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

Reporting Period: June 1, 2013 – November 30, 2013

October 2014

[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

October 2014

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

October 2014

Reporting Period: June 1, 2013 – November 30, 2013

(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. This report sets forth the Department of Justice, National Security Division (NSD) and Office of Director of National Intelligence's (ODNI) eleventh joint compliance assessment under Section 702, covering the period June 1, 2013, through November 30, 2013 (hereinafter the "reporting period"). This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was submitted as required by Section 707(b)(1) of FISA (hereinafter "the Section 707 Report") on March 6, 2014 and covers the same reporting period.

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

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

(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 which occurred during the reporting period represent a very small percentage of the overall collection activity, which has increased from the last Joint Assessment. Individual incidents, however, can have broader implications, as further discussed herein and in the Section 707 Report. Based upon a review of these compliance incidents, the joint 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, relevant portions of which are codified at 50 U.S.C. §1881 – 1881g (hereinafter "FAA"), requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq*., as amended (hereinafter "FISA" or "the Act"), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter "Section 702") have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI's eleventh joint compliance assessment under Section 702, covering the period June 1, 2013, through November 30, 2013 (hereinafter the "reporting period").[1]

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

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

[1] (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on March 6, 2014, as required by Section 707(b)(1) of FISA, and covers the same reporting period.

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

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 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

[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).

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 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 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 of National Intelligence for Intelligence Integration/Mission Integration Division (ODNI DDII/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

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

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.

(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
August 19, 2013	June 1, 2013 – July 31, 2013
October 16, 2013	August 1, 2013 – September 30, 2013
December 16, 2013	October 1, 2013 – November 30, 2013

(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 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, NSD attorneys determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that 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

[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 (also referred to as "selectors"), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. A fuller description of the Section 702 targeting process may be found in the Appendix.

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

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 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) The joint oversight team additionally investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be compliance incidents (e.g., NSA must report all instances in which Section 702 acquisition continued while a targeted individual was in the United States), but the report of which may lead to the discovery of an underlying compliance incident. Investigations of all of these incidents often result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report, and to the FISC through quarterly reports or individualized notices.

(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 periodic 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
September 4, 2013	June 1, 2013 – July 31, 2013
October 30, 2013	August 1, 2013 – September 30, 2013
December 19, 2013	October 1, 2013 – November 30, 2013

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) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with the CIA minimization procedures and/or the Attorney General Acquisition Guidelines.[7] 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

~~(S//NF)~~ FBI fulfills three separate roles in the implementation of Section 702. First, FBI is authorized under the certifications to acquire foreign intelligence information [redacted] from electronic communication service providers, by targeting facilities that NSA designates for such acquisition (hereinafter "Designated Accounts"). [redacted] must be conducted pursuant to FBI's targeting procedures. Second, FBI conveys [redacted] from the electronic communications service providers [redacted] for processing in accordance with the agencies' FISC-approved minimization procedures. Similarly, FBI also provides [redacted] Third, FBI may receive [redacted][8] 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. During this reporting period, FBI continued to expand this nominating process to its FBI field offices.

(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.

[7] (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.

[8] [redacted]

(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
September 5, 2013	June 2013 taskings
September 26, 2013	July 2013 taskings; June 1, 2013 – July 31, 2013 minimization
October 31, 2013	August 2013 taskings
December 4, 2013	September 2013 taskings; August 1, 2013 – September 30, 2013 minimization
January 8, 2014	October 2013 taskings
January 16, 2014	November 2013 taskings; October 1, 2013 – November 30, 2013 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 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 sixteen FBI field offices between June 1, 2013, through November 30, 2013 and reviewed [redacted] involving Section 702-

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

tasked facilities. ODNI participated in one of these reviews,[10] and received written summaries regarding any issues discovered in the other reviews.

(U//~~FOUO~~) NSD's review of field offices coincided with FBI's broadening of the use of Section 702-acquired data at these field offices. Although there were isolated instances of non-compliance with the FBI minimization procedures and/or FBI policy, NSD and ODNI found that overall agents understood and were properly applying the requirements of FBI policy and the minimization procedures.[11]

~~(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. Because the May 2014 review is outside this Joint Assessment's covered reporting period, the findings of this review will be address by the next Joint Assessment.

~~(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. 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) ODNI joins NSD on these reviews when the FBI field offices are located in or within reasonable driving distance of the Washington, D.C. area (e.g., the Washington Field Office and the Baltimore Field Office). During this reporting period, ODNI joined NSD for the Baltimore Field Office review. ODNI plans to continue to accompany NSD during the minimization reviews of the FBI Washington and Baltimore field offices and is continuing to explore the feasibility of joining NSD on reviews of other FBI field offices.

