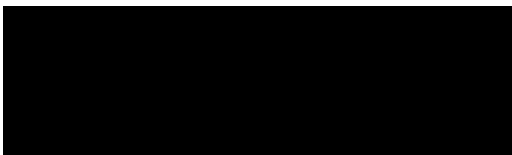




(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: December 1, 2014 – May 31, 2015

February 2016



**(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**

**February 2016**

**TABLE OF CONTENTS**

(U) Executive Summary	3
(U) Section 1: Introduction	4
(U) Section 2: Oversight of the Implementation of Section 702	6
(U) I. Joint Oversight of NSA	7
(U) II. Joint Oversight of CIA	9
(U) III. Joint Oversight of FBI	10
(U) IV. Joint Oversight of NCTC	13
(U) V. Interagency/Programmatic Oversight	13
(U) VI. Training	14
(U) VII. The Privacy and Civil Liberties Oversight Board	14
(U) Section 3: Trends in Section 702 Targeting and Minimization	15
(U) I. Trends in NSA Targeting and Minimization	15
(U) II. Trends in FBI Targeting	20
(U) III. Trends in CIA Minimization	22
(U) Section 4: Compliance Assessment – Findings	26
(U) I. Compliance Incidents – General	26
(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures	33
(U) III. Review of Compliance Incidents – CIA Minimization Procedures	41
(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures	42
(U) V. Review of Compliance Incidents – Provider Errors	43
(U) Section 5: Conclusion	44
(U) Appendix A	A-1

**(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**

**February 2016**

**Reporting Period: December 1, 2014 – May 31, 2015**

**(U) EXECUTIVE SUMMARY**

(U) The FISA Amendments Act of 2008 (hereinafter “FAA”) requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended, (hereinafter “FISA” or “the Act”) and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting and minimization procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the fourteenth joint compliance assessment of the Section 702 program. This assessment covers the period from December 1, 2014, through May 31, 2015 (hereinafter the “reporting period”) and accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was submitted as required by Section 707(b)(1) of FISA (hereinafter “the Section 707 Report”) on September 3, 2015, which covered the same reporting period.

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

(U) This Joint Assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities and to impose internal controls for compliance and verification purposes. The compliance incidents that occurred during this reporting period represent a very small percentage (0.35%) of the overall collection activity. This represents a decrease from the last Joint Assessment’s rate of 0.37%. Individual incidents, however, can have broader implications, as further discussed herein and in the Section 707 Report. Based upon a review of these compliance incidents, the joint oversight team believes that none of these incidents represent an intentional attempt to circumvent or violate the Act, the targeting or minimization procedures, or the Attorney General’s Acquisition Guidelines.

**(U) SECTION 1: INTRODUCTION**

(U) The FISA Amendments Act of 2008 (hereinafter, “FAA”) requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended (hereinafter, “FISA” or “the Act”), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter, “Section 702”) have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI’s fourteenth joint compliance assessment under Section 702, covering the period December 1, 2014, through May 31, 2015 (hereinafter, the “reporting period”).<sup>1</sup>

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

An acquisition authorized under subsection (a)—

- (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

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

---

<sup>1</sup> (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on September 3, 2015, as required by Section 707(b)(1) of FISA, and covers the same reporting period.

(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.<sup>2</sup> 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 FBI pursuant to Section 702 of FISA, as amended.”<sup>3</sup>

(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 Two also briefly discusses the July 2014 Section 702 Report by the Privacy and Civil Liberties Oversight Board. Section Three compiles and presents data acquired from the joint oversight team’s compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the Section 707 Report. As with the prior Joint Assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent recurrences.

(U) In summary, the joint oversight team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and

2



<sup>3</sup> (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).

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. In its ongoing efforts 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 enhance monitoring of purge practices and systems and withdrawal of disseminated reports as may be required. Further, the joint oversight team will also continue to monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report. As appropriate, this Joint Assessment provides updates on these on-going efforts.

**(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<sup>4</sup> each handle Section 702-acquired data in accordance with their own minimization procedures.<sup>5</sup> 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 each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

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

---

<sup>4</sup> (U) As discussed herein, CIA receives Section 702-acquired data from NSA and FBI.

<sup>5</sup> (U) The DNI released, in redacted form, NSA's, FBI's, and CIA's 2014 minimization procedures on ODNI's *IC on the Record* website as part of its SIGINT Intelligence Reform 2015 Anniversary Report (hereinafter the "2015 Anniversary Report"). These three sets of released minimization procedures are in the 2015 Anniversary Report's section entitled "Strengthening Privacy and Civil Liberties" under New Privacy Protections for Information Collected Under Section 702. Each agencies targeting and minimization procedures are approved by the Attorney General and reviewed by the Foreign Intelligence Surveillance Court.

**(U) I. Joint Oversight of NSA**

(U) Under the process established by the Attorney General and Director of National Intelligence’s certifications, all Section 702 targeting is initiated pursuant to the NSA’s targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities<sup>6</sup> 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,<sup>7</sup> 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**

<b>Date of Review</b>	<b>Taskings/Minimization Reviewed</b>
<b>February 24, 2015</b>	December 1, 2014 – January 31, 2015
<b>May 1, 2015</b>	February 1, 2015 – March 31, 2015
<b>June 19, 2015</b>	April 1, 2015 – May 31, 2015

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

(U) The joint oversight review process for NSA targeting begins well before the onsite review. Prior to each review, NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the review period to NSD and ODNI. Members of the joint oversight team review tasking sheets and then NSD prepares a detailed report of the findings, which they share with the ODNI members of the joint oversight team. During this initial review, the joint oversight team determines whether the tasking sheets meet the documentation standards required by NSA’s targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA’s foreignness determinations. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that did not provide sufficient information and requests additional information.

---

<sup>6</sup> (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities, including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. A fuller description of the Section 702 targeting process may be found in the Appendix.

<sup>7</sup> (U) NSA’s targeting procedures require that the onsite reviews occur approximately every two months.



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

(U) The joint oversight team also reviews NSA's minimization of Section 702-acquired data. NSD reviews all of serialized reports, with ODNI reviewing a sample that NSA has disseminated and identified as containing Section 702-acquired United States person information. The team also reviews a sample of serialized reports that NSA has disseminated and identified as containing Section-702 acquired *non*-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.

(U) With respect to queries of Section 702-acquired content using a United States person identifier, the joint NSD and ODNI oversight team review all approved United States person identifiers to ensure compliance with the minimization procedures. For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the duration for which the United States person identifier has been authorized to be used as a query term, and any other relevant information. In addition, with respect to queries of Section 702-acquired metadata using a United States person identifier, NSA's internal procedures require that NSA analysts document the basis for each metadata query prior to conducting the query. NSD reviews the documentation for 100% of the metadata queries that NSA provides to NSD.

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be incidents of non-compliance. For example, NSA is required to report all instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target's travel to the United States.<sup>8</sup> The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. Investigations of all of these incidents sometimes result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the

---

<sup>8</sup> (U) If NSA had no prior knowledge of the target's travel to the United States and, upon learning of the target's travel, immediately "detasked" (*i.e.* stopped collection against) the target's facility, as is required by NSA's targeting procedures, then the collection while the target was in the United States would not be considered a compliance incident under NSA's targeting procedures, although the collection would generally be subject to purge under the applicable minimization procedures. The joint oversight team carefully considers and, where appropriate, obtains additional facts regarding every reported detasking decision to ensure that NSA's collection and detasking complied with its targeting and minimization procedures.



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 or acquisition, it does nominate potential Section 702 targets to NSA. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team conducts onsite visits at CIA and the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities.

(U) The onsite reviews also focus on CIA’s application of its Section 702 minimization procedures. For this reporting period, NSD and ODNI conducted the following onsite reviews at CIA:

**Figure 2: (U) CIA Reviews**

<b>Date of Visits</b>	<b>Minimization Reviewed</b>
<b>March 2 and 4, 2015</b>	December 1, 2014 – January 31, 2015
<b>May 4 and 6, 2015</b>	February 1, 2015 – March 31, 2015
<b>June 25 and July 1, 2015</b>	April 1, 2015 – May 31, 2015

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 CIA’s 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.

(S//NF)<sup>9</sup> CIA may receive [REDACTED]<sup>10</sup> unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. [REDACTED] as further described in detail in Appendix A, CIA nominates potential Section 702 targets to NSA. [REDACTED] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [REDACTED] the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA's minimization procedures, the Attorney General Acquisition Guidelines, or other agencies' procedures in which CIA is involved.<sup>11</sup> Investigations are coordinated through the CIA FISA Program Office and CIA's Office of General Counsel (CIA OGC), and when necessary, may involve requests for further information, meetings with CIA legal, analytical, and/or technical personnel, or the review of source documentation. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC through quarterly reports or individualized notices.

(U) **III. Joint Oversight of FBI**

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

(S//NF) More specifically, FBI provides [REDACTED]  
Pursuant to its own authority, FBI is authorized [REDACTED] from electronic

---

<sup>9</sup> (U//FOUO) This paragraph carried a different portion marking in prior joint assessments (those joint assessments have not been publicly released). We are continuing to review the information in this paragraph to determine the proper portion marking (in anticipation of publicly releasing, in redacted form, this and prior joint assessments). In the meantime, the portion-marking of this paragraph has been upgraded.

<sup>10</sup> [REDACTED] This footnote carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this footnote to determine the proper portion marking, but, in the meantime, the portion-marking of this footnote has been upgraded.

<sup>11</sup> (S//NF) 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. This footnote carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this footnote to determine the proper portion marking, but, in the meantime, the portion-marking of this footnote has been upgraded.

communication service providers by targeting facilities that NSA designates (hereinafter “Designated Accounts”). FBI conveys [REDACTED] from the electronic communications service providers to [REDACTED] for processing in accordance with the agencies’ FISC-approved minimization procedures.

