(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: December 1, 2013 – May 31, 2014

June 2015

[redacted]

(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

June 2015

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

June 2015

Reporting Period: December 1, 2013 – May 31, 2014

(U) EXECUTIVE SUMMARY

(U) The FISA Amendments Act of 2008 (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. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting and minimization procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the twelfth joint compliance assessment of the Section 702 program. This assessment covers the period from December 1, 2013, through May 31, 2014 (hereinafter the "reporting period") and 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 September 4, 2014, which covered the same reporting period.

(U) This Joint Assessment is based upon the compliance assessment activities that have been jointly conducted by the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI).

(U) 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 that occurred during the reporting period represent a very small percentage of the overall collection activity, which has decreased 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 oversight 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 (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 twelfth joint compliance assessment under Section 702, covering the period December 1, 2013, through May 31, 2014 (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
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

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.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United

[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 September 4, 2014, as required by Section 707(b)(1) of FISA, and covers the same reporting period.

States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information.[2] 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). An overview of how these agencies implement the authority appears in Appendix A of this assessment. The other agency involved in implementing Section 702 is the National Counterterrorism Center (NCTC), which has a limited role, as reflected in the "Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended."[3]

(U) 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) In summary, the joint oversight 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 oversight 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

[2] [redacted]

[3] (U) 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).

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. Further, the joint oversight team will also continue to 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

(U) 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[4] 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 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 oversight 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 oversight team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this Joint Assessment.

(U) I. Joint Oversight of NSA

(U) 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 checks of all Section 702-tasked communication facilities[5] 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.

[4] (U) As discussed herein, CIA receives Section 702-acquired data from NSA and FBI.

[5] (U) 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 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.

(U) NSD and ODNI's joint oversight of NSA's implementation of Section 702 consists of periodic compliance reviews, which the NSA targeting procedures require,[6] 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: (U) NSA Reviews

Date of Review	Taskings/Minimization Reviewed
February 19, 2014	December 1, 2013 – January 31, 2014
April 24, 2014	February 1, 2014 – March 31, 2014
June 18, 2014	April 1, 2014 – May 31, 2014

(U) Reports for each of these reviews, which document the relevant time period of the review, the number and types of communication facilities tasked, 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.

(U) The joint oversight 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 facility 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, the joint oversight team determines 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 did not provide sufficient information, and requests additional information.

(U) 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 electronic and telephonic exchanges to answer questions and clarify issues.

(U) 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

[6] (U) NSA's targeting procedures require that the onsite reviews occur approximately every two months.

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.

(U) Additionally, the joint oversight team 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 incidents of non-compliance. For example, NSA is required to report all instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target's travel to the United States. The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. 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.

(U) II. Joint Oversight of CIA

(U) 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. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team conducts onsite visits at CIA and 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.

(U) The onsite reviews also focus on CIA's application of its minimization procedures. For this reporting period, NSD and ODNI conducted the following onsite reviews at CIA:

Figure 2: (U) CIA Reviews

Date of Visit	Minimization Reviewed
March 5, 2014	December 1, 2013 – January 31, 2014
April 30, 2014	February 1, 2014 – March 31, 2014
June 25, 2014	April 1, 2014 – May 31, 2014

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.

(U) 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 personnel 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 foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.

(U) CIA may receive [redacted][7] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's Section 702 minimization procedures. [redacted] as further described in detail in Appendix A, CIA nominates potential Section 702 targets to NSA. [redacted] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [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. These processes are further described in Appendix A.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with the CIA minimization procedures, the Attorney General Acquisition Guidelines, or other agencies' procedures in which CIA is involved.[8] 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.

(U) III. Joint Oversight of FBI

(U) FBI fulfills various roles in the implementation of Section 702. First, FBI is authorized under the certifications to acquire foreign intelligence information. These acquisitions must be conducted pursuant to FBI's targeting procedures. Second, FBI also provides [redacted]

(S//NF) More specifically, FBI provides [redacted] Under its own authority, FBI is authorized [redacted] from electronic communication service providers, by targeting facilities that NSA designates (hereinafter "Designated Accounts"). FBI conveys [redacted] from the electronic communications service providers [redacted] for processing in accordance with the agencies' FISC-approved minimization procedures.

[7] [redacted]

[8] (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve CIA.

(U) Third, [redacted] FBI may receive [redacted] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI's Section 702 minimization procedures. Like CIA, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

(U) 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 FBI's internal compliance program, are set forth in further detail in Appendix A.

(U) NSD and ODNI generally conduct monthly reviews of FBI's compliance with its targeting procedures and bi-monthly reviews of FBI's compliance with its minimization procedures. For this reporting period, onsite reviews were conducted on the following dates:

Figure 3: (U) FBI Reviews

Date of Visit	Tasking and Minimization Reviewed
February 21, 2014	December 2013 taskings
March 28, 2014	January 2014 taskings; December 1, 2013 – January 31, 2014 minimization
May 9, 2014	February 2014 taskings
June 11, 2014	March 2014 taskings; February 1 – March 31, 2014 minimization
July 2, 2014	April 2014 taskings
July 15, 2014	May 2014 taskings; April 1 – May 31, 2014 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.

(U) In conducting the targeting review, the joint oversight team reviews the targeting checklist completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.[9] The joint oversight team also reviews a sample of other 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.

(U) With respect to minimization, the joint oversight team reviews documents related to FBI's application of its minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations of information acquired under Section 702 that FBI identified as potentially containing United States person information. In

[9] ~~(S//NF)~~ Supporting document includes, among other things, [redacted] The joint oversight team reviews every file identified by FBI [redacted]

addition, during reviews at individual FBI field offices, NSD reviews FBI's use of identifiers to query raw FISA-acquired data, including Section 702-acquired data.

(U) During this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at thirteen FBI field offices between December 1, 2013, through May 31, 2014, and reviewed [redacted] involving Section 702-tasked facilities. These reviews are further discussed in Section IV below.[10]

(S//NF) Separately, in order to evaluate the FBI's [redacted] acquisition [redacted] and provision of [redacted], the joint oversight team conducts an annual process review with FBI's technical personnel to ensure that these activities comply with applicable minimization procedures. The most recent annual process review occurred in May 2014. That review revealed no issues with the process used by FBI's [redacted].

(U) Additionally, and as further described in detail in Appendix A, FBI nominates potential Section 702 targets to NSA. [redacted] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) 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.[11] 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 by these investigations are reported to the congressional committees in the Section 707 Report, and to the FISC through quarterly reports or individualized notices.