[11] ~~(S//NF)~~ NSD's review found only one instance where U.S. person information was not properly handled as required by the minimization procedures. Specifically, the agent improperly disseminated U.S. person information that did not meet the standard minimization procedures requirement. Although the information reasonably appeared to be foreign intelligence information, it did not seem to have met the requirement that such information shall not be disseminated in a manner that identifies a United States person unless such person's identity is necessary to understand foreign intelligence information or to assess its importance. In this case, upon NSD's review, the agent agreed that the disseminated U.S. person identity did not meet the above standard. NSD confirmed that the agent recalled the dissemination and re-issued the dissemination without identifying the U.S. person.

(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. Because the May 2014 review is outside this Joint Assessment's covered reporting period, the findings of this review will be addressed in the next Joint Assessment.

(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 meetings 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. Other Compliance Efforts

[redacted]

[redacted]

[redacted]

[12] [redacted]

[redacted]

(U) B. 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 been engaged in broader training efforts to ensure compliance with the targeting and minimization procedures. For example, during this reporting period, NSA implemented a new compliance training course that NSA personnel are required to complete on an annual basis in order to have 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, as discussed in the previous Joint Assessment, in 2013, CIA began a training program to provide hands-on experience with handling and minimizing Section 702-acquired data. CIA has continued to conduct this new training program during this reporting period. FBI, in conjunction with its broader roll-out of its formal Section 702 nomination program, has continued its training program. Additionally, as noted in the previous Joint Assessment, FBI had previously implemented (after consultation with NSD and ODNI) an online training program regarding nominations and other requirements; FBI already had an online training regarding compliance with its Section 702 minimization procedures. Both FBI online training programs continue to be required training for FBI personnel who request access to Section 702 information. NSD has also conducted numerous in-person trainings at FBI field offices.

(U) C. NSA's Office of Inspector General Report Regarding Section 702

(U) The previous Joint Assessment described the results of NSA's Office of Inspector General (OIG) issued a report titled "Assessment of Management Controls Over FAA § 702" in November 2012 and revised and reissued this report in March 2013 (hereinafter, NSA OIG Report). As previously stated, the NSA OIG Report identified several issues that required further action by NSA. NSD, ODNI, and NSA are continuing to ensure that all appropriate action is taken in response to the NSA OIG Report.

(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

~~(TS//SI//NF)~~ NSA reports that, on average, approximately [redacted] facilities were under collection pursuant to Certifications [redacted] any given day during the reporting period. This represents a 9.8% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period. While the program continues to grow, this 9.8% increase is lower than the rates of increase in the prior two reporting periods, which were 13.4% and 18.0%, respectively. As Figure 4 demonstrates, with one exception, the average number of facilities under collection has increased every reporting period.

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

[redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ 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] NSA provided documentation of [redacted] new taskings during the reporting period. This represents a 1.2% decrease in new taskings from the previous reporting period. [redacted]

(U) Figure 5 charts the total monthly numbers of newly tasked facilities since collection pursuant to Section 702 began in September 2008.[14]

Figure 5: ~~(S)~~ New Taskings by Month (Monthly Average for 2008 through 2012)

[redacted]

[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.

(U) As the chart demonstrates, the number of newly tasked telephone numbers decreased after 2009, but began to increase again in 2012.

~~(TS//SI//NF)~~ The average number of telephone numbers tasked each month in 2012 was [redacted], and [redacted] average monthly telephone taskings for the first eleven months of 2013. These average taskings [redacted]. As a year over year measure, the average number of electronic communication accounts has continued to increase. The average number of electronic communications accounts tasked each month in 2012 [redacted] increase from the prior year. The average number of electronic communication accounts tasked for the first eleven months of 2013 [redacted] increase over 2012's monthly average.

~~(TS//SI//NF)~~ With respect to minimization, 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.[15] This represents a 17.8% 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; this increase is consistent with prior increases in reporting based on Section 702- and PAA-acquired data.

[15] ~~(TS//SI//NF)~~ [redacted] serialized reports is greater than the [redacted] serialized reports for this period that the Congressional Committees were previously advised, in attachments to the March 2014 Section 707 Report, had been issued in this same reporting period. The total number of reports containing United States person information is also [redacted] fewer than previously reported. [redacted] serialized reports for the prior reporting period is less than [redacted] serialized reports previously reported. The total number of reports containing United States person information is [redacted] greater than previously reported. In August 2014, NSA determined that it had previously misreported the total number of serialized reports for this reporting period and the prior reporting period due to human errors in calculating the number of reports.

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

~~(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. NSD and ODNI's review revealed that in the vast majority of circumstances, the United States person information was at least initially masked.[16] The percentage of reports containing United States person information has remained low at 11.0% for this reporting period, a slight decrease from the 11.2% in the prior reporting period, and is within the same range of percentages of the earlier reporting periods.

(U) II. Trends in FBI Targeting

~~(TS//SI//NF)~~ FBI reports that NSA designated [redacted] accounts [redacted] during the reporting period – an average of [redacted] accounts designated per month. This [redacted] increase 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]

[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.