(S//NF)<sup>12</sup> Third, [REDACTED] FBI may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI’s Section 702 minimization procedures. Like CIA, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

(U) FBI’s internal compliance program and NSD and ODNI’s oversight program are designed to ensure FBI’s compliance with statutory and procedural requirements for each of these three roles. Each of the roles discussed above, as well as FBI’s internal compliance program, are set forth in further detail in Appendix A.

(U) NSD and ODNI generally conduct monthly reviews of FBI’s compliance with its targeting procedures and bimonthly 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**

<b>Date of Visit</b>	<b>Targeting and Minimization Reviewed</b>
<b>February 25, 2015</b>	December 2014 targeting decisions
<b>March 25, 2015</b>	January 2015 targeting decisions and December 1, 2014 through January 31, 2015, minimization decisions
<b>April 29, 2015</b>	February 2015 targeting decisions and February 1 through March 31, 2015, minimization decisions
<b>May 20, 2015</b>	March 2015 targeting decisions
<b>June 11, 2015</b>	April 2015 targeting decisions and April 1 through May 31, 2015, minimization decisions
<b>June 24, 2015</b>	May 2015 targeting decisions

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.<sup>13</sup> The joint oversight team also reviews a sample of other files to

<sup>12</sup> (U//FOUO) This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

<sup>13</sup> (S//NF) Supporting document includes, among other things, [REDACTED]. The joint oversight team reviews every file identified by FBI [REDACTED]

identify any other potential compliance issues. FBI analysts, supervisory personnel, and attorneys from FBI's Office of General Counsel (FBI OGC) 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 Section 702 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 non-publicly available information concerning unconsenting 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<sup>14</sup> in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During these field office reviews, NSD also audits a sample of FBI personnel queries in systems that contain unminimized Section 702 collection. As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at 13 FBI field offices between December 1, 2014, and May 31, 2015, and reviewed [REDACTED] involving Section 702-tasked facilities. These reviews are further discussed in Section IV below.

(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 on May 12, 2015. That review revealed no issues with the process used by FBI's [REDACTED]

(S//NF)<sup>15</sup> As further described in detail in Appendix A, FBI nominates potential Section 702 targets to NSA. [REDACTED]

[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.

---

<sup>14</sup> (U) ODNI is able to join NSD at a subset of reviews conducted in FBI field offices outside the Washington, D.C., area. ODNI receives written summaries from NSD regarding all reviews.

<sup>15</sup> (U//FOUO) This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

(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.<sup>16</sup> 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.

**(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 22, 2014, NSD and ODNI conducted a review of NCTC's access, receipt, and processing of Section 702 information received from FBI. The report of this review, which concluded that NCTC's systems and process complied with the NCTC's Section 702 minimization procedures, has previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

**(U) V. Interagency/Programmatic Oversight**

(U) Because the implementation and oversight of the Government's Section 702 authorities are 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 twice monthly telephone calls and quarterly meetings (in addition to ad hoc calls and meetings on specific topics as needed) with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures.

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

---

<sup>16</sup> (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.

minimization procedures, as well as to some related internal guidance, based on recommendations made by the Privacy and Civil Liberties Oversight Board.

**(U) VI. Training**

(U) In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have also continued their training efforts to ensure compliance with the targeting and minimization procedures. NSA continued to administer the compliance training course implemented in the prior reporting period. All NSA personnel are required to complete this course on an annual basis in order to gain access to raw Section 702 acquisitions. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. NSA also began designing new training reminders in November 2015 (which, although outside this Joint Assessment's reporting period, is included herein for context) on an internal agency website where personnel could obtain information about specific types of Section 702-related issues and compliance matters. CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a training program that provides hands-on experience with handling and minimizing Section 702-acquired data. During this reporting period, CIA centralized its FISA training to provide greater consistency and added a program that provides greater depth on the Section 702 nomination process. FBI has similarly continued implementing its online training programs regarding nominations, minimization, and other requirements. Completion of these FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI have also conducted in-person trainings at multiple FBI field offices. For example, during this current reporting period, NSD and FBI provided additional focused training at FBI field offices on the Section 702 minimization procedures, including the attorney-client privileged communication provisions of FBI's minimization procedures.<sup>17</sup>

**(U) VII. Privacy and Civil Liberties Oversight Board**

(U) In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on the Section 702 program entitled, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (PCLOB's Section 702 Report). According to page 2 of the PCLOB's Section 702 Report:

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702

---

<sup>17</sup> (U) This specific training began before and continued after the current reporting period of December 2014 – May 2015.



program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program's implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons' communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

(U) The Government made revisions to the relevant 2015 targeting and minimization procedures in response to the PCLOB's recommendations. Subsequently, the FISC, after the appointment of an amicus curiae, found that those revised procedures complied with Section 702 and were consistent with the requirements of the Fourth Amendment in an opinion.<sup>18</sup> Because the continuation and completion of the Government's efforts to address the PCLOB's recommendations occurred outside this Joint Assessment's reporting period, these efforts will be addressed in the next appropriate Joint Assessment(s).

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

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

#### **(U) I. Trends in NSA Targeting and Minimization**

(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,<sup>19</sup> the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities

---

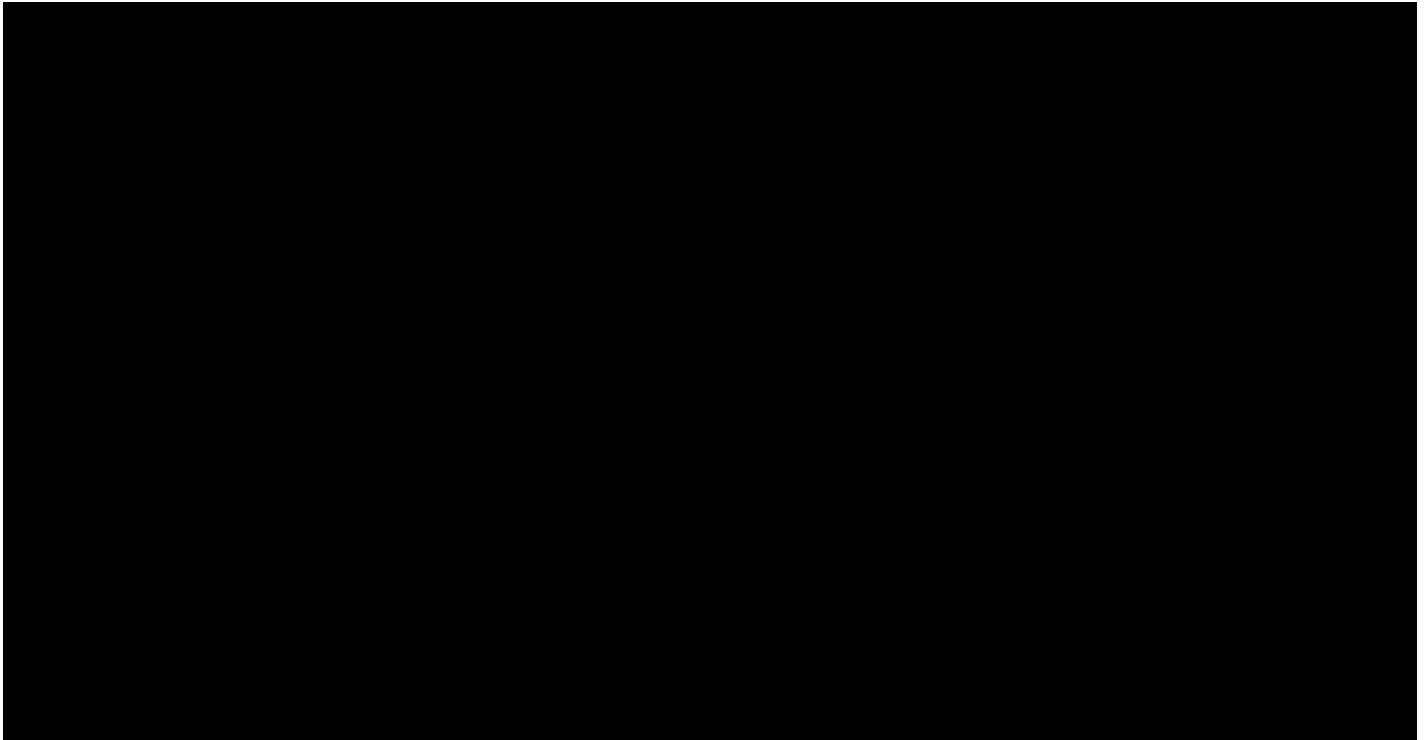
<sup>18</sup> (~~S//NF~~) These procedures were filed with the FISC as part of the 2015 Certifications renewal application, which the FISC approved on November 6, 2015. The ODNI plans to publicly post the Court's opinion, in redacted form, on its website IC On The Record.

<sup>19</sup> (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). Subsequently, on April 22, 2015, ODNI released its 2014 Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities (hereafter the 2014 Transparency Report). The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified number provided in both the 2013 and 2014 Transparency Reports estimate the number of Section 702 *targets*. As noted in both the Transparency Reports, the "number of 702 'targets' reflects an estimate of the number of known users of particular facilities subject to intelligence collection under those Certifications." Furthermore, the classified numbers of facilities account for the number of facilities subject to Section 702 acquisition *during the current six month reporting period* (June 1, 2014 – November 30, 2014), whereas the Transparency Reports estimate the number of targets affected by Section 702 *during the calendar year* (e.g. 2013 and 2014).



under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.