[10] (U) Previously, ODNI joined NSD on these reviews when the FBI field offices were located in or within reasonable driving distance of the Washington, D.C., area (e.g., the Washington Field Office and the Baltimore Field Office). No such reviews in the Washington, D.C., area were conducted during this reporting period. Subsequent to this reporting period, ODNI began joining NSD in reviews conducted in FBI field offices outside the Washington, D.C., area. ODNI receives written summaries from NSD regarding all reviews.

[11] (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.

(U) IV. Joint Oversight of NCTC

(U) As noted above, NCTC is also involved in implementing Section 702, albeit in a limited role, as reflected in the "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 but NCTC has been provided access to certain FBI systems containing minimized Section 702 information. As part of the joint oversight of NCTC to ensure compliance with these procedures, on May 15, 2014, NSD and ODNI conducted a review of NCTC's access, receipt, and processing of Section 702 information received from FBI. The report of this review, which concluded that NCTC's systems and process complied with the NCTC's Section 702 minimization procedures, has previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

(U) V. Interagency/Programmatic Oversight

(U) 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 telephone calls and quarterly meetings (in addition to ad hoc calls and meetings on specific topics as needed) with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures.

(U) 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) VI. Training

(U) 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 continued their training efforts to ensure compliance with the targeting and minimization procedures. NSA continued to administer the new compliance training course implemented in the prior reporting period. All NSA personnel are required to complete this course on an annual basis in order to gain access to raw Section 702 acquisitions. CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a training program that provides hands-on experience with handling and minimizing Section 702-acquired data. FBI has similarly continued implementing its online training programs regarding nominations, minimization, and other requirements. Completion of

these FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI have also conducted several in-person trainings at FBI field offices.

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

(U) 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.

(U) I. Trends in NSA Targeting and Minimization

(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,[12] the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced decreases. For example, there was a slight decrease from the prior reporting period to the current reporting period.

[12] (U) The provided number of facilities on average subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released on June 26, 2014, by ODNI in its 2013 Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities (hereafter the 2013 Transparency Report). The classified numbers provided in the table above estimates the number of *facilities* subject to Section 702 acquisition, whereas the unclassified number provided in the 2013 Transparency Report estimates the number of *targets* affected by Section 702 (89,138). As noted in the 2013 Transparency Report, the "number of 702 'targets' reflects an estimate of the number of known users of particular facilities subject to intelligence collection under those Certifications." Furthermore, the classified numbers of facilities in the table above account for the number of facilities subject to Section 702 acquisition *during the current six month reporting period* (e.g., December 1, 2013 – May 31, 2014), whereas the 2013 Transparency Report estimates the number of targets affected by Section 702 *during the calendar year 2013*.

Figure 4: ~~(TS//SI//NF)~~ Average Number of Facilities Under Collection

~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [redacted] facilities were under collection [redacted] any given day during the reporting period. This represents a 0.2% decrease from the approximately [redacted] facilities under collection on any given day in the last reporting period. [redacted]

(U) The above statistics describe the average number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.[13] Classified Figure 5 charts the total monthly numbers of newly tasked facilities since collection pursuant to Section 702 began in September 2008.[14]

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

[14] (U) 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.

Figure 5: (~~TS//SI//NF~~) New Taskings by Month (Monthly Average for 2008 through November 2013)

(~~TS//SI//NF~~) Specifically, NSA provided documentation of [redacted] new taskings during the reporting period. This represents a 2.2% decrease in new taskings from the previous reporting period. [redacted]

(TS//SI//NF) The average number of telephone numbers tasked each month in 2013 was [redacted] and [redacted] average monthly telephone taskings for the first five months of 2014. This represents [redacted] increase in the average monthly telephone taskings in the first five months of 2014 compared to 2013's monthly average. [redacted] As a year over year measure, the average number of electronic communication accounts increased through 2013, but began to decrease in 2014. Specifically, the average number of electronic communications accounts tasked each month in 2013 [redacted] increase from the prior

15 [redacted]

year. The average number of electronic communication accounts tasked for the first five months of 2014 [redacted] decrease from 2013's monthly average, but roughly equivalent to the average number of electronic communication accounts that were tasked each month in 2012.

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702- or Protect America Act (PAA)-acquired data, and provided NSD and ODNI access to all reports NSA identified as containing United States information. Figure 6 contains the classified actual number of serialized reports and reports identified as containing United States person information over the last six reporting periods. NSD and ODNI's review revealed that in the vast majority of circumstances, the United States person information was at least initially masked.[16] During the past six reporting periods, the number of serialized reports based upon minimized Section 702- or Protect America Act (PAA)-acquired data has steadily increased. During the past six reporting periods, the number of these serialized reports that NSA identified as containing United States person information has steadily increased, with the exception of the last reporting period when the number of these reports decreased.

Figure 6: ~~(S//NF)~~ Total Disseminated NSA Serialized Reports Based Upon Section 702- or PAA-Acquired Data and Number of Such Reports NSA Identified as Containing USP Information

[redacted]

[16] (U) 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.

~~(TS//SI//NF)~~ Specifically, in 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 4.2% increase from the [redacted] such serialized reports NSA identified in the prior reporting period. Figure 6 reflects NSA reporting over the last six reporting periods; the fact that reporting based on Section 702 or PAA-acquired data increased is consistent with prior reporting periods, although the rate of increase slowed during this reporting period.

~~(TS//SI//NF)~~ Figure 6 also shows the number of these serialized reports that NSA identified as containing United States person information. During this reporting period, NSA identified [redacted] serialized reports as containing United States person information derived from Section 702- or PAA-acquired data. The percentage of reports containing United States person information also decreased to 9.8% for this reporting period, a decrease from the 11.0% in the prior reporting period, and was lower than the percentages in the last five reporting periods.

(U) II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA designated-facilities that FBI approved.[17] As detailed below, the number of facilities designated for acquisition has decreased from the past reporting period, which departs from the trend in prior reporting periods.

(U) As classified Figure 7 details, FBI approves a majority of NSA's designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA designated facilities have already been evaluated and found to meet NSA's targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility 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 facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion[18] were rejected on the basis that they were ineligible for Section 702 collection.

(U) Between 2009 and November 2013, the *yearly average* of designated facilities approved by FBI steadily increased. Between December 2013 and May 2014, the *number* of designated facilities approved by FBI *each month* also steadily increased, with the exception of May 2014 (which had the lowest number of approvals recorded in 2014). NSD and ODNI have

17 [redacted]

18 [redacted]

continued to track the number of facilities approved by FBI in 2014 and will incorporate this information into future Joint Assessments.