[redacted]

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

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

[18] [redacted]

Figure 7: [redacted]

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

~~(S//NF)~~ Prior Joint Assessments provided figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. During the prior reporting period, however, 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-acquired data containing United States person information. The following chart compiles the number of such disseminations of reports containing United States person information identified in the last six reporting periods.

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

[redacted]

(~~S//NF~~) During this reporting period, CIA identified [redacted] disseminations of Section 702-acquired data containing minimized United States person information. This is a [redacted] decrease from the [redacted] such disseminations CIA made in the prior reporting period. [redacted] and as reported in prior Joint Assessments, CIA also permits some personnel with [redacted]. NSD and ODNI, however, review [redacted] containing Section 702-acquired data that CIA has shared with NCTC and has identified as potentially containing United States person information to ensure compliance with CIA's minimization procedures.

(~~S//NF~~) In addition to disseminations, 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. The files retained may contain only a portion of a particular communication or numerous communications. In making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information. The following chart includes the total number of retained files and the number of retained files potentially containing United States person information in the last six reporting periods.[19]

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

[redacted]

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

[19] [redacted]

(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, CIA and/or FBI procedures.[20] Additionally, there were [redacted] incidents of noncompliance 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[21] during the reporting period:

[20] (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 involving noncompliance with the CIA minimization procedures.

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

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

Compliance incidents during reporting period (June 1, 2013 – November 30, 2013) (including provider incidents)	[redacted]
Number of facilities on average subject to acquisition during the reporting period[22]	[redacted]
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.64%

(U) The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of 0.64% represents an increase from the 0.42% compliance incident rate in the prior reporting period. While the total compliance incident rate has increased during this reporting period, it is important to note that this increase largely resulted from an increase in a specific type of incident. As discussed in detail below, the number delays in notification of the joint oversight team increased 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 0.24%, as compared with 0.19% for the prior period. This information is explained below and detailed in Figure 11 below.

~~(S//NF)~~ The value of statistical information in assessing compliance in situations such as this is unclear. A single incident, for example, may have broad ramifications and may involve multiple facilities. Multiple incidents (e.g., notification delays are, on the whole, less serious than other incidents, but can comprise a significant number of incidents) may increase the incident count, but may be deemed of limited significance with respect to United States person information.[23] The joint oversight team will 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.

[redacted]

(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 number 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 (sometimes referred to as selectors) subject to intelligence collection under those Certifications." Furthermore, the classified number of facilities in the table above accounts for the number of facilities subject to Section 702 acquisition *during the current six month reporting period* (e.g., June 1, 2013 – November 30, 2013), whereas the 2013 Transparency Report estimates the number of targets affected by Section 702 *during the calendar year 2013*.

[23] (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 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.

(U) During this reporting period, however, in 62% of incidents,[24] 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.[25] The median length of these reporting delays is two business days and the average reporting delay is approximately three business days. The joint oversight team unfortunately notes that these notification type incidents has increased since the last reporting period (from 54% previously)[26] and has further emphasized to NSA the importance of notifying NSD and ODNI in a timely manner so as to reduce NSA's notification delay incident rate. The joint oversight team will continue to work with NSA to ensure that notifications are made to NSD and ODNI within the time frame specified in the relevant procedures. In fact, subsequent to the current reporting period, the joint oversight team has found that NSA's efforts have resulted in an approximately 75% decrease in such notification incidents in the six months that followed this current 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:

[2] [redacted]

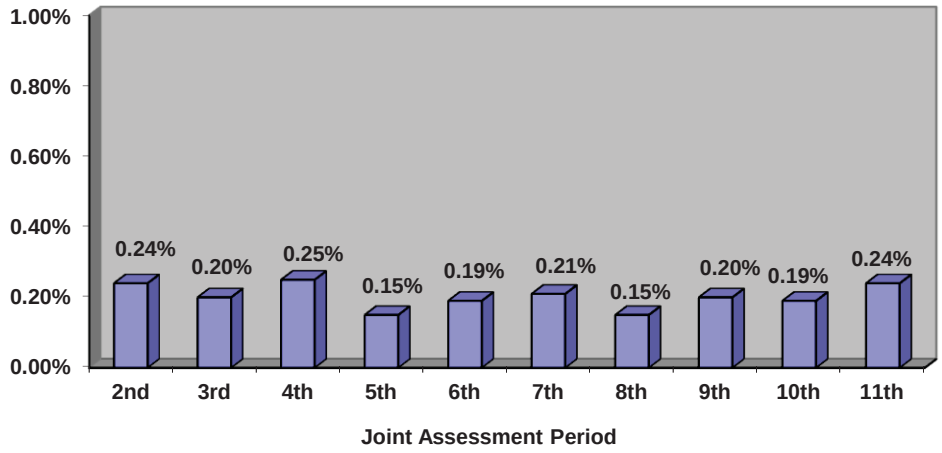
[25] ~~(S//NF)~~ Specifically, NSA's targeting procedures require:

[redacted]

NSA Targeting Procedures at [redacted]

[26] ([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 0.24%, which is consistent with low compliance incident rates seen in prior reporting periods.