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



~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [redacted] facilities were under collection [redacted] on any given day during the reporting period. This represents a 9.3% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period. [redacted]

(U) The above statistics describe the average number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.<sup>20</sup> Classified Figure 5 charts the total monthly

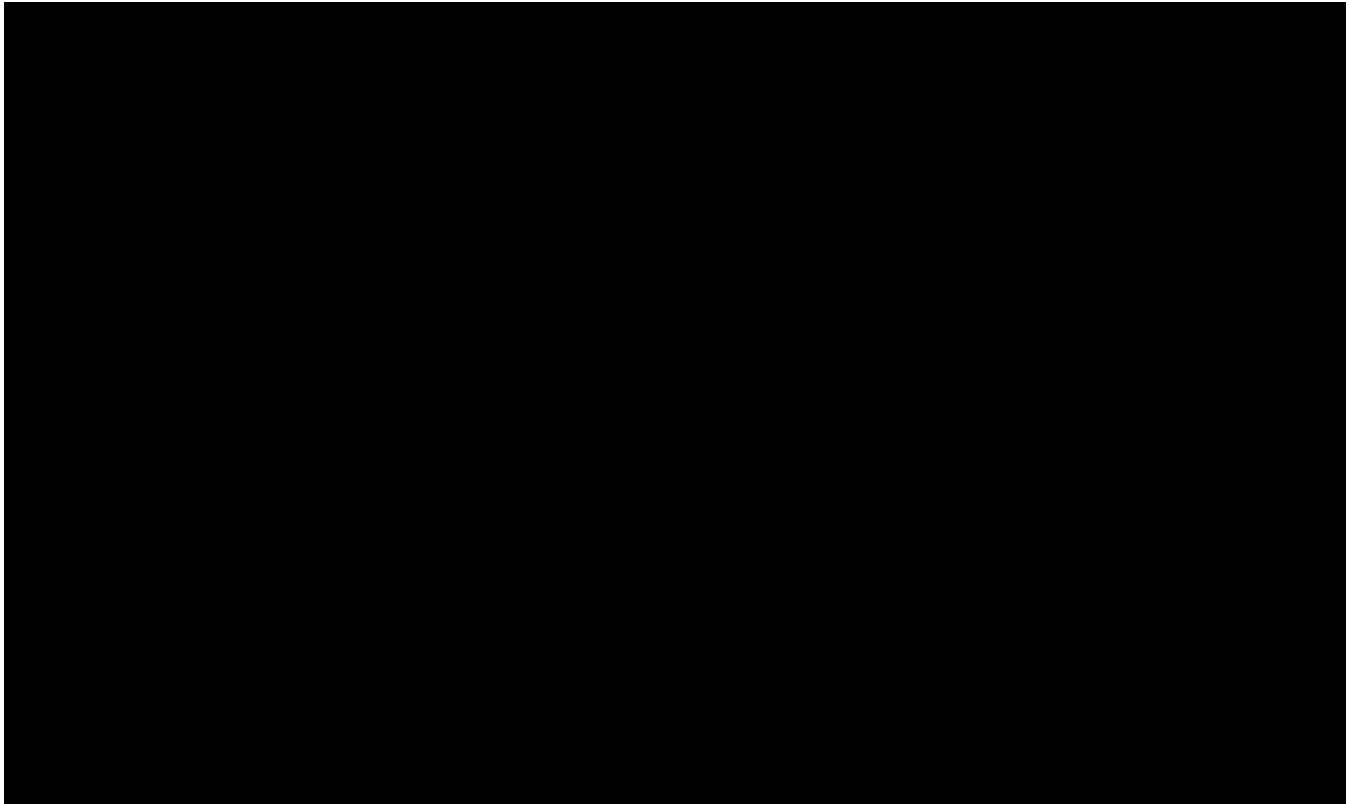
---

<sup>20</sup> (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.



numbers of newly tasked facilities since collection pursuant to Section 702 began in September 2008.<sup>21</sup>

**Figure 5: ~~(TS//SI//NF)~~ New Taskings by Month (Yearly Average for 2008 through November 2014)**



~~(TS//SI//NF)~~ Specifically, NSA provided documentation of [REDACTED] new taskings during the reporting period. This represents a 1.6% increase in new taskings from the previous reporting period. [REDACTED]

~~(TS//SI//NF)~~ NSA tasked an average [REDACTED] telephony facilities each month in 2014. During the first five months of 2015, NSA has tasked an average of [REDACTED] telephony facilities. This represents a [REDACTED] increase in the average monthly telephony facilities in the first five months of 2015 compared to 2014.

~~(TS//SI//NF)~~ As a year-over-year measure, the average number of electronic communication accounts tasked by NSA increased through 2013, but decreased slightly in 2014.

---

<sup>21</sup> (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.

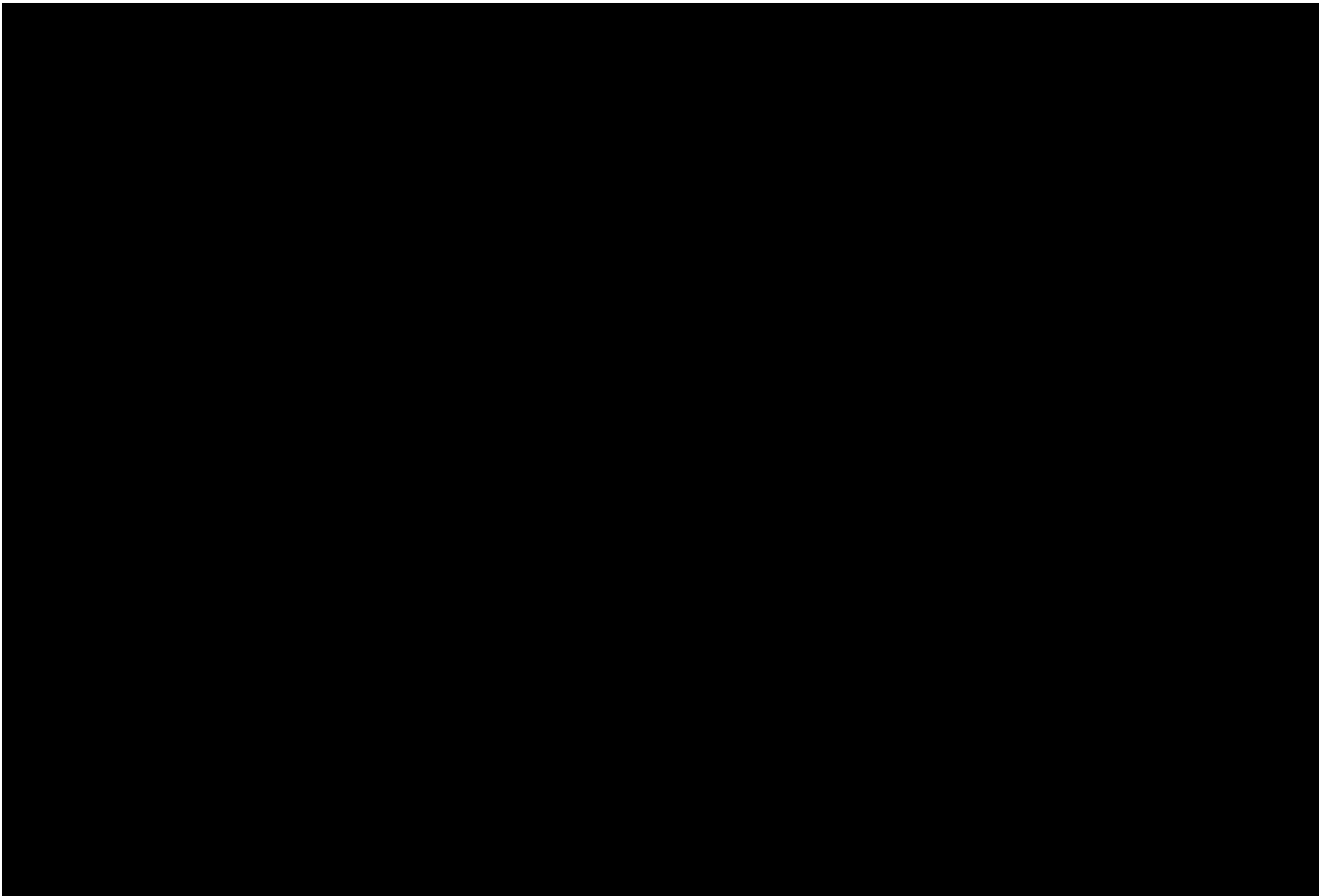
Specifically, NSA tasked an average of [REDACTED] electronic communications accounts each month in 2014 ([REDACTED] decrease from the average number of taskings in 2013). However, NSA tasked an average of [REDACTED] electronic communication accounts during the first five months of 2015 ([REDACTED] increase from 2014's monthly average and [REDACTED] increase from 2013's monthly average). NSA advises that the decrease in 2014 was at least partially due to [REDACTED]

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702- or Protect America Act (PAA)-acquired data, and provided NSD and ODNI access to all reports NSA identified as containing United States person information. Figure 6 contains the classified number of serialized reports and reports identified as containing United States person information over the last seven reporting periods. NSD and ODNI's review revealed that the United States person information was at least initially masked in the vast majority of circumstances.<sup>22</sup> The number of serialized reports NSA has identified as containing United States person information has also increased, but generally at a lower rate than the overall increase in reporting. As a result, the percentage of reports containing United States person information in this reporting period is the lowest it has been in the last eight reporting periods.

---

<sup>22</sup> (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.

**Figure 6: ~~(TS//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)~~ Specifically, in this reporting period NSA identified to NSD and ODNI [REDACTED] serialized reports based upon minimized Section 702- or Protect America Act (PAA)-acquired data. This represents a 3.1% increase from the [REDACTED] such serialized reports NSA identified in the prior reporting period. Figure 6 reflects NSA reporting over the last eight reporting periods; the fact that reporting based on Section 702 or PAA-acquired data increased is consistent with prior reporting periods.

~~(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.<sup>23</sup> The percentage of reports containing United States person information was

---

<sup>23</sup> ~~(C//NF)~~ NSA does not maintain records that allow it to readily determine, in the case of a report that includes information from several sources, from which source a reference to a U.S. person was derived. Accordingly, the references to U.S. person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.

slightly lower this reporting period (9.7%), than the 9.8% reported in the two prior reporting periods.

