted]

~~(S//SI//REL TO USA, FVEY)~~ NSA also requires that tasking analysts review information collected from the selectors they have tasked. [redacted]

[10] ~~(S//NF)~~ [redacted]

[11] ~~(S)~~ Prior Joint Assessments have stated that the automated notification and review process described in this paragraph applied to all Section 702 acquisition. The past Joint Assessment stated that NSA and ODNI were looking into this issue, and in June 2013 NSA reported that its automated notification system to ensure targeters have reviewed

[redacted]

(U) D. Documentation

~~(S//NF)~~ The procedures provide that analysts will document in the tasking database a citation to the information that led them to reasonably believe that a targeted person is located outside the United States. The citation is a reference that includes the source of the information, [redacted], enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable belief. Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information.

[redacted]

collection is currently implemented only for [redacted], not [redacted]. NSA is currently attempting to develop a similar system for [redacted]

[redacted]

~~(S//NF)~~ The source records cited [redacted] are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations [redacted] Other source records may consist of "lead information" from other agencies, such as disseminated intelligence reports [redacted]

[redacted]

(U) F. Internal Procedures

~~(S//NF)~~ NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA Office of General Counsel (OGC) and Signals Intelligence Directorate (SID) Oversight and Compliance training program; review the targeting and minimization procedures as well as other documents filed with the certifications; and must pass a competency test. The databases NSA analysts use are subject to audit and review by SID Oversight and Compliance. For guidance, analysts consult standard operating procedures, supervisors, SID Oversight and Compliance personnel, NSA OGC attorneys, and the NSA Office of the Director of Compliance.

~~(S//NF)~~ NSA's targeting and minimization procedures require NSA to report to NSD and ODNI any incidents of non-compliance with the procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the

intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States, with a requirement to purge from NSA's records any resulting collection. NSA must also report any incidents of non-compliance, including overcollection, by any electronic communication service provider issued a directive under Section 702. Additionally, if NSA learns, after targeting a person reasonably believed to be outside the United States, that the person is inside the United States, or if NSA learns that a person who NSA reasonably believed was a non-United States person is in fact a United States person, NSA must terminate the acquisition, and treat any acquired communications in accordance with its minimization procedures. In each of the above situations, NSA's Section 702 procedures during this reporting period required NSA to report the incident to NSD and ODNI within the time specified in the applicable targeting procedures (five business days) of learning of the incident.

~~(S//NF)~~ The NSA targeting and minimization procedures require NSA to conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA Office of the Inspector General (NSA OIG) and NSA's OGC. SID Oversight and Compliance conducts spot checks of targeting decisions and disseminations to ensure compliance with procedures. SID also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

~~(S//NF)~~ NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. The SID Oversight and Compliance office works with analysts at NSA, and with CIA and FBI points of contact as necessary, to compile incident reports which are forwarded to both the NSA OGC and NSA OIG. NSA OGC then forwards the incidents to NSD and ODNI.

(U/~~FOUO~~) On a more programmatic level, under the guidance and direction of the Office of the Director of Compliance (ODOC), NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protection to United States persons during NSA missions. ODOC complements and reinforces the intelligence oversight program of NSA OIG and oversight responsibilities of NSA OGC.

~~(S//NF)~~ A key component of the CMCP, is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort, known as "Rules Management," focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA and (2) technological solutions to support (and simplify) Rules Management activities. ODOC also coordinated NSA's use of the Verification of Accuracy (VoA) process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy and compliance officials within NSA. NSA has also developed a Verification of Interpretation (VoI) review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA's FISA activities. ODOC has also developed a risk assessment process to assess the potential risk of non-compliance with the rules designed to protect United States person

privacy. The assessment is conducted and reported to the NSA Deputy Director and NSA Senior Leadership Team bi-annually.

~~(S//NF)~~ II. Overview - CIA

[redacted]

[redacted] Based on its foreign intelligence analysis, CIA may "nominate" a selector to NSA for potential acquisition under one of the Section 702(g) certifications. [redacted]

[redacted]

[redacted]

Nominations are reviewed and approved by a targeting officer's first line manager, a component legal officer, a senior operational manager and the FISA Program Office prior to export to NSA for tasking. [redacted]

[redacted]

[redacted]

[redacted]

(S//NF) The FISA Program Office was established in December 2010 [redacted] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, with program external focus and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts [redacted] The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