(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.[27]

- (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."

- (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. The following chart depicts the numbers of compliance incidents in each category that occurred during this reporting period.

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

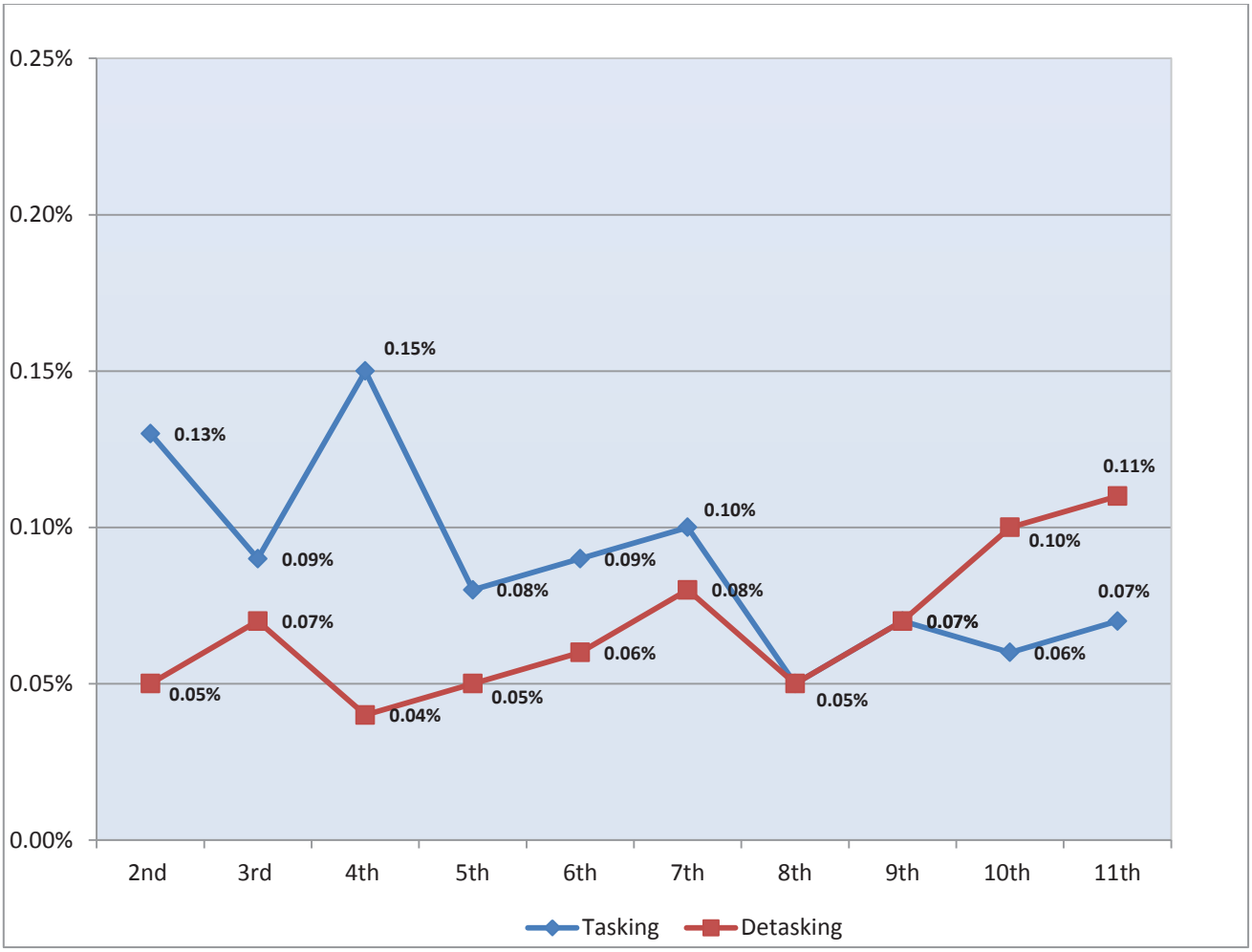
Figure 12: ~~(S)~~ Compliance Incidents Involving the NSA Targeting and Minimization Procedures

(U) As Figure 12 demonstrates, the majority of compliance incidents during the reporting period were notification delays. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, minimization procedures compliance incidents are also viewed with concern because these types of incidents may involve information concerning United States persons.

~~(S)~~ During this reporting period, the numbers of incidents in each of the categories increased from the incidents during the previous reporting period. Specifically, the number of tasking incidents increased ; detasking incidents increased ; minimization incidents increased ; documentation incidents increased ; and notification delays increased . Additionally, during the current reporting period, overcollection and "other" category incidents, whereas during the previous reporting period overcollection incidents or "other" category incidents. While this report addresses some of the possible reasons for the increase in incidents below, it is important to note that the number of facilities subject to acquisition increased during this reporting period.