**(U) II. Trends in FBI Targeting**

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA designated-facilities that FBI approved.<sup>24</sup> As detailed below, the number of facilities designated for acquisition has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.<sup>25</sup>

(U) As classified Figure 7 details, FBI approves the vast majority of NSA's designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA-designated facilities have already been evaluated and found to meet NSA's targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion<sup>26</sup> were rejected on the basis that they were ineligible for Section 702 collection.

(U) Between 2009 and December 2014, the *yearly average* of designated facilities approved by FBI steadily increased. Between January and May 2015, the *number* of designated facilities approved by FBI *each month* has varied. NSD and ODNI have continued to track the number of facilities approved by FBI in 2015 and will incorporate this information into future Joint Assessments.

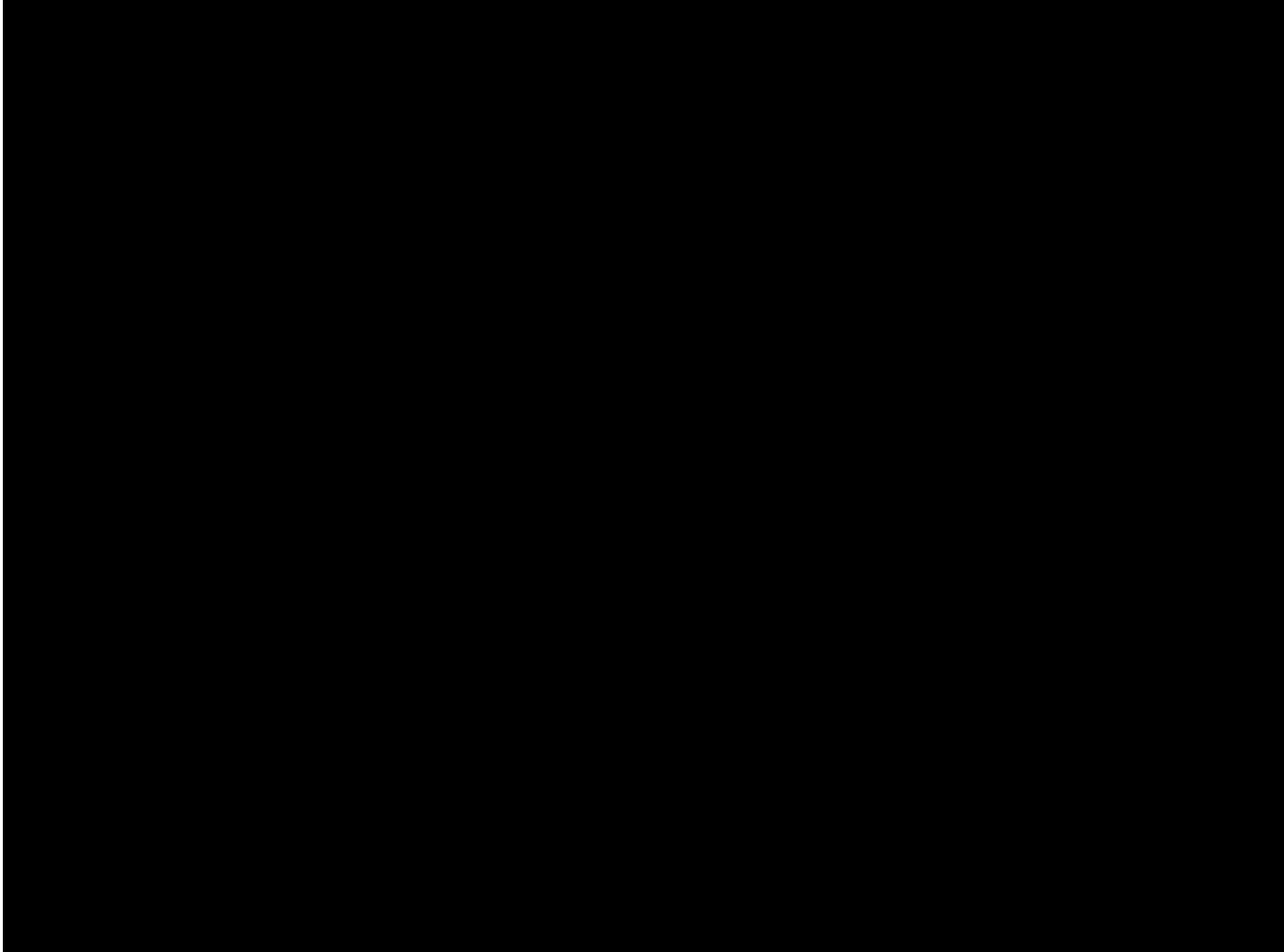
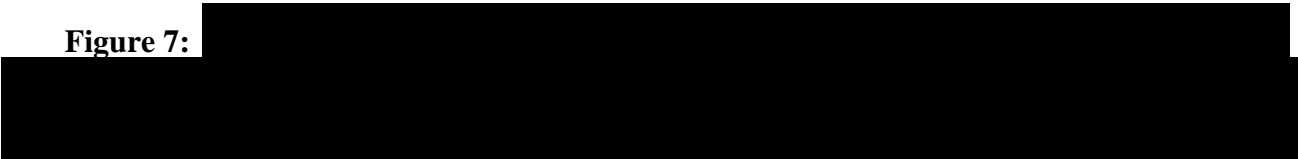
---

24

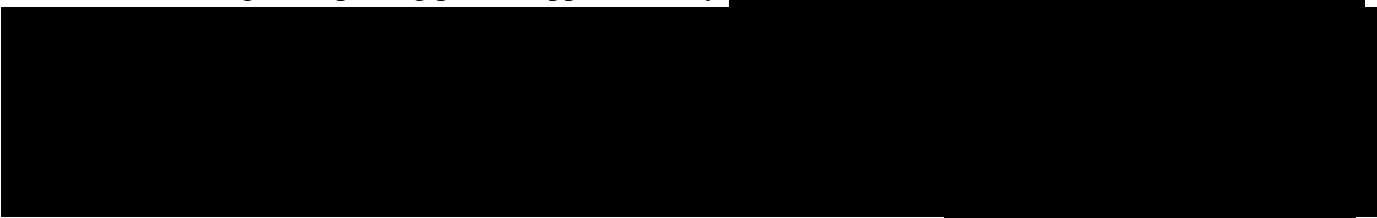
25

26

Figure 7:

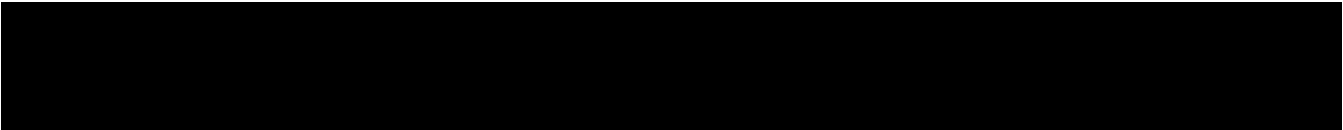


(TS//SI//NF) Specifically, FBI reports that NSA designated [redacted] accounts [redacted] [redacted] during the reporting period – an average of [redacted] designated accounts per month. This is a [redacted] increase from the [redacted] accounts designated in the prior six-month reporting period. Of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



(TS//SI//NF) FBI approved [redacted] requests for [redacted]





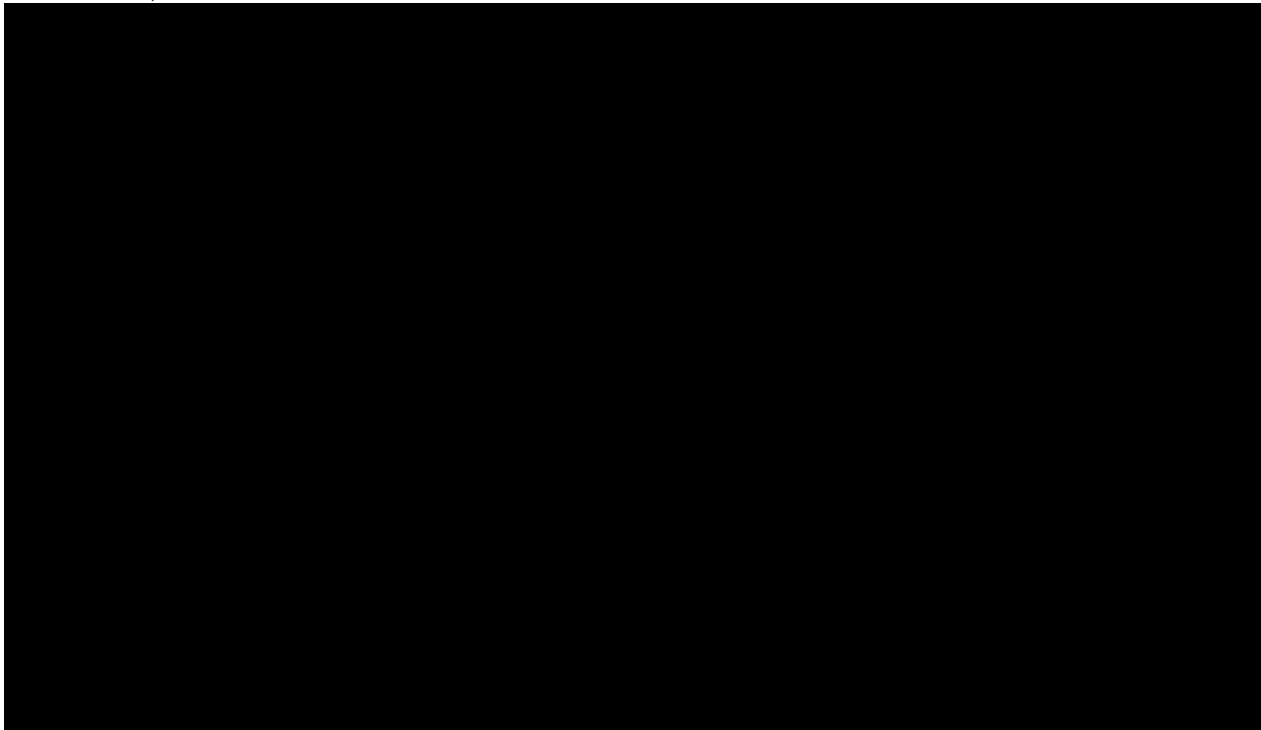
(U) As indicated in the prior Joint Assessment, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its dissemination of Section 702-acquired information from FBI Headquarters to FBI field offices. NSD conducts oversight reviews at FBI field offices each year, and during those reviews, NSD reviews a sample of the Section 702 disseminations issued by the respective field office. Because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of Section 702-acquired United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. § 1881a(l)(3)(i).