Figure 7: [redacted]

[redacted]

(TS//SI//NF) Specifically, FBI reports that NSA designated [redacted] accounts [redacted] during the reporting period – an average of [redacted] accounts designated per month. This is a [redacted] decrease from the [redacted] accounts designated in the prior six-month reporting period. Of the electronic communications accounts for which [redacted] Section 702 collection during the reporting period, approximately [redacted]

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

(U) While prior Joint Assessments provided figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information, in 2013 FBI transitioned much of its dissemination from FBI Headquarters to FBI field offices. NSD is conducting oversight reviews of FBI field offices use of these disseminations, but because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. §1881a(l)(3)(i).

(U) III. Trends in CIA Minimization

(U) CIA only identifies for NSD and ODNI disseminations of Section 702 data containing United States person information. Classified Figure 8 compiles the number of such disseminations of reports containing United States person information identified in the last six reporting periods (June 2011-November 2011 through the current period of December 2013-May 2014). During the past six reporting periods, the number of CIA-identified disseminations containing United States person information steadily decreased, with the last reporting period having the lowest number of these disseminations.

Figure 8: ~~(S//NF)~~ Disseminations Identified by CIA as Containing Minimized Section 702-Acquired United States Person Information (Excluding Certain Disseminations to NCTC)

~~(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] and as reported in prior Joint Assessments, CIA also permits some personnel with [redacted]

[redacted] NSD and ODNI review all [redacted] containing Section 702-acquired data that CIA has identified as potentially containing United States person information to ensure compliance with CIA's minimization procedures.

(U) CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. CIA's minimization procedures must be applied to these files before they are retained or transferred to systems with broader access.[19] Classified Figure 9 details the total number of retained files and the number of those retained files that contain identified United States person information. During four of the last six reporting periods, CIA increased the number of these retained files.[20] The number of retained files identified by CIA as potentially containing United States person information has been consistently a very small percentage of the total number of retained files.

Figure 9: ~~(S//NF)~~ Total CIA Files Retained and Retained Files Containing Potential United States Person Information

[redacted]

[19] (S//NF) [redacted] In making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

[20] [redacted]

(S//NF) For this reporting period, CIA analysts retained [redacted] of which were identified by CIA as containing a communication with potential United States person information. This constitutes a [redacted] decrease in the number of files retained in the previous reporting period when [redacted] of which contained potential United States person information.

(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U) 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) 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 oversight team does not believe that these incidents represent an intentional attempt to circumvent or violate the procedures required by the Act.

(U) 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) 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. Statistical Data Relating To Compliance Incidents

~~(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 and [redacted] involving noncompliance with FBI targeting and minimization procedures; for a total of [redacted] incidents involving NSA and/or FBI procedures.[21] During this reporting period, there were no identified incidents of either noncompliance with CIA minimization procedures or noncompliance

[21] (U) 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. During this reporting period, NSD and ODNI did not identify any incidents involving noncompliance with the CIA minimization procedures.

by electronic communication service providers issued a directive pursuant to Section 702(h) of FISA.

(U) The following table puts these compliance incidents in the context of the average number of facilities subject to acquisition on any given day[22] during the reporting period:

Figure 10: ~~(TS//SI//NF)~~ Compliance Incident Rate

Compliance incidents during reporting period (December 1, 2013 – May 31, 2014)	[redacted]
Number of facilities on average subject to acquisition during the reporting period[23]	[redacted]
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.32%

(U) The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of 0.32% represents a substantial decrease from the 0.64% compliance incident rate in the prior reporting period. While the total compliance incident rate has decreased during this reporting period, it is important to note that this decrease largely resulted from a decrease in one specific type of incident: delays in notification. As discussed in detail below, the number of delays in notification of the joint oversight team decreased substantially from the prior period. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is actually 0.25%, as compared with 0.24% for the prior period. This information is explained below and detailed in Figure 11 below.

(U) While the incident rate remains low, this percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States person information.[24]

[22] (S//NF) [redacted] he Attorney General's Section 707 report provides further details with respect to any particular incident.

[redacted]

[23] (U) As detailed in the footnote above, the provided number of facilities on average subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released on June 26, 2014, by ODNI in its 2013 Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities (hereafter the 2013 Transparency Report).

[24] (U) The Joint Assessment has traditionally compared the number of compliance incidents to the number of average tasked facilities. Using the number of average facilities subject to acquisition as the denominator provides a general

(U) During this reporting period, in 22% of incidents,[25] 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.[26] The median length of these reporting delays was two business days and the average reporting delay was approximately ten business days.[27] The oversight team notes that the number and proportion of these notification-type incidents, relative to other types of incidents, substantially decreased since the previous reporting period.[28] This decrease in notification delays is due to discussions between NSD/ODNI and NSA and subsequent efforts by NSA ensure compliance with the notification requirement. NSA's efforts have led to continued improvement on this issue following the present reporting period.

(U) The joint oversight team assesses that another measure of substantive compliance with the applicable targeting and minimization procedures is to compare the compliance incident rate excluding these notification delays. The following Figure 11 shows this adjusted rate:

---

proxy for an activity level that is relevant from a compliance perspective. That is, the joint oversight team believes that the number of targeted facilities generally comports with the number of activities that could result in compliance incidents (e.g., taskings, detaskings, disseminations, and queries). Tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint. Previously, the Joint Assessment indicated that the joint oversight team would continue to investigate if other means of comparison could be possible either with the currently tracked actions or by implementing the tracking of certain other data. Although other methodologies are possible, the joint oversight team has found that the methodology used currently provides a useful means of tracking this rate over consecutive years so as to discern general trends regarding how the Section 702 program is functioning from a compliance standpoint.

[25] [redacted]

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

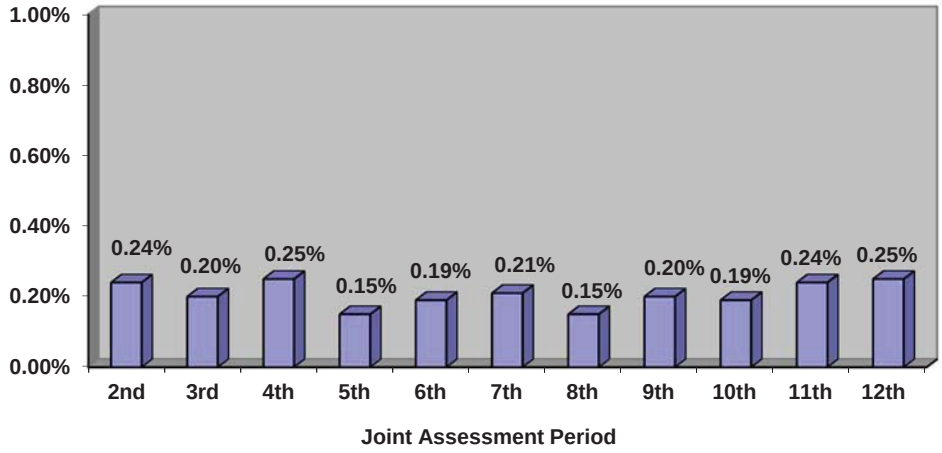
[redacted]

NSA Targeting Procedures at [redacted].