(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.

Figure 13: ~~(S//NF)~~ 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 only fractions of a percentage point as compared to the average size of the collection. While tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States, 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 intended target.[28] The percentage of compliance incidents involving such detasking incidents has remained consistently low.

~~(S//NF)~~ With respect to the other targeting and minimization procedures, [redacted] incidents involved noncompliance with FBI's targeting or minimization procedures [redacted] involved targeting

[28] [redacted]

and [redacted] involved minimization issues. This was a slight increase in the number of incidents from the last reporting period in which FBI [redacted] incidents. As discussed below, each of [redacted] targeting or minimization errors resulted from unintentional errors in the targeting or minimization processes. [redacted] FBI targeting incidents occurred in the course of approving [redacted] and thus represented [redacted] of the total number of facilities tasked under FBI's targeting procedures during this reporting period. FBI's rate of [redacted] decreased slightly from the last reporting period.

~~(S//NF)~~ Furthermore, there were no incidents during this reporting period that involved CIA's minimization procedures, which represents a decrease from [redacted] incidents that occurred during the previous reporting period for CIA. Additionally, and as described below, [redacted] involved errors by communications service providers, which represents a slight increase from the one incident in the last reporting period.

(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. The first subsection examines compliance incidents that have the greatest potential to impact United States persons' privacy interests, a particular focus of the joint oversight team. Subsequent subsections discuss incidents caused by intra- and inter-agency communications (i.e., the ability of the agencies to communicate information between and among themselves in a timely manner to avoid compliance incidents), technical and system errors, and incidents caused by human errors. In addition to the trends, the subsections note whether the compliance incidents increased or decreased compared to the previous Joint Assessment and provide potential causes of the increase or decrease. The joint oversight team believes that analyzing these trends, especially in regards to determining the causes of incidents, help the agencies avoid future incidents and improve overall compliance.

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

(U) A primary concern of the joint oversight team is the impact of certain compliance incidents on United States persons. The Section 707 Report discusses every incident of noncompliance with the targeting and minimization procedures, including any necessary purges resulting from these incidents. 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 had entered the United States, or notification delays.

(U) 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 involving the unintentional improper dissemination, retention, or querying of Section 702 information. Due to their importance, these incidents are highlighted in this subsection. With regards to incidents arising from tasking errors and delays in detasking facilities concerning United States persons, either no information was acquired or, in the instances that information was acquired, such information was destroyed and no reporting was generated as a result of the erroneous acquisition. With regards incidents resulting from the unintentional improper dissemination or querying of United States person information, the disseminated reports were recalled and the queries, and their corresponding results, were destroyed. As noted above, the Section 707 Report provides further details regarding each individual incident and how any erroneously acquired, disseminated, or queried United States person information was handled through various purge, recall, and deletion processes. Although incidents of overcollection can impact United States persons, the overcollection incident that occurred during this reporting period did not involve United States persons.

(U) (1) Tasking Errors Impacting United States Persons

~~(U)~~ Of the tasking incidents described in the Section 707 report,[29] [redacted] where at the time of tasking the Government knew or should have known that one of the users of the facility was a United States person. This was a decrease from [redacted] that occurred in the prior reporting period. [redacted] incidents in this reporting period represent isolated instances of insufficient due diligence, as compared with the [redacted] of proper taskings that occurred during the reporting period and did not involve an intentional effort to target a United States person. The joint oversight team will continue to work with NSA, as well as other the agencies, to assess ways in which to avoid such mistakes in the future.[30]

~~(TS//SI//NF)~~ In NSA Incident [redacted] involved the misapplication of the rules regarding who is considered a "user" of a Section 702-tasked account. Specifically, while conducting a review in late May 2013, NSD noticed [redacted]

[29] ~~(S)~~ The Section 707 report described [redacted]

[30] ~~(U)~~ The previous Joint Assessment noted that the joint oversight team would like to see a decrease of these incidents in the future and that the NSA had revised its training, in coordination with NSD and ODNI, to address these matters. Specifically, the previous Joint Assessment stated that some of these incidents could have been avoided with a more thorough and diligent examination of the Government's databases and that following the reporting period, NSA revised its training to include providing clearer guidance to avoid these types of errors. The joint oversight team notes that in fact there was a decrease in these types of incidents [redacted] in this reporting period.

[redacted] While of concern that a United States person was tasked under Section 702 in this compliance incident, the fact that the United States person was already subjected to Court-authorized electronic surveillance and physical search pursuant to Titles I and III of FISA mitigates the impact of this Section 702 compliance incident on the United States person. Additionally, NSA advised that it recalled or cancelled disseminations resulting from the Section 702 acquisition.