(U) **III. Trends in CIA Minimization**

(U) CIA only identifies for NSD and ODNI disseminations of Section 702 data containing United States person information. Classified Figure 8 compiles the number of such disseminations of reports containing United States person information identified in the last eight reporting periods (June-November 2011 through the current period of December-May 2015). In the first six reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the prior reporting periods, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the last reporting period, the number of CIA-identified disseminations containing United States person information again slightly decreased.



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



(S//NF) During this reporting period, CIA identified [redacted] disseminations of Section 702-acquired data containing minimized United States person information. This is a [redacted] decrease from the [redacted] such disseminations CIA made in the prior reporting period. [redacted] and as reported in prior Joint Assessments, CIA also permits some personnel with [redacted]

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

(U) CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. CIA's minimization procedures must be applied to these files before they are retained or transferred to systems with broader access.<sup>27</sup> Classified Figure 9 details the total number of files that were either retained or transferred, as well as the number of those

---

<sup>27</sup> (S//NF) [redacted] in making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

retained or transferred files that contain identified United States person information.<sup>28</sup> Beginning in the middle of the previous reporting period, CIA began reporting the number of files CIA transferred to systems with broader access, instead of the number of files retained in systems of limited access, as the number of transferred files provides a more accurate portrayal of CIA's use of Section 702-acquired information. This current assessment reports the total number of files CIA transferred from December 2014 through May 2015. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.<sup>29</sup> In all reporting periods, the number of retained or transferred files identified by CIA as potentially containing United States person information has been consistently a very small percentage of the total number of retained or transferred files.

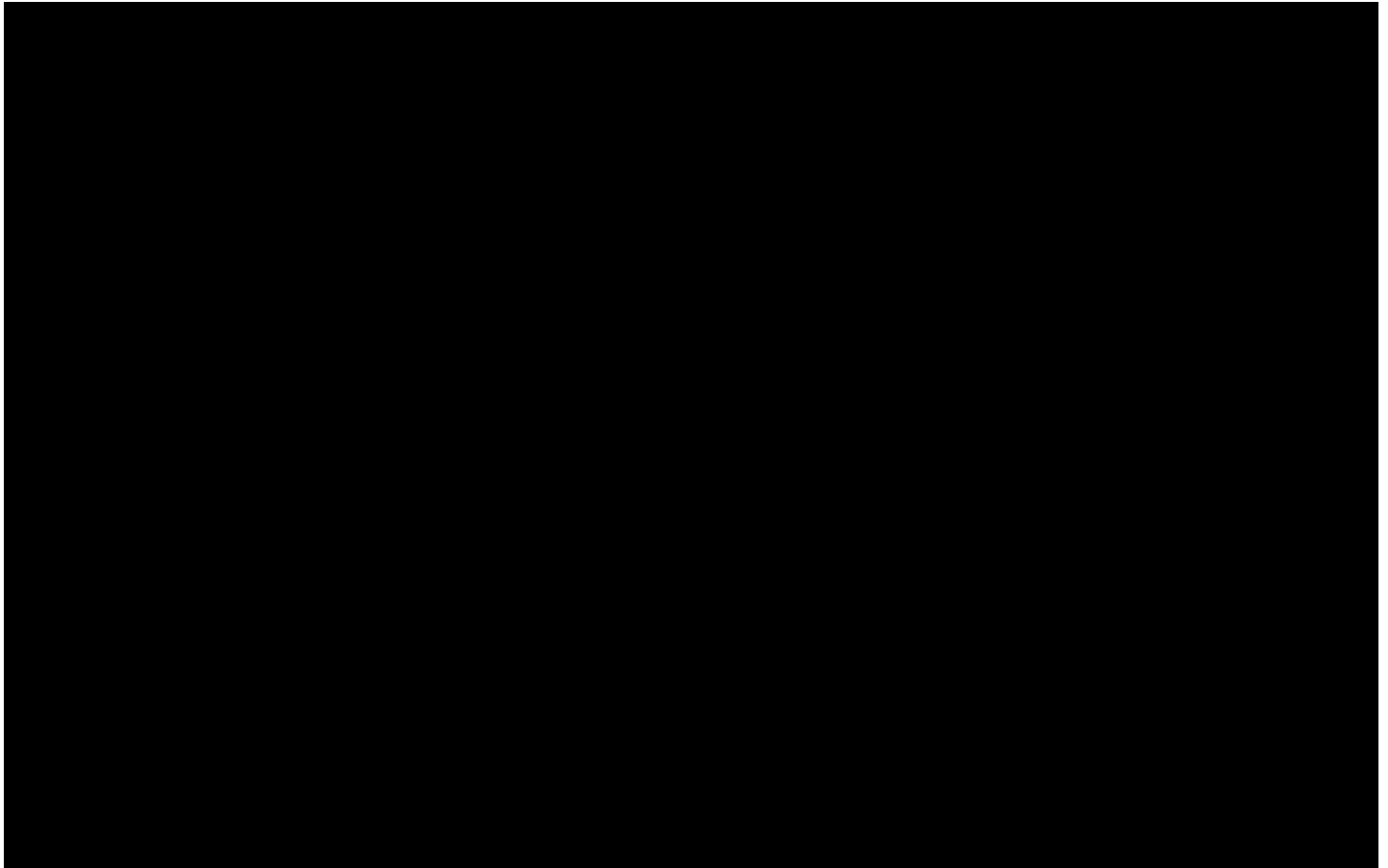
---

<sup>28</sup> (U) As reported in the eleventh Joint Assessment (October 2014), CIA determined in September 2014 that characterizations in prior assessments of the number of files having been "transferred" was not the most appropriate term as some files had been retained for long term retention but had not been transferred to systems of broader access. Consequently, the numbers of files for which CIA had made a retention decision were re-characterized as having been "retained." Because the terms transferred and retained attempt to describe the same authorized actions under CIA's Minimization Procedures, this Joint Assessment just refers to retention decisions.

<sup>29</sup>



**Figure 9: ~~(S//NF)~~ Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred Files Which Contained Potential United States Person Information**



(S//NF) For this reporting period, CIA analysts transferred [REDACTED] of which were identified by CIA as containing a communication with potential United States person information. This is a [REDACTED] increase in the number of files transferred, when compared to the previous reporting period when [REDACTED] of which contained potential United States person information.

**(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS**

(U) The joint oversight team finds that during this 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) Each of the compliance incidents for this current reporting period are described in detail in the corresponding Section 707 Report. The Joint Assessment provides NSD and ODNI's analysis of those compliance incidents in an effort to identify existing patterns or trends that might identify the underlying causes of those incidents. The joint oversight team then considers whether and how those underlying causes could be addressed through additional remedial or proactive measures and assesses whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures, some of which are detailed below, especially as it pertains to investigating whether additional and/or new system automation may assist in preventing compliance incidents.

**(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 NSA's targeting or minimization procedures and [REDACTED] compliance incidents involving noncompliance with FBI's targeting and minimization procedures; for a total of [REDACTED] incidents involving NSA and/or FBI procedures.<sup>30</sup> During this reporting period, there was one identified incident of noncompliance with CIA's minimization procedures, and [REDACTED] identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

---

<sup>30</sup> (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.

(U) The following table puts these compliance incidents in the context of the average number of facilities subject to acquisition on any given day<sup>31</sup> during the reporting period:

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

Compliance incidents during reporting period (December 1, 2014 – May 31, 2015)	[REDACTED]
Number of facilities on average subject to acquisition during the reporting period <sup>32</sup>	[REDACTED]
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.35%

(U) The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of 0.35% represents a slight decrease from the 0.37% compliance incident rate in the prior reporting period. As discussed in the prior Joint Assessment, the number of delays in notification of the joint oversight team decreased substantially. The number of notification delays continued to fall during this reporting period. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is actually 0.32% as compared with 0.34% for the prior period. This information is explained below and detailed in Figure 11 below.

(U) While the incident rate remains low, this percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States person information.<sup>33</sup>

---

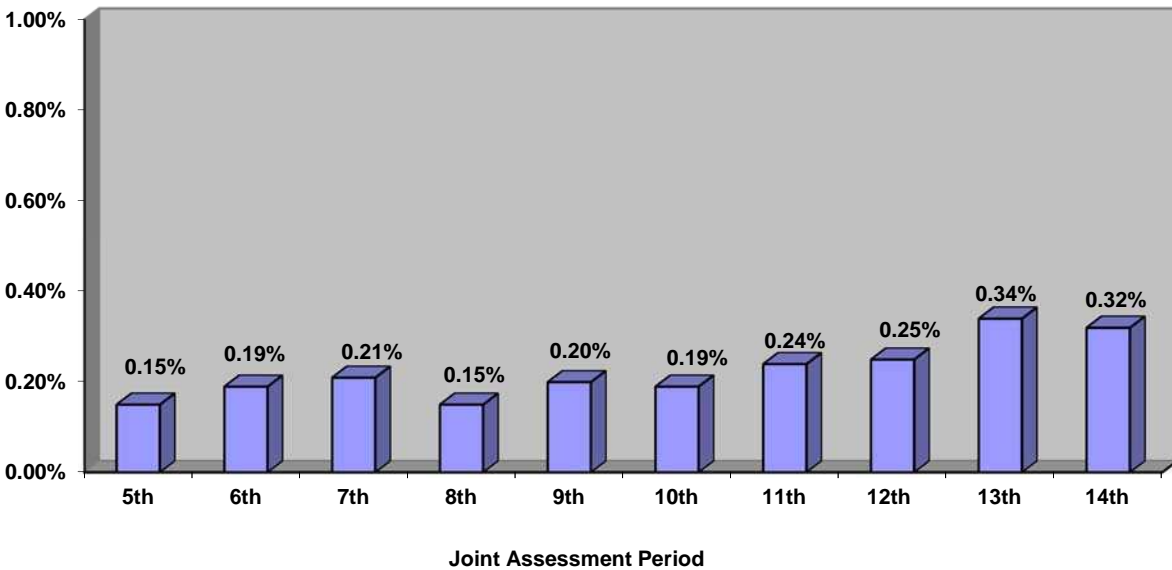
<sup>31</sup> [REDACTED] he Attorney General's Section 707 report provides further details with respect to any particular incident.