[27] [redacted]

[28] [redacted]

Figure 11: (U) Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), Not including Notification Delays



(U) As Figure 11 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.25%, which is consistent with low compliance incident rates seen in prior reporting periods. The joint oversight team assesses that the consistently low compliance rate is a result of its training, internal processes designed to identify and remediate potential compliance issues, as well as a continued focus by internal and external oversight personnel to ensure a continued focus on ensuring compliance with the applicable targeting and minimization procedures.

(U) B. Categories of Compliance Incidents

(U) 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:

- (U) *Tasking Issues.* This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.

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

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

- (U) *Documentation Issues.* This category involves incidents where the determination to target a facility was not properly documented as required by the targeting procedures.[29]

- (U) *Overcollection.* This category involves incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection." No overcollection incidents occurred during this reporting period.

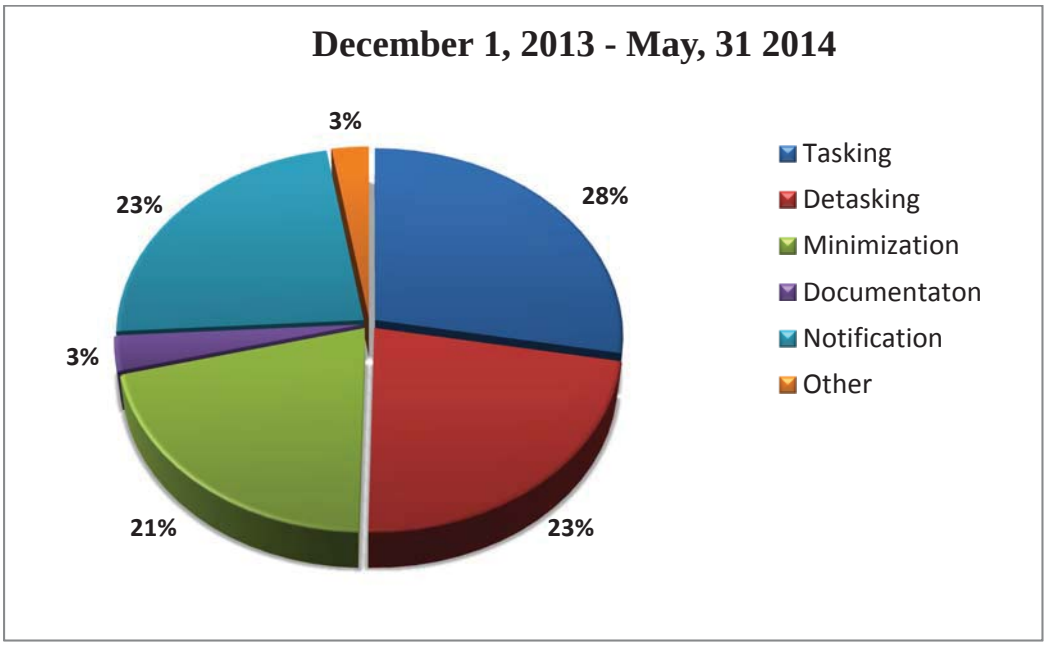
- (U) *Minimization Issues.* This category involves NSA's compliance with its minimization procedures.

- (U) *Other Issue.* This category involves incidents that do not fall into one of the six above categories.

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

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 12A depicts the percentage of compliance incidents in each category that occurred during this reporting period, whereas Figure 12B provides that actual number of incidents.

Figure 12A: (U) Percentage Breakdown of Compliance Incidents Involving the NSA Targeting and Minimization Procedures



[29] (U) As described in the Section 707 Report, not all documentation errors have been separately enumerated as compliance incidents.

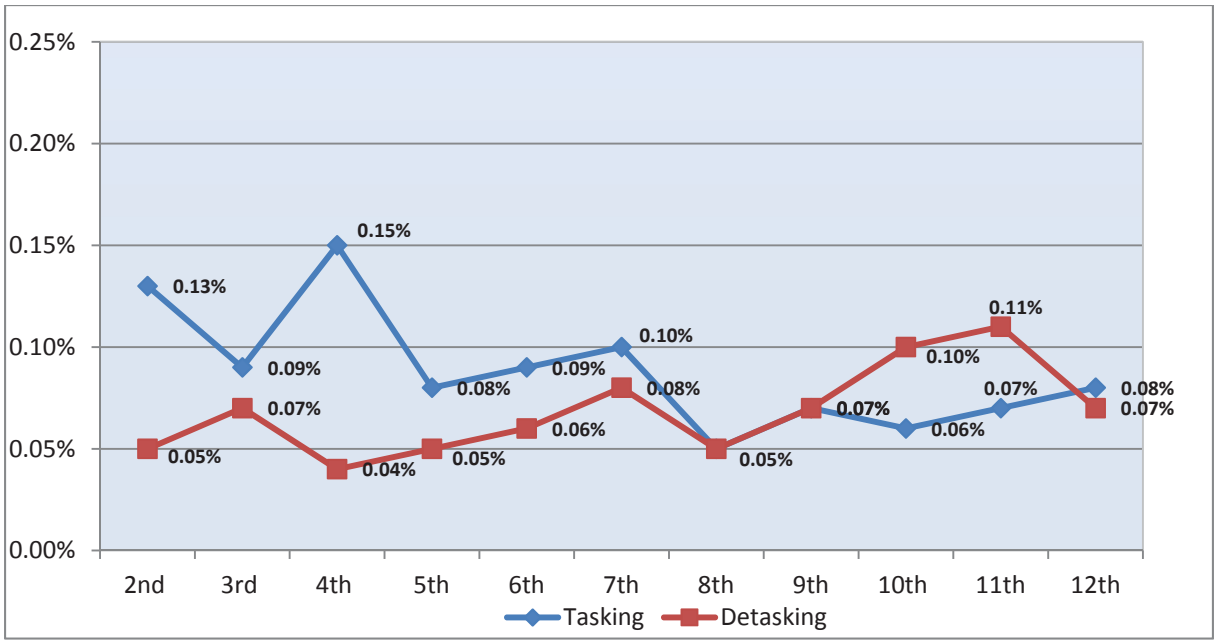
Figure 12B: ~~(S//NF)~~ Number of Compliance Incidents Involving the NSA Targeting and Minimization Procedures

(U) As Figures 12A and B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, have been substantially reduced. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, minimization procedures compliance incidents are also a focus of the joint oversight team because these types of incidents may involve information concerning United States persons.