(TS//SI//NF) [redacted] NSA Incident [redacted] resulted from a human error in which an NSA analyst incorrectly checked the status of a pending tasking in an NSA system. [redacted]

(U) (2) Delays in De-Tasking Impacting United States Persons

(U) The majority of the detasking incidents[31] involved non-United States persons who traveled to the United States, appeared to have traveled to the United States, or involved a non-resolvable unexplained indication of an account appearing to be accessed from within the United States.[32] [redacted] these detasking delays are confirmed to have involved a United States person. This represents a decrease from [redacted] such incidents in the prior reported period. However, the overall number of detasking errors has increased during the last three reporting periods. [33] Some of

31 [redacted]

32 [redacted]

33 [redacted]

this increase could be attributed to the increase in the number of facilities under Section 702 acquisition. That said, as noted in the previous Joint Assessment, the joint oversight team is working with NSA to evaluate other causes contributing to the rise of detasking errors, and to find possible was to avoid such errors in the future. For example, the joint oversight team is examining training and potential process improvements.

(TS//SI//NF) [redacted] (NSA Incidents [redacted] involved a recurring problem, discussed in further detail below with regard to incidents concerning non-United States persons, in which some, but not all, Section 702-tasked facilities are detasked when a target is found to be a United States person or in the United States. Such incidents often involve a contributing factor, such as a key individual who has knowledge about the target being out of the office [redacted] or because information regarding whom uses which tasked facility is lost when taskings are transferred from targeting office to another [redacted] As is discussed in Subsection II.B below, NSD and ODNI assess that better records and additional detasking procedures could help prevent detasking delays such as these.

~~(TS//SI//NF)~~ The [redacted] detasking delays concerning United States persons involved misapplications of the requirement to timely detask facilities when the basis that a facility is used by a non-United States person has been lost. Specifically, in NSA Incident [redacted]

[redacted]

(U) (3) Non-Compliance with NSA's Minimization Procedures Impacting United States Persons

(S) [redacted] incidents of non-compliance with NSA's minimization procedures occurred during this reporting period, as compared to [redacted] incidents in the prior reporting period. Although the number of incidents being reported has increased, the joint oversight team assesses that this increase appears to be due to NSA instituting additional internal reviews focused on identifying querying errors rather than an actual increase in the number of incidents that have occurred. [redacted] incidents of non-compliance, [redacted] were types that have been commonly reported in prior Joint Assessments and each of these incidents were detailed in the Section 707 report, specifically: [redacted] overly-broad queries or unauthorized queries using

United States person identifiers;[34] improper dissemination of United States person information. The number of inappropriate queries and disseminations remain an extremely small fraction of NSA's overall query and dissemination activities. For example, in this reporting period NSA disseminated containing United States person information. The incidents involving dissemination errors therefore represent error rate.

(TS//SI//NF) The joint oversight team, however, is concerned about the increase in incidents involving improper queries using United States person identifiers, including incidents involving NSA's querying of Section 702-acquired data in upstream data using United States Person identifiers. Specifically, although section 3(b)(5) of NSA's Section 702 minimization procedures permits the scanning of media using United States person identifiers, this same section prohibits using United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques. NSA incidents of non-compliance with this subsection of its minimization procedures, many of which involved analysts inadvertently searching upstream collection. For example, , the NSA analyst conducted approved querying with United States persons identifiers ( ), but inadvertently forgot to exclude Section 702-acquired upstream data from his query.

(TS//SI//NF) In addition, section 3(b)(5) of NSA's Section 702 minimization procedures requires that queries using United States person identifiers must be first be approved in accordance with NSA internal procedures. In this reporting period, NSA was in non-compliance with this requirement, either because a prior authorization was not obtained or the authorization to query had expired. For example, in NSA Incidents NSA analysts performed queries using United States person identifiers that had not been approved as query terms. These queries occurred for a variety of reasons, including because analysts continued queries on terms that they suspected (but had not confirmed) were used by United States persons, forgot to exclude Section 702 data from queries , or did not realize that constitute a United States person identifier even if the analyst was seeking information on a non-United States person. In each case, the analyst involved was retrained regarding the requirement to seek prior authorization before a Section 702 query using a United States person identifier is performed. In NSA Incident , the NSA analyst obtained proper authorization to query

[34] (S//NF) Overly-broad queries are almost always the result of inadvertent mistakes. For example, United States person queries are authorized, under particular circumstances, by NSA's Minimization Procedures. Compliance incidents result when an analyst either (1) inadvertently fails to follow NSA's internal procedures prior to conducting a query using a United States person identifier, and/or (2) uses a United States person identifier when querying NSA's upstream collection.

[35]

(i.e. the query met the appropriate foreign intelligence justification requirement) a United States person's facilities, but with a limited duration. The analyst [redacted] continued to query Section 702-acquired data after the authority to query had expired. NSA has implemented additional technological solutions to help prevent such continued querying after a query authorization has expired.

(U) The joint oversight team will continue to conduct close oversight of NSA's use of United States person identifiers to query data and will continue to work with NSA to ensure its personnel receive ongoing training that will allow them to comply with the minimization procedures.