<sup>32</sup> (U) As detailed in the footnote above, the provided number of *facilities* on average subject to acquisition during the *current six month (which covers part of 2015)* reporting period remains classified and is different from the *calendar year* of the unclassified estimated number of *targets* affected by Section 702 released by ODNI in its public 2013 and 2014 Transparency Reports.

<sup>33</sup> (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) 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:

**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 0.32%, which is slightly below what was reported in the prior reporting period and still well below 1%. The joint oversight team assesses that the consistently low compliance incident rate of less than 1% is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures.

**(U) B. Categories of Compliance Incidents**

(U) Most of the compliance incidents occurring during the reporting period involved non-compliance with the NSA’s targeting or minimization procedures. This largely reflects the centrality of NSA’s targeting and minimization efforts 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.<sup>34</sup>
- (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." There were no instances of overcollection in this reporting period.
- (U) *Minimization Issues*. This category involves NSA's compliance with its minimization procedures.
- (U) *Other Issues*. This category involves incidents that do not fall into one of the six above categories.

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

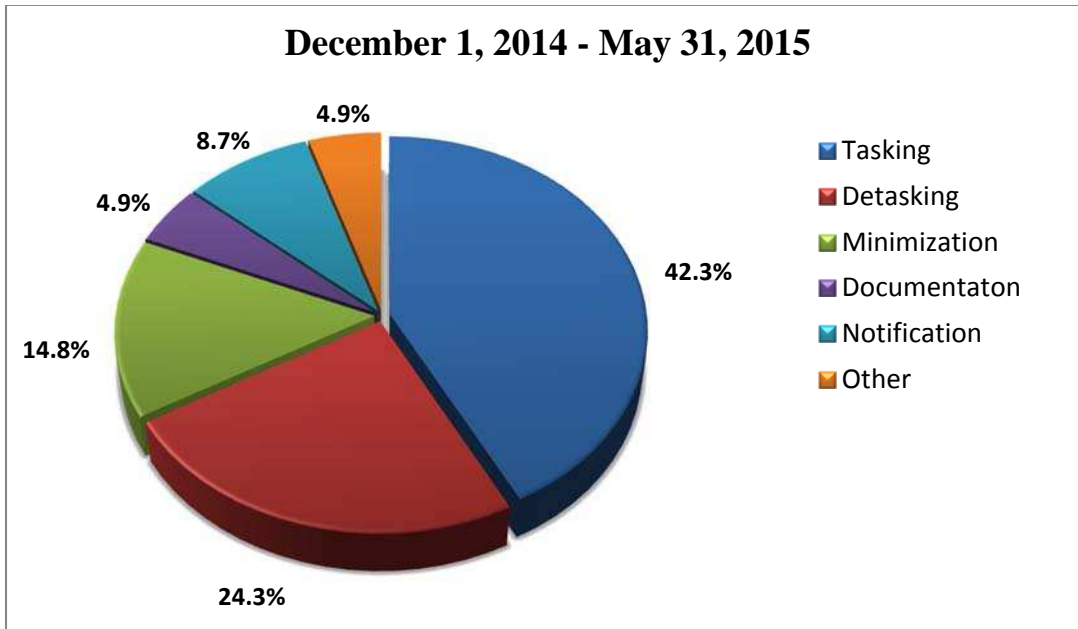
(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 12A depicts the percentage of compliance incidents in each category that occurred during this reporting period, whereas Figure 12B provides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

---

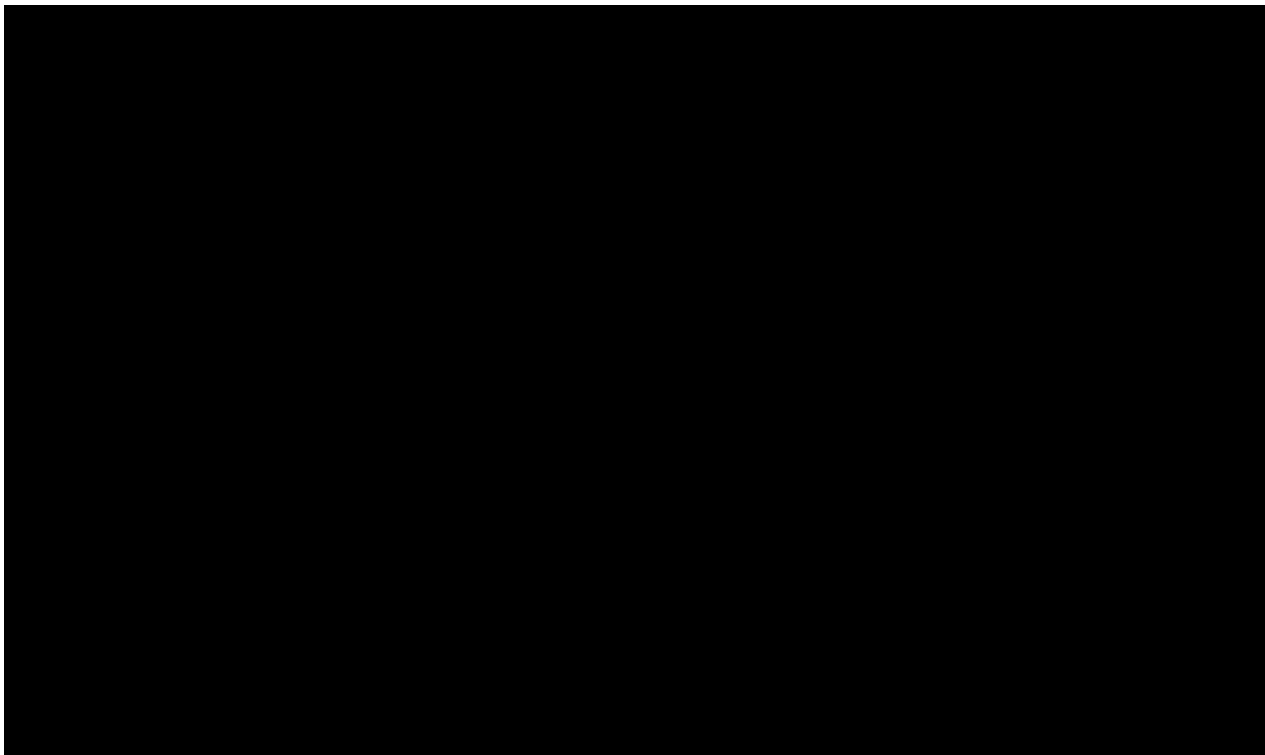
<sup>34</sup> (U) As described in the Section 707 Report, not all documentation errors are separately enumerated as compliance incidents.



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



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

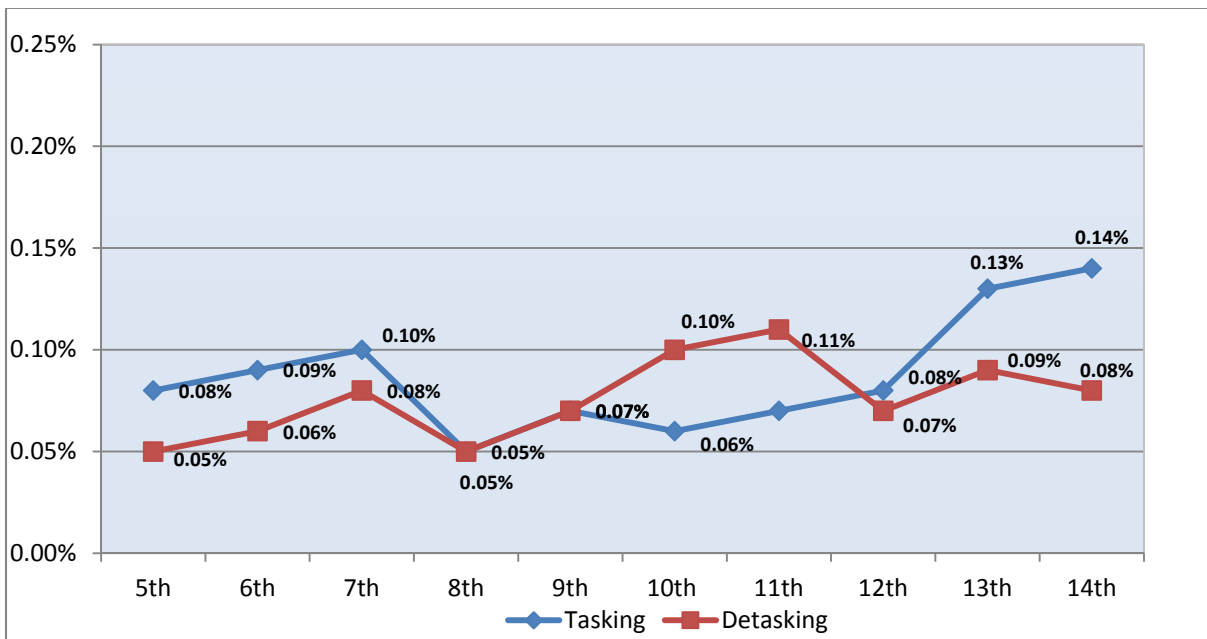


(U) As Figures 12A and B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, has been substantially reduced. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve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

(S//NF) More specifically, the number of tasking incidents increased [REDACTED]; [REDACTED] detasking incidents decreased [REDACTED]; minimization incidents decreased [REDACTED]; documentation incidents increased [REDACTED]; and “other” category incidents increased [REDACTED]. The number of notification delays increased [REDACTED]. Additionally, there were no overcollection incidents in the current reporting period, whereas there was one in the prior 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. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other, *i.e.* an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate.