~~(S)~~ More specifically, during this reporting period, the proportions of the incident categories changed substantially due to substantial decrease in notification delays. However, the actual numbers of non-notification delay incidents in each of the categories remained relatively constant in comparison to the prior reporting period. Specifically, the number of tasking incidents increased ; detasking incidents decreased ; minimization incidents increased ; documentation incidents increased . The number of notification delays decreased from . Additionally, during the current reporting period, "other" category incidents, whereas during the previous reporting period "other" category incidents.

(U) The following chart, Figure 13, depicts the compliance incident rates, as compared to the average facilities on task, for tasking and detasking incidents over the previous reporting periods. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other, i.e. an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate.

Figure 13: (U) Tasking and Detasking Incident Compliance Rates



(U) Over the time periods covered in the above chart, the tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection. 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 that affect no United States persons or persons located in the United States. On the other hand, detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.[30] The percentage of compliance incidents involving such detasking incidents has remained consistently low.[31]

(U) With respect to FBI's targeting and minimization procedures, incidents of non-compliance with the FBI targeting procedures occurred at the same 0.02% rate seen in the prior

[30] [redacted]

[31] (U) NSD and ODNI note that the above incident rates fluctuate by hundredths of a percentage point. Any perceived significant fluctuation is due to the scale of the graph (.00% to .25%). If, for example, the chart used a 0% to 1% scale to show fluctuations, the chart would show two virtually flat lines hugging the bottom. NSD and ODNI do not believe that any of different incident rates are statistically significant, and note that the incident rate is consistently quite low.

reporting period.[32] The total number of identified minimization errors also remains low.[33] The joint oversight team assesses that FBI's overall compliance with its targeting and minimization procedures is a result of FBI's training and the processes it has designed to effectuate its procedures.

(U) Furthermore, there were no incidents during this reporting period that involved CIA's minimization procedures, which represents a decrease from the incidents[34] that occurred during the previous reporting period for CIA. The joint oversight team assesses that CIA's compliance is a result of its training, systems and processes that were implemented when the Section 702 program was developed to ensure compliance with its minimization procedures, and the work of its internal oversight team.

(U) Finally, there were no incidents of non-compliance caused by errors made by communications service providers in this reporting period, which represents a slight decrease from the number of incidents in the last reporting period.[35] As discussed below, the joint oversight team assesses that the low number of errors by the communications service providers is the result of a [redacted] continuous effort [redacted] providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers' customers.

(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures

(U) 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 Joint 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. Most of these incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. 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 facility was a United States person, and (3) non-compliance with the NSA's minimization procedures

[redacted]

involving the unintentional improper dissemination, retention, or querying of Section 702 information.

(U) In the subsections that follow, this Joint Assessment examines some of the underlying causes of incidents of non-compliance, with a focus on the minority of incidents that have the greatest potential to impact United States persons' privacy interests. Different types of communication issues, technical and system errors, and human errors are detailed and discussed below.[36] The joint oversight team believes that analyzing the trends of these incidents, especially in regards to their causes, help the agencies focus resources, avoid future incidents, and improve overall compliance.

(U) A. Intra- and Inter-Agency Communications

(U) Section 702 compliance requires good communication and coordination within and between agencies. In order to ensure targeting decisions are made based on the totality of the circumstances, those involved in the targeting decision must communicate the relevant facts to each other. Analysts also must have access to the necessary records that inform such decisions. Good communication among analysts is also needed to ensure that facilities are promptly detasked when it is determined that the Government has lost its reasonable basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Furthermore, query rules regarding United States person identifiers and dissemination decisions regarding United States person information require inter- and intra-agency communications regarding who the Government has determined to be a United States person.

(U) In general, the joint oversight team found that better communication and coordination between and among the agencies reduced certain types of errors from occurring during this reporting period. However, the joint oversight team assesses that there is also room for continued improvement. Only one incident (discussed below) is attributable to a communication issue and resulted in a tasking error involving a United States person. Approximately 37% of the detasking delays that occurred during this reporting period are attributable to miscommunications or delays in communicating relevant facts. As with all detasking delays, these detasking delays typically involved travel or possible travel of non-United States persons to the United States. However, some of these incidents concerned delays of several days in detasking the facilities thus allowing for the potential that those facilities may have been used by United States persons located in the United States. Two more complex incidents are discussed further below.

(U) (1) Intra-Agency Communications

(U) The joint oversight team assesses that intra-agency communication and coordination have continued to improve, thereby enhancing compliance. Historically, many detasking delays resulted from a lack of intra-agency communication and coordination in the detasking of facilities

[36] (U) This current Joint Assessment is organized slightly differently than prior Assessments. Although the subsections have been reorganized, the Joint Assessment continues to analyze the underlying causes of compliance incidents while simultaneously evaluating how any compliance trends may potentially impact United States person privacy interests.

used by non-United States persons who traveled or may have traveled to the United States, especially in instances where the non-United States persons used multiple tasked accounts. As discussed below, there was a significant reduction in incidents stemming from this cause during this reporting period.

(U) More specifically, a few detasking delays occurred because the Government assessed that a non-United States person target had entered the United States, but not all Section 702-tasked facilities used by that target were promptly detasked.[37] This is a significant decrease from the number of these types of detasking delays that occurred in the prior reporting period for the same reason.[38] The joint oversight team attributes this reduction to NSA's effort to ensure analysts have ready access to a full list of all of the facilities known to be used by the target. The joint oversight team commends NSA for its improved performance in this area, and urges all agencies to continue their efforts in this regard.

(U) Other detasking delays resulted from more diffuse forms of intra-agency communication issues. For example, a small number of detasking delays (involving facilities that remained up for collection for several days after the Government should have concluded its investigation and determined that the facilities may have been used from within the United States) resulted from gaps in communication while key agency personnel were on leave during the holiday season.[39] In a comparable incident,[40] an NSA analyst discovered [redacted] but did not properly communicate with his/her team that the facility needed to be detasked; the facility was detasked [redacted]. In a separate incident,[41] one NSA targeting office determined [redacted] but the facility remained on collection for approximately two weeks because this information was not communicated to the NSA target office responsible for tasking the target's account. In an incident concerning a CIA-nominated account,[42] a facility remained on collection for approximately two days after CIA determined [redacted] because the primary CIA officer was on sick leave and other CIA officers reviewing coverage were not aware of the newly discovered information [redacted]. The above incidents are representative of the types of detasking delays that were discovered during this reporting period as a result of intra-agency communication issues. As with all detasking delays, any data acquired from such detasking delays has been purged from agency repositories.