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

(U) (1) Intra-Agency Communications

(U) The joint oversight team assesses that intra-agency communication and coordination has 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 used by non-United States persons who traveled to the United States, especially in instances where the non-United States persons used multiple tasked accounts. While, as noted below, the joint oversight team believes there are specific improvements that could further decrease the number of detasking delays in multiple account detasking situations, a very small number of intra-agency miscommunication directly resulted in a detasking delay during this period.[36] The joint oversight team commends the agencies for their improved performance in this area.

~~(TS//SI//NF)~~ Apart from miscommunications [redacted] detasking delays occurred because the Government determined 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] While such errors can occur from intra-agency miscommunications, most of these errors in the current reporting period were instead the result of human errors. For example, [redacted]

[36] [redacted]

[37] (U) *See infra* footnote 42.

[redacted]

(U) (2) Inter-Agency Communications

(U) As noted in the prior Assessments, communications between and among the different agencies have continued to improve, which enhances compliance. While communications issues continue to arise in the context of compliance incidents (see, for example, NSA Incident [redacted] in which an incorrect [redacted] was tasked based on a miscommunication in an oral conversation between NSA and CIA; no data was acquired as a result of the incident), the joint oversight team assesses that these issues accounted for only a handful of compliance incidents during this reporting period.

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

(U) C. Effect of Technical Issues

(U) There were a small number of compliance incidents resulting from technical issues during this reporting period, but technical issues can have larger implications than other incidents because they often involve more than one 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 significant overcollection incidents[38] during this reporting period resulted from the efforts of all of the involved agencies.

[38] [redacted]

~~(U)~~ The most substantial compliance incidents involving technical issues during this reporting period resulted from certain NSA technical systems such [redacted] system checks (e.g., post-tasking). These technical issues resulted in compliance incidents that affected numerous facilities. If a post-tasking method leads to the determination that a target has entered the United States, NSA analysts are responsible for ensuring all tasked facilities—including both electronic communications accounts and telephony identifiers—are detasked from collection. While these targets are non-United States persons, the joint oversight team recognizes that failures in post-tasking checks can lead to continued collection of a non-United States person now located in the United States [redacted] post-tasking check incidents were discovered in this reporting period. In each of [redacted] incidents, post-tasking checks did not operate as designed because NSA systems did not communicate with each other as intended.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

~~(U)~~ These types of technical issues highlight the complexity of the technical systems used to both conduct Section 702 acquisition and, in this reporting period, to verify that targets remain located outside the United States. In each of the three incidents discussed above, systems did not communicate with each other as intended, often due to unintended consequences to related systems that were caused by changes made to primary systems at points after they were initially designed. The joint oversight team believes that the lessons that should be drawn from these incidents 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. The [redacted] post-tasking incidents was discovered not because problems were apparent on their face, but because NSD realized that certain facts reported by NSA in the normal course of reporting instances [redacted] by Section 702 targets suggested that something may have been awry with NSA's [redacted] post-tasking check system. All agencies must remain similarly attuned to factual situations that indicate that technical systems may not be operating as intended.

(U) D. Effect of Human Errors

(U) As reported in previous Assessments, human errors have often caused many of the compliance incidents. Some of these errors are isolated events that do not lend themselves to categorization or development of standard processes. For example, there were instances of typographical errors or similar errors that occurred when NSA was entering the facility name into the collection system or at some earlier time in the targeting process.[41] The joint oversight team assesses that the overall rate of these types of errors is low reflecting the great care analysts use to

[41] [redacted]

enter information and the effectiveness of the NSA pre-tasking review process in catching potential errors.

(U) Other errors, however, present patterns that could be addressed with new training, procedures or system modification reminders. As was the case in the last several reporting periods, one of the most common errors in this reporting period involved situations where a target who used multiple facilities tasked to Section 702 or Executive Order 12333 collection was discovered to be in, or known to be traveling to, the United States, and some of the Section 702 facilities were missed in the detasking process.[42] Most of these detasking delays were quickly identified and remedied. However, the joint oversight team remains concerned that these types of detasking delays involving multiple facilities continue to happen with consistent frequency.

~~(U//FOUO)~~ Ensuring that facilities are detasked when a target enters the United States requires not only that analysts be attentive, but also that they have access to accurate and up-to-date tasking records [redacted] tasked for a particular target, [redacted] The joint oversight team assesses that this linkage problem needs to be addressed to prevent future situations where some of a target's facilities are not promptly detasked, as required by the NSA targeting procedures. This is also one of the many instances in which good compliance practice is also good intelligence practice – ensuring that NSA has up-to-date, accessible, and accurate corporate records of all of the known communication facilities used by the targets of its acquisitions will also facilitate the analysis and production of foreign intelligence information. NSA has reported that it is examining how NSA targeting databases can be better used to centralize knowledge regarding all of a target's known facilities, which could have prevented some of the detasking delays. As noted in the previous Joint Assessment, the joint oversight team assesses that improved linkage among the various NSA databases should continue to be given high priority despite the challenges in improving this area. The joint oversight team notes that NSA has continued to work on improving linkages during the last reporting session, but the number of compliance incidents that still occur [redacted] demonstrates that this remains a persistent challenge.