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



(U) Over the time periods covered in the above chart, the tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection. Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United

States persons or persons located in the United States. On the other hand, detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.<sup>35</sup> The percentage of compliance incidents involving such detasking incidents has remained consistently low.<sup>36</sup>

(U) With respect to FBI's targeting and minimization procedures, incidents of non-compliance with the FBI targeting procedures decreased from the rate of 0.03% in the prior reporting period to the rate of 0.01% in the current reporting period.<sup>37</sup> The total number of identified minimization errors also remains low.<sup>38</sup> The joint oversight team assesses that FBI's overall compliance with its targeting and minimization procedures is a result of FBI's training and the processes it has designed to effectuate its procedures.

~~(S//NF)~~<sup>39</sup> Furthermore, there was one incident during this reporting period that involved CIA's minimization procedures, which represents a decrease from the [REDACTED] incidents that occurred during the previous reporting period for CIA. The joint oversight team assesses that CIA's compliance is a result of its training, systems and processes that were implemented when the Section 702 program was developed to ensure compliance with its minimization procedures, and the work of its internal oversight team.

~~(S//NF)~~<sup>40</sup> Finally, there were [REDACTED] incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents an increase from the single incident reported in the prior reporting period. The joint oversight team assesses that the low number of errors by the communications service providers is the result of continuous efforts by the Government and providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers' customers.

35 [REDACTED]

<sup>36</sup> (U) NSD and ODNI note that the above incident rates fluctuate by hundredths of a percentage point. Any perceived significant fluctuation is due to the scale of the graph (.00% to .25%). If, for example, the chart used a 0% to 1% scale to show fluctuations, the chart would show two virtually flat lines hugging the bottom. NSD and ODNI do not believe that any of different incident rates are statistically significant, and note that the incident rate is consistently quite low.

37 [REDACTED]

38 [REDACTED]

<sup>39</sup> ~~(U//FOUO)~~ This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

<sup>40</sup> ~~(U//FOUO)~~ This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

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

(U) As with the prior Joint Assessment, this Joint Assessment takes a broad approach and discusses the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The Joint Assessment primarily focuses on incidents involving NSA’s targeting and minimization procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA’s targeting and minimization procedures. Most of these incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-compliance with the NSA’s minimization procedures involving the unintentional improper dissemination, retention, or querying of Section 702 information.

(U) In the subsections that follow, this Joint Assessment examines some of the underlying causes of incidents of non-compliance focusing on incidents that have the greatest potential to impact United States persons’ privacy interests, albeit that those incidents represent a minority of the overall incidents. Different types of communication issues (*e.g.*, technical and system errors) are detailed and discussed below.<sup>41</sup> The joint oversight team believes that analyzing the trends of these incidents, especially in regards to their causes, help the agencies focus resources, avoid future incidents, and improve overall compliance.

**(U) A. Reverse Targeting**

(U) One of NSA’s tasking errors<sup>42</sup> involved the tasking of a facility that was used by a non-United States person located outside the United States that was determined to involve reverse targeting. Reverse targeting occurs when NSA tasks a communication facility used by a non-United States person reasonably located outside the United States for the purpose of acquiring the communications of a United States person or a person located in the United States. Reverse targeting is barred by statute and NSA policy and the prevention of reverse targeting is a key component of both the internal and external review of the Section 702 program.

~~(S//NF)~~ Among other things, Section 702 requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with Section 702’s targeting restrictions. The Attorney General’s Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1987, as Amended state, [REDACTED]

---

<sup>41</sup> (U) As with the prior Joint Assessment, this Assessment analyzes the underlying causes of compliance incidents while simultaneously evaluating how any compliance trends may potentially impact United States person privacy interests.

<sup>42</sup> [REDACTED]

the

guidelines prohibit reverse targeting of either persons located inside the United States, regardless of their nationality, or United States persons, regardless of their location.

(U) In this incident, the Attorney General authorized the targeting of the United States person pursuant to Section 705(b) of FISA. This reverse targeting incident resulted from an NSA analyst misunderstanding the reverse targeting prohibition and not because an NSA analyst intentionally attempted to violate Section 702 or NSA policy.<sup>43</sup> Despite the misunderstanding of law that caused this current incident, the joint oversight team assesses that the extreme rarity of reverse targeting incidents demonstrates the success of NSA's training efforts on this issue.

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

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

(U) In general, the joint oversight team found that better communication and coordination between and among the agencies reduced certain types of errors from occurring during this reporting period. Still, in this reporting period, miscommunications resulted in errors and the joint oversight team assesses that there is room for continued improvement: approximately 15% (down from the prior reporting period's 16%) of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.<sup>44</sup> Specifically, these detasking delays typically involved travel or possible travel of non-United States persons to the United States. Significantly, however, none of the inter- or intra-agency miscommunications resulted in the erroneous tasking, or the delay in the detasking, of a facility used by a United States person

43

44

(whereas [REDACTED] such incidents involving United States persons occurred during the previous reporting period).

(U) The joint oversight team believes that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its on-going oversight efforts, the joint oversight team will also continue to monitor NSA, CIA and FBI's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

**(U) C. Due Diligence and Pre-Tasking Information**

(U) During this reporting period and the prior reporting period, there were increases in the number of incidents involving the failure to conduct necessary foreignness checks or to otherwise exercise due diligence prior to the tasking of a facility. The joint oversight team is continuing to work with NSA to ensure that appropriate additional training efforts are utilized. Furthermore, and as mentioned in the prior Joint Assessment, the joint oversight team has continued to monitor NSA Section 702 activities and practices to ensure that NSA has a sufficient basis to task accounts.

(U) Approximately 64%<sup>45</sup> (last reporting period was approximately 43%) of the tasking errors in this reporting period involved instances in which NSA did not take sufficient pre-tasking steps to try to find information regarding the location of the targeted user or otherwise did not properly establish a sufficient basis to assess that the targeted user was outside the United States.<sup>46</sup> The two most common examples include situations in which the analyst did not conduct a necessary pre-tasking check<sup>47</sup> or there was too long of a delay between the necessary pre-tasking checks and the actual tasking of the account.<sup>48</sup>

---

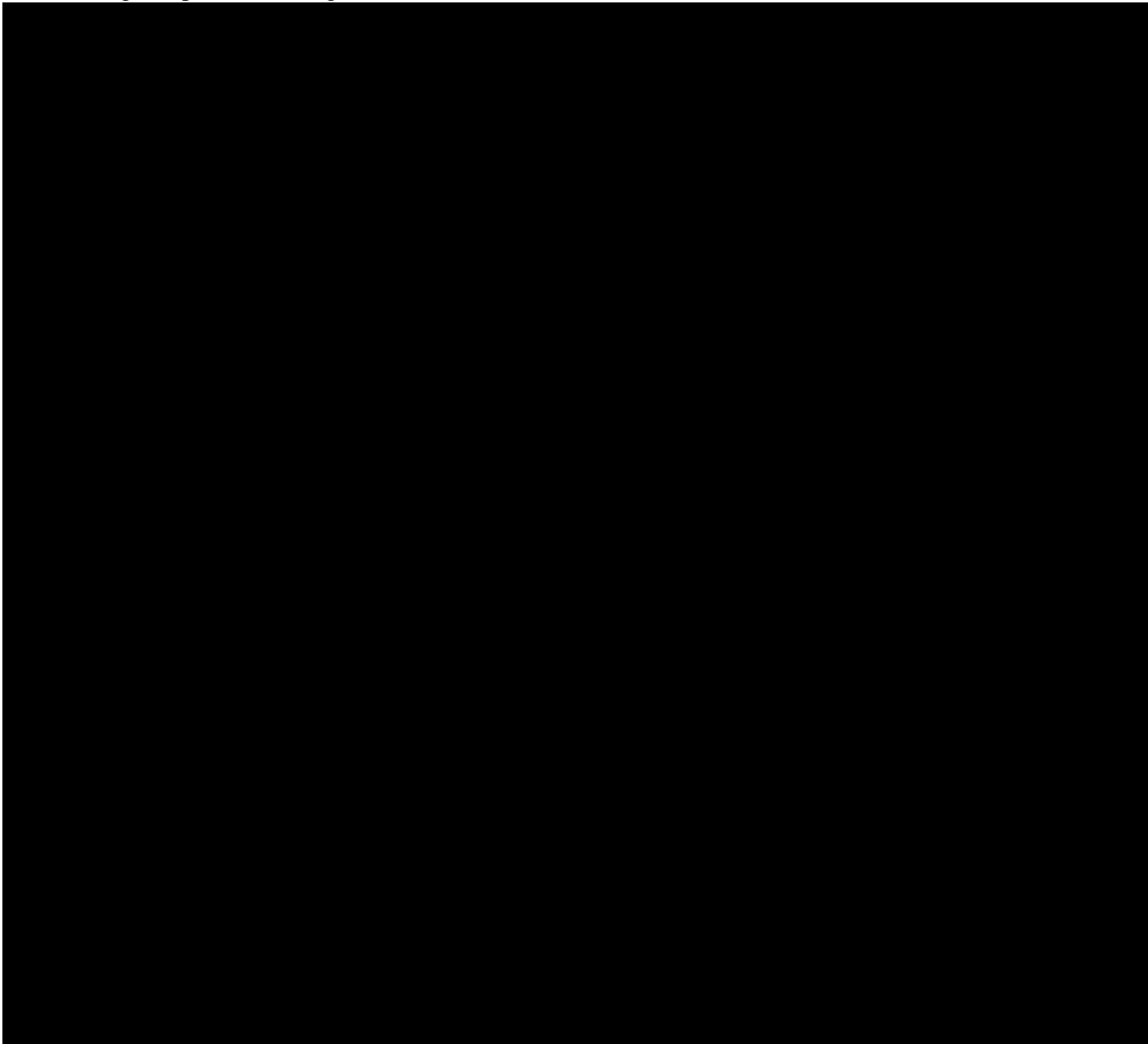
45 [REDACTED]

<sup>46</sup> (U) In most instances, NSA subsequently conducted the necessary foreignness checks and confirmed that there was no information in NSA systems indicating that the facility was used by a United States person or by someone in the United States. In the limited instances in which this was not the case, NSA detasked the account. All Section 702 data acquired as a result of the incomplete application of NSA's targeting procedures was subject to purge.