37 [redacted]
38 [redacted]
39 [redacted]
40 [redacted]
41 [redacted]
42 [redacted]

[redacted]

(U) (2) Inter-Agency Communications

(U) As noted in the prior Assessments, communications between and among the different agencies have continued to be robust, which enhances compliance. A handful of detasking delays[43] during this reporting period were caused by breakdowns in inter-agency communications. For example, in one incident,[44] CIA determined that a facility it had nominated was [redacted] and requested NSA detask the account.[45] This request was overlooked by NSA personnel and the facility remained on collection, including for a one month period [redacted]. In a similar incident,[46] CIA determined [redacted] and notified NSA, but not through the standard channels [redacted] detasking requests, resulting in an eight day delay in the detasking. In a third incident,[47] FBI personnel also did not use standard channels and instead e-mailed an NSA analyst [redacted]

[redacted]

[redacted]; this message was not reviewed by the NSA analyst until several days later [redacted] the facility was promptly detasked. In addition to the required purges, in each of these isolated incidents, the appropriate personnel have been reinstructed on the importance of clear, prompt, and effective communication of information indicating that a Section 702 target may be a United States person or traveling to the United States, or the facility is no longer of foreign intelligence interest.

(~~U//FOUO~~) The one tasking incident[48] attributable to a communication issue involves a mismatch between the information known to two agencies. Specifically, in March 2014, CIA determined that [redacted] it had nominated [redacted] were used by a United States person; [redacted] were promptly and properly detasked and the required purges were initiated. In May 2014, an NSA analyst tasked [redacted] unaware of CIA's determination that the target was a United States person. The error was identified nine days after [redacted] was tasked, the facility was promptly detasked, and the acquired data was purged. NSD, ODNI, and NSA discussed how this incident could have been prevented, but the joint oversight team assesses that the fact that only one such tasking incident occurred during the reporting period speaks to the overall success of interagency communications regarding potential targets.

(~~S~~) A more complicated issue, which potentially could have resulted in non-compliance, but regarding which no specific instance of non-compliance was identified, involves how the *agencies themselves* communicate certain information, as opposed to how individuals within the agencies communicate. NSA Incident [redacted] details an instance where multiple redisseminations[49] of minimized Section 702-acquired information may have resulted in a dissemination of such data for a law enforcement purpose without the specific caveat language required by use 50 U.S.C. §1806(b) governing the use of such information in legal proceedings. [redacted]

[48] [redacted]

[49] (U) A "redissemination" occurs when an agency disseminates information that was previously disseminated. For example, the FBI may initially disseminate Section 702-acquired information to a federal law enforcement agency. If the FBI subsequently disseminated the same Section 702-acquired information to a foreign government, that second dissemination would be considered a "redissemination."

[redacted] The joint oversight team assesses that this complex incident demonstrates the need of agencies to communicate with each other regarding both their disseminations and redisseminations of information in order to ensure that all legal requirements are met as intended.

(U) The joint oversight team has found that the agencies have established effective 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 also continue to monitor NSA, CIA and FBI's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

(U) B. Effect of Technical Issues

(U) There were a small number of compliance incidents resulting from technical issues during this reporting period. Technical issues potentially have larger implications than other incidents because they often involve more than one facility. 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 to 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 efforts, 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. The joint oversight team believes that the lack of any overcollection incidents during this reporting period resulted from the efforts of all of the involved agencies.

(U) While technical issues can potentially have larger implications, this potential was not manifested in this reporting period. For example [redacted]

50 [redacted]

51 [redacted]

[redacted]

(U) Two incidents, which are detailed below, had moderately more substantial implications than the incidents discussed above. One incident involved the scope of purges under particular circumstances where NSA's technical processes used to identify purges was not fully identifying all the collection that it needed to purge. The other incident involved NSA's technical tools not comprehensively checking, as previously believed, underlying information that could then impact the identification of the totality of circumstances in making targeting decisions.

[redacted]

52 [redacted]

(U) These types of technical issues highlight the complexity of the technical systems used to conduct Section 702 acquisition, review information relevant to targeting decisions, and identify data subject to purge. The joint oversight team believes that the lessons that should be drawn from the incidents identified in this reporting period and prior reporting periods are three-fold. First, in designing—or even altering—interrelated systems, it is important for agencies to carefully consider the potential effects that changing one part of the system will have on other interrelated components. Second, because in a complex environment not all effects on interrelated components can be anticipated, the joint oversight team assesses that agencies must regularly monitor and reevaluate the functioning of relevant systems used to acquire and process Section 702 information. Third, independent of such system analysis, all agencies must remain vigilant to fact patterns that suggest that systems are not operating as intended.

(U) C. Effect of Human Errors

(U) As reported in previous Assessments, human errors cause the bulk of compliance incidents. Each of the agencies has established a variety of processes to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated. For example, despite multiple checks prior to tasking, as in past reporting periods, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors accounted for 46% of the tasking errors made in this reporting[53]; only one, however, resulted in the tasking of a facility used by a United States person or person in the United States. Approximately 10% of the detasking delays from this reporting period[54] resulted from an analyst [redacted] As with all other compliance incidents, any data acquired as a result of such tasking and detasking errors—regardless of whether or not the user proves to be a United States person or person in the United States—is required to be, and has been, purged. Similarly, NSA's minimization procedures required queries of Section 702-acquired data to be designed in a manner "reasonably likely to return foreign intelligence information." Fifty one percent[55] of the minimization errors in this reporting period involved non-compliance with this rule regarding queries, but in all but one of these cases the error in ensuring that the query was reasonably designed is traceable to a typographical or comparable

53 [redacted]

54 [redacted]

55 [redacted]

error in the construction for the query. For example, an overbroad query can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overbroad results as a result of the query.[56] The one exception in this reporting period involved a new analyst who was still learning how to use a query tool; [redacted]. When an overbroad query is identified, any stored results of the query are deleted and the analyst is counseled regarding the need to verify that queries are properly constructed. No incidents of an analyst purposely running a query for non-foreign intelligence reasons against Section 702-acquired data were identified during the reporting period, nor did any of the overbroad queries identified involve the use of a United States person identifier as a query term.[58]

(U) The joint oversight team assesses that the overall rate of the types of errors described above is low. The joint oversight team believes that the low rate reflects the great care analysts use to enter information, the effectiveness of the NSA pre-tasking review process in catching potential errors, and the focus in NSA training and oversight in constructing reasonably designed queries.