(S//NF) Another persistent but correctable error involved [redacted]

[redacted]

42 [redacted]

43 [redacted]

~~(TS//SI//NF)~~ One human error was more systemic in nature insofar as it caused delays in NSA's purging of Section 702-acquired data related to multiple required purges. As discussed in the Section 707 Report, many of the compliance incidents required NSA to purge Section 702-acquired data from appropriate systems and, thus, the joint oversight team finds issues that negatively affecting the proper functioning of NSA's remedial purging of heightened concern. The first step in any required purge is to identify what data must be purged. NSA Incident [redacted] describes human errors that were made in identifying data to be purged from one of NSA's new data repositories [redacted] unintentionally under-inclusive because the individual performing the queries was not aware of a particular [redacted]. The identified data was subsequently purged. This incident shows that the implementation period of new systems or processes is more susceptible to human errors. Thus, the joint oversight team must continue to work closely with agencies who want to implement new systems prior to such implementation to ensure the agencies take appropriate steps, such as training and automated safety nets, to mitigate the chance of human error during the implementation period. The joint oversight must also work with agencies to ensure that they have processes in place that will check for human error after implementation and that those processes will include ways in which to quickly resolve any errors.

(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 [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 overall compliance incident rate during this reporting period declined slightly to 0.02%.

44 [redacted]

~~(S//NF)~~ Several of the incidents were relatively narrow in impact insofar as they were limited to process errors involving individual targeting decisions. For example, [redacted]) during this reporting period concerned errors in the processing of requests [redacted] for accounts, where FBI did not properly complete a [redacted] required by FBI's targeting procedures. In each case, the required [redacted] and in neither of these cases was anything discovered that undermined FBI's targeting determination that the target was a non-United States person reasonably believed to be located outside the United States. In another incident ([redacted]), a tasking error occurred when FBI approved the Section 702 [redacted] from an e-mail account where there was information suggesting that the user may have been a United States person [redacted]

~~(S//NF)~~ FBI Incident [redacted] involved a technical system error with potentially broader implications to the application of FBI's targeting procedures. More specifically, FBI determined that a new system [redacted] Like some of the NSA incidents discussed above, this incident highlights the need for agencies to continually ensure that interrelated systems, particularly new or modified systems, continue to operate as intended.

~~(S//NF)~~ The remaining incidents were the result of non-compliance of FBI's minimization procedures. FBI Incident [redacted] involved FBI's storage of Section 702-acquired data in repositories that did not have the capabilities and restrictions required by FBI's Section 702 minimization procedures. [redacted]

[redacted]

(S//NF) [redacted] involved the improper dissemination of Section 702-acquired United States person information in violation of FBI's minimization procedures.[45] For example, [redacted] NSD and ODNI assessed that, based on the totality of the facts, FBI did not properly conclude that, at the time of the dissemination, each of the presumed United States person recipients of the e-mail message were [redacted] or that these identifiers otherwise constituted foreign intelligence information or were necessary to understand foreign intelligence information.

(S//NF) Although [redacted] targeting incidents involve onl [redacted] FBI authorized during this reporting personnel, FBI personnel [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 [redacted] incidents of noncompliance by an electronic communication service provider with a Section 702(h) directive. These incidents of non-compliance involved the overproduction of Section 702-acquired data by the service providers and these incidents were discovered by the Government and reported to the service providers. 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 low number of compliance incidents caused by service providers, and the speed with which the Government identified issues when they did occur,

45 [redacted]
46 [redacted]

indicates that the Government is effectively monitoring the acquisitions from the service providers. The Government must continue to work with the service providers to prevent future incidents.

(TS//SI//NF) [redacted] provider incidents involved the overproduction of data by an electronic communication service provider. As described in the Section 707 report [redacted]

[redacted]

48 [redacted]

[redacted]

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

(U) SECTION 5: CONCLUSION

(U) 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, including maintaining close monitoring of collection activities and a continued focus on 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).

[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 (also referred to as selectors) 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" or "selector" 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 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 initially 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 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

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

(U) 2. Electronic Communications Identifiers

~~(S//SI//NF)~~ For electronic communications identifiers, NSA analysts may [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 review information 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 collection for the facility. NSA analysts are expected to review this collection within five business days to confirm

[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]

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.

~~(S//SI//NF)~~ NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular "selector" (i.e. 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 "selector" (i.e. 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 selector (i.e. facility) 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 "selector" (i.e. 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 direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, with program external focus and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts . 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 to identify foreign intelligence targets to NSA for the acquisition of in-transit communications , including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to NSA for tasking.

(S//NF) The 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 wil [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.