(U) B. Oversight and Compliance

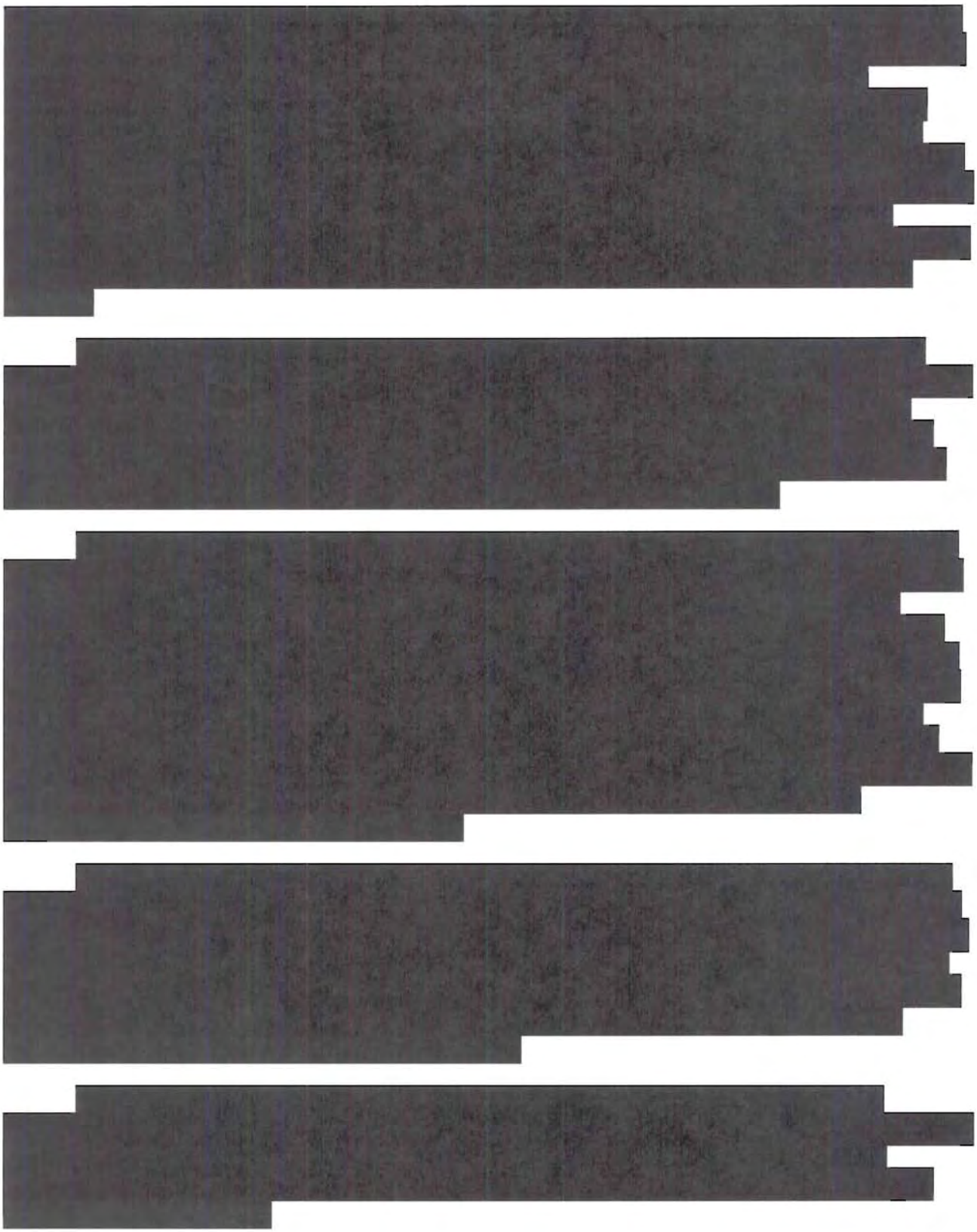
~~(S//NF)~~ CIA's compliance program is coordinated by its FISA Program Office and CIA's Office of General Counsel (CIA OGC). CIA provides small group training to analysts who nominate accounts to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained analysts. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination and minimization questions. Identified incidents of noncompliance with the CIA minimization procedures are reported to NSD and ODNI by CIA OGC.

~~(S//NF)~~ III. Overview - FBI

~~(S//NF)~~ A. FBI's Role in Targeting -- [redacted]

~~(S//NF)~~ [redacted] including information underlying the basis for the foreignness determination and the foreign intelligence interest [redacted]

[redacted]



[redacted]

[redacted]

[redacted]

(U) C. Documentation

~~(S//NF)~~ The targeting procedures require that [redacted]. FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [redacted], extending through [redacted], and culminating in approval or disapproval of the acquisition. In addition, the FBI standard operating procedures call for [redacted] depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications [redacted] regarding its review of the [redacted] information. Additional checklists have been created to capture information on requests withdrawn [redacted], or not approved by FBI.

(U) D. Implementation, Oversight and Compliance

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI's Office of General Counsel (FBI OGC), particularly the National Security Law Branch (NSLB), as well as FBI's Exploitation Threat Section (XTS), formerly the Communications Exploitation Section

(CXS),[13] FBI's Data Intercept Technology Unit (DITU), and FBI's Inspection Division (INSD). DITU personnel conduct [redacted], as well as provide technical assistance [redacted] in the acquisition of [redacted] communications. All acquisitions must be conducted in accordance with established DITU practices. XTS has the lead responsibility in FBI for both [redacted] requests [redacted]. XTS personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests for the [redacted]. XTS also has the lead responsibility for facilitating FBI's nominations [redacted] for the acquisition of [redacted] communications. XTS, NSLB, NSD, and ODNI have all worked on training FBI personnel to ensure that FBI nominations and post-tasking review comply with [redacted] targeting procedures. Numerous such trainings were provided during the current reporting period. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in the FBI's [redacted]

~~(S//NF)~~ [redacted] periodic reviews by NSD and ODNI, at least once every 60 days. FBI must also report incidents of non-compliance with the FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. XTS and NSLB are the lead FBI elements in ensuring that NSD and ODNI received all appropriate information with regard to these two requirements.

(U) IV. Overview - Minimization

~~(S//NF)~~ Once a selector has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, and CIA. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

~~(S//NF)~~ The minimization procedures do, however, impose additional obligations or restrictions as compared to minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications 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 the communication is acquired, or was in fact a United States person at the time of targeting.

[13] (U//~~FOUO~~) The change of name was effective July 15, 2012.

~~(S//NF)~~ NSA, CIA, and FBI have created systems to track the purging of information from their systems. CIA and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.