(U) While the joint oversight team assesses that existing practices and systems adequately reduce the number of incidents discussed above, the joint oversight team assesses that other errors could potentially be reduced with new training, procedures, or system modifications. The following subdivides such incidents into errors that could be potentially reduced through system or process changes, and those that could be addressed through training. Independent of the broader system, process, or training changes suggested below, in each of the individual incidents discussed below, data acquired as a result of the specific incidents has been purged and the personnel directly involved have been reinstructed regarding the applicable requirements.

(U) *(1) Errors That Could Be Reduced Through System/Process Changes*

~~(S//NF)~~ In response to internal oversight and NSD/ODNI requests, during or soon after the end of this reporting period, NSA made two process changes that will reduce the compliance impact of certain human errors in the future. With respect to the first change, [redacted] incidents[59] that occurred during this reporting period resulted from NSA detasking a facility when it was discovered that the facility was no longer appropriate for targeting, but the NSA an [redacted] non-emergency reason for the detask in NSA's targeting software tool.

[redacted]

56 [redacted]

57 [redacted]

58 (U) There were, however, isolated incidents in which a query identifier otherwise properly used to identify foreign intelligence information was subsequently determined to be the identifier a United States person regarding which NSA analysts took other actions, but forgot to promptly terminate [redacted] queries using the now-recognized-to-be United States person identifier.

[redacted]

59 [redacted]

[redacted] This, however, resulted in a compliance incident when a non-emergency incident detasking request was chosen when the facility should have been emergency detasked because the Government had lost its basis for assessing that all users of the tasked facility were non-United States persons reasonably believed to be located outside the United States [redacted] NSA ended the practice of the one-day delay in non-emergency detasking requests. NSA analysts, however, need to continue to take care to choose the correct detasking reason, as detasking attempts for facilities that are routed to multiple offices and/or agencies will not result in the termination of all collection unless an emergency detasking reason is selected.[60]

~~(S//NF)~~ In a second change to NSA's systems, NSA recently updated its targeting tool to further enforce an aspect of the targeting process that was previously implemented via policy.

[redacted]

(U) Additionally, but separately, the joint oversight team believes NSA should assess modifications to systems used to query raw Section 702-acquired data to require analysts to identify

60 [redacted]

61

62

63

when they believe they are using a United States person identifier as a query term. Such an improvement, even if it cannot be adopted universally in all NSA systems, could help prevent instances of otherwise approved United States person query terms being used to query upstream Internet transactions, which is prohibited by the NSA minimization procedures.[64]

(U) *(2) Errors Caused by Misunderstandings of Processes or Procedures That Can Be Addressed Through Training*

(U) The joint oversight team identified an increase during this reporting period of incidents caused by analysts, officers, or agents misunderstanding or misapplying the requirements of NSA's targeting or minimization procedures. Approximately 16% of the incidents[65] identified during this reporting period were attributable, to varying degrees, to a misunderstanding or misapplication of these rules. The overall number of such incidents compared with the number of targeting, detasking, and minimization decisions made by Government personnel remains very low, and the particular aspects of the procedures misunderstood or misapplied were diverse. The joint oversight team assesses that the low overall rate of such incidents and the fact that such incidents are not overly concentrated in any particular area generally reflects the strength of the agencies training programs. The joint oversight team, however, assesses that there are some areas where further improvements can be made.

(U) *(a) Loss of Basis for Targeting*

(U) Section 702 permits the Government to target, pursuant to specific targeting procedures, (1) non-United States persons who are (2) reasonably believed to be located outside the United States in order to (3) acquire foreign intelligence information. If the Government's basis for any of these three criteria has been undermined, detasking is required. Although each lasted only for a few days, several of the detasking delays in this reporting period were caused when Government personnel realized that the basis for one of these criteria was no longer sufficiently supported, but continued collection against the account for several days until the location or United States person status of the target was actually confirmed.

[redacted]

64 [redacted]

65 [redacted]

[redacted]

(U) The joint oversight team assesses that in light of these incidents, the agencies should reemphasize in trainings the need to promptly detask a facility when the basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States is no longer valid or has been substantially undermined by new information, which can be before location in the United States or status as a United States person is in fact confirmed.

(U) *(b) Loss of United States Person Status*

(U) Other incidents resulted from analysts/officers/agents not properly understanding the circumstances involving an individual's Lawful Permanent Resident (LPR) status.[67] Although the overall number of incidents caused by this specific issue is small, incidents that have occurred have caused new guidance to be sent to agency personnel.

[redacted]

(U) The information acquired as a result of these incidents has been purged. Due to the complex nature of immigration law, NSA, CIA, and FBI have issued written guidance regarding the need to consult with legal personnel when complex matters of law such as these develop. In addition, the joint oversight team has increased its scrutiny of potential issues related to the loss of United States person status.

66 [redacted]

67 [redacted]

(U) *(c) Sufficiency of the Information Relied Upon in Tasking/Retasking*

(U) All Section 702 tasking decisions must be made upon the totality of the circumstances. In the current reporting period, approximately 20% of the compliance incidents[68] involve initial targeting decisions based upon insufficient information to support a determination that a target was a non-United States person reasonably believed to be located outside the United States. Many of these incidents involve process issues in which the error was a failure to consider the totality of relevant circumstances; in the vast majority, but not all, of the cases, there is no indication that the individual targeted actually was in the United States or a United States person.

[redacted]

(U) The requirement that the totality of the circumstances be considered in making targeting decisions is already a core component of all of the agencies training, and the overwhelming majority of targeting decisions reflect the care with which targeting has been undertaken. The joint oversight team does not believe that further restrictions on what information must be identified or the manner in which available data must be queried to make such determinations would be advisable, as these determinations are extraordinarily fact-dependent. One improvement the joint oversight team assesses could be made, however, is to incorporate into trainings more real-world examples of how in practice relevant facts are identified and the totality of the circumstances are considered. Providing analysts, agents, and officers more practical examples regarding how to make targeting decisions will improve their targeting efforts and reduce compliance errors.

68 [redacted]

69 [redacted]

70 [redacted]

(U) III. Review of Compliance Incidents – CIA Minimization Procedures

(U) During this reporting period, there were no incidents involving noncompliance with the CIA minimization procedures, which is a decrease from the [redacted] incidents that occurred during the previous reporting period. [redacted]

(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures

(U) There were a minimal number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period. As a percentage of FBI's targeting actions during the reporting period, the FBI targeting compliance incident rate during this reporting remained at 0.02%. The targeting incidents in this reporting period that did occur were process issues that were narrow in impact, and none involved the targeting of an individual who was in fact a United States person or person located in the United States.

[redacted]

(U) Most minimization incidents were similarly minor, including an instance[71] in which an FBI analyst mistakenly conducted a query [redacted] instances of FBI agents or analysts disseminating United States person identities acquired from Section 702 in FBI's case management system in a manner that did not meet the standards of the FBI minimization procedures.[72]

[redacted]

[71] [redacted]

[72] [redacted]

[redacted]

(U) Separately, in one incident,[73] FBI identified a gap in its purge protocol for deleting communications as required by the FBI minimization procedures. As described in detail in the Section 707 report, [redacted] allowing FBI [redacted] The joint oversight team believes this incident is an example of the need of agency personnel to review the capabilities of their systems on an ongoing basis to ensure that existing protocols continue to adequately accomplish the requirements of each agency's minimization procedures.

(S//NF) Although [redacted] FBI targeting incidents involve [redacted] FBI authorized during this reporting [redacted] have been reminded of the importance of properly completing the required [redacted] Similarly, relevant FBI personnel have been instructed on the proper application of the FBI Section 702 minimization procedures. 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.

(U) V. Review of Compliance Incidents – Provider Errors

(U) During this reporting period, there were no incidents of noncompliance by an electronic communication service provider with a Section 702(h) directive. Given that errors by the service providers can result in the acquisition of U.S. person information, the Government must actively monitor the acquisitions that the providers transmit to the Government. The joint oversight team believes that the historically low number of compliance incidents caused by service providers reflect, in part, the service providers' commitment to comply with the law while protecting their customers' interests. However, the low number of these incidents also reflects continued efforts by the Government to work with service providers to ensure that lawful intercept systems are effective and compliant with all applicable law and other requirements. The Government must continue to work with the service providers to prevent future incidents of non-compliance.

[73] [redacted]

(U) SECTION 5: CONCLUSION

(U) During the reporting period, the joint oversight 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. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection activities and continued personnel training. 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

(U) I. Overview - NSA

(U) 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.

~~(S//NF)~~ 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]

[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).

[3] [redacted]

[4] [redacted]

(U) 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 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.

(U) Under the Section 702 targeting process, NSA targets persons by tasking facilities used by those persons to communicate foreign intelligence information. A facility is a specific communications identifier or facility tasked to acquire information that is to, from, or about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.[5] In order to acquire foreign intelligence information from or with the assistance of an electronic communication service provider, NSA uses as a starting point the identification of a facility to acquire the relevant communications, and, after applying the targeting procedures (further discussed below) and other internal reviews and approvals, "tasks" that facility in the relevant tasking system. The facilities 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 facilities, 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 routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.[6]

(U) 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 facilities, and the documentation required.

[5] [redacted]

[6] (S//NF) As noted in the Section 707 Report, with respect to ongoing acquisitions from certain electronic communication service providers, [redacted]

(U) A. Pre-Tasking Location

(U) 1. Telephone Numbers

[redacted]

(U) 2. Electronic Communications Identifiers

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

[redacted]

7 [redacted]

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

9 [redacted]

[redacted]

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

[redacted]

(U) C. Post-Tasking Checks

[redacted]

~~(S//SI//REL TO USA, FVEY)~~ NSA also requires that tasking analysts r[redacted] collected from the facilities they have tasked. With respect to NSA's review of [redacted],[11] a notification e-mail is sent to the tasking team upon initial c

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

facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority. [redacted] Should traffic not be viewed in at least once every 30 days, a notice is sent to the tasking team, as well as to their management, who then have the responsibility to follow up.

(U) D. Documentation

~~(S//NF)~~ The procedures provide that analysts will document in the tasking database a citation to the information leading 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.

~~(S//SI//NF)~~ NSA has [redacted] an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. [redacted] to assist analysts as they conduct their work. This tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain fields and features for targeting, documentation, and oversight purposes. Accordingly, the tool allows analysts to document the required citation to NSA records on which NSA relied to form the reasonable belief that the target was located outside the United States. [redacted] The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields [redacted] each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked. The joint oversight team assesses that the TAR has improved the oversight team's ability to understand NSA's foreign intelligence purpose in tasking facilities.

(S//NF) [redacted] Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the

record or records relied upon by the analyst, [redacted] the analyst's foreignness explanation, the targeting rationale, [redacted] These records, referred to as "tasking sheets," are reviewed by the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

~~(S//NF)~~ The source records cited on these tasking sheets 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 recorded on the tasking sheets. Other source records may consist of "lead information" from other agencies, such as disseminated intelligence reports or lead information [redacted]

[redacted]

(U) F. Internal Procedures

(U) 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.

(U) 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.

(U) 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.

(U) 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) 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.

(U) 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.

(U) II. Overview - CIA

~~(S//NF)~~ A. CIA's Role in Targeting

(S//NF) Although CIA does not target or acquire communications pursuant to Section 702, CIA has put in place a process, in consultation with NSA, FBI, NSD, and ODNI, to identify foreign intelligence targets to NSA (hereinafter referred to as the "CIA nomination process"). Based on its foreign intelligence analysis, CIA may "nominate" a facility to NSA for potential acquisition under one of the Section 702(g) certifications. [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]

12 [redacted]

(U) The FISA Program Office was established in December 2010 and is charged with providing strategic directi 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, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts 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

(U) 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 personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. 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 generally reported to NSD and ODNI by CIA OGC.

(U) III. Overview - FBI

(U) A. FBI's Role in Targeting -- Nomination for Acquiring In-Transit Communications

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process intelligence targets to NSA for the acquisition of in-transit communications information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nom NSA for tasking.

(S//NF) he FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a United States person. NSA is also responsible for determining that a significant purpose of the

acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate [redacted] FBI must then apply its own additional procedures, which require FBI to review NSA's conclusion of foreignness [redacted]

~~(S//NF)~~ More specifically, after FBI obtains the tasking sheet from NSA, it reviews the information provided by NSA regarding the location of the person and the non-United States person status of the person. [redacted]

~~(S//NF)~~ Unless FBI locates information indicating that the user is a United States person or is located inside the United States, FBI will [redacted]

(S//NF) If FBI identifies information indicating that NSA's determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve [redacted]

(U) C. Documentation

~~(S//NF)~~ The targeting procedures require that FBI retain the information [redacted] in accordance with its records retention policies [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), FBI's [redacted] and FBI's Inspection Division (INSD). [redacted] XTS has the lead responsibility in FBI for [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 [redacted]. XTS also has the lead responsibility for facilitating FBI's nominations [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 the NSA 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)~~ The FBI's targeting procedures require 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

(U) Once a facility 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.

(U) 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.

(U) 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.