47 [REDACTED]

48 [REDACTED]

(U) As noted above, NSA and the joint oversight team are committed to ensuring that all indications of United States person status or possible location in the United States are appropriately investigated prior to tasking.



49

50

51

**(U) E. Effect of Technical Issues**

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

~~(S//NF)~~ For example, [REDACTED] technical issues resulted in delayed detaskings. In one of those incidents, a CIA system error prevented NSA from receiving numerous detasking requests (including emergency detaskings for compliance-related reasons and detaskings requests for lack of foreign intelligence interest) that CIA sent to NSA [REDACTED].<sup>52</sup> NSA subsequently confirmed that all facilities have either been detasked or remain subject to acquisition pursuant to Section 702 because an NSA analyst continues to have a foreign intelligence interest in the target. Furthermore, CIA advised that the system error was subsequently corrected and that the relevant systems are now working as intended.

**(U) F. Effect of Human Errors**

(U) As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established a variety of processes to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated. For example, despite multiple pre-tasking checks, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors accounted for approximately 8% of the tasking errors made in this reporting period, which is a decrease from the previous reporting period's 18%.<sup>53</sup> Furthermore,

<sup>52</sup> [REDACTED]

<sup>53</sup> [REDACTED]



only one such incident during this reporting period resulted in the tasking of a facility used by a United States person or person in the United States. Approximately 14% of the detasking delays from this reporting period were the result of inadvertent errors, [REDACTED]<sup>54</sup> As discussed below, approximately 27% of the detasking delays were the result of faulty analysis or misunderstanding of procedures.<sup>55</sup> As with other compliance incidents, any data acquired as a result of such tasking and detasking errors - regardless of whether or not the user proves to be a United States person or person in the United States - is required to be, and has been, purged.

(U) NSA's minimization procedures require queries of Section 702-acquired data to be designed in a manner "reasonably likely to return foreign intelligence information." Approximately 29% of the minimization errors in this reporting period involved non-compliance with this rule regarding queries (54% in the last reporting period).<sup>56</sup> As with prior Joint Assessments, this is the cause of most compliance incidents involving NSA's minimization procedures. These types of errors are typically traceable to a typographical or comparable error in the construction for the query. For example, an overbroad query can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overbroad results as a result of the query. No incidents of an analyst purposely running a query for non-foreign intelligence reasons against Section 702-acquired data were identified during the reporting period, nor did any of the overbroad queries identified involve the use of a United States person identifier as a query term.

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

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

54

55

56

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

~~(S//SI//NF)~~ As noted in prior Joint Assessments, the joint oversight team believes that NSA should strongly consider two changes to its tasking tool, though the team recognizes that the changes suggested may have implications beyond Section 702 as NSA uses the same tasking tool for multiple authorities. First, NSA's tasking tool is currently configured in such a manner that [REDACTED] can result in the unintentional retasking of a facility without the application of the NSA targeting procedures. [REDACTED] such incidents were identified during this reporting period.<sup>57</sup> Similarly, in processing [REDACTED] requests from CIA and FBI, detasked facilities will be erroneously retasked without application of the NSA targeting procedures unless NSA personnel verify that the facility [REDACTED] is currently subject to Section 702 acquisition; one such error occurred during this reporting period.<sup>58</sup> While modifications to NSA's tasking tool that would have prevented these two methods of erroneously retasking facilities would eliminate only 5% of the tasking errors that occurred in this reporting period, such changes would have eliminated 8% and 16% of tasking errors in the prior two reporting periods, respectively. The past three reporting periods demonstrate that these types of changes could potentially reduce the already very small overall compliance rate. Nonetheless, NSA is currently reviewing this recommendation and plans to engage in further discussions with DOJ and ODNI.

(U) Additionally, as noted in prior Joint assessments, the joint oversight team believes NSA should assess modifications to systems used to query raw Section 702-acquired data to require analysts to identify when they believe they are using a United States person identifier as a query term. Such an improvement, even if it cannot be adopted universally in all NSA systems, could help prevent compliance instances with respect to the use of United States person query terms.<sup>59</sup> NSA plans to test and implement this recommendation during calendar year 2016. The new internal compliance control mechanism being developed for NSA data repositories containing unevaluated and unminimized Section 702 information will require analysts to document whether the query being executed against the database includes a known United States person identifier. Once the query is executed, the details concerning the query will be passed to NSA's auditing system of record for post-query review and potential metrics compilation. As part of the testing, NSA will evaluate the accuracy of reporting this number in future Joint Assessments.<sup>60</sup>

57

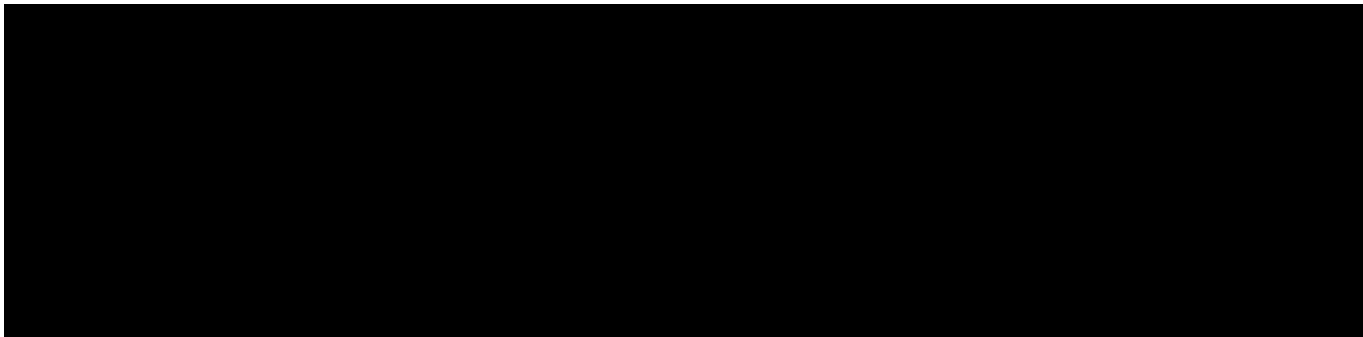
58

59

<sup>60</sup> (U) In a letter dated October 27, 2015, the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI) requested that the Director of National Intelligence submit a report about specific questions

(U//FOUO) In addition, the PCLOB, in its Section 702 report, recommended that NSA implement processes to annually count “the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles or other identifiers potentially associated with individuals.” PCLOB 702 Report Recommendation 9(4). In the Section 707 Report, the Department of Justice reports (i) the number of metadata queries that use a United States person identifier and (ii) the number of United States person identifiers approved for content queries. [REDACTED]

[REDACTED] Currently, both sets of number are classified; NSA plans to declassify future numbers so as to report these numbers publicly as part of ODNI’s Transparency Report.



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

(U) Consistent with the general increase in the number of compliance incidents during this reporting period, the joint oversight team has identified a slight increase of incidents caused by analysts, officers, or agents misunderstanding or misapplying the requirements of NSA’s targeting or minimization procedures. A number of incidents identified during this reporting period were attributable, to varying degrees, to a misunderstanding or misapplication of these rules. The overall number of such incidents compared with the number of targeting, detasking, and minimization decisions made by Government personnel remains very low, and the particular aspects of the procedures misunderstood or misapplied were diverse.

(U) For example, in one incident,<sup>61</sup> NSA’s internal oversight questioned an analyst’s cited connection between the target user of the tasked facility and the specifically referenced Section 702 certification pertaining to the purpose of obtaining foreign intelligence information. NSA’s targeting procedures require that analysts identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information. NSA also has internal documentation requirements whereby analysts must provide a linkage between the user of

---

contained in the letter pertaining to Section 702, including an update on the “status of the proposed changes [DOJ] suggested the [NSA] make to its tasking tool for Section 702 queries” and references the previous Joint Assessment. This October 2015 letter also requested that the report evaluate “the possibility of including additional automated mechanisms for analyzing the foreignness of a target pre- and post- tasking.” Additional information will be provided on this report in future Joint Assessments, as appropriate.

<sup>61</sup> [REDACTED]

the facility and the foreign intelligence purpose covered by the certification under which it is being tasked, as detailed further in the attached appendix. In this NSA incident, the analyst subsequently confirmed that there was insufficient information to appropriately link the target with the foreign intelligence information purpose of the Section 702 certification. NSA detasked the facility and advised that there was no indication that the facility was used by a United States person or by someone in the United States. NSA further advised that the relevant personnel have been reminded of the Section 702 tasking requirements and that all necessary purge requirements were completed.

(U) The joint oversight team assesses that the low overall rate of such incidents and the fact that such incidents are not overly concentrated in any particular area generally reflects the strength of the agencies training programs.

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

(~~S//NF~~)<sup>62</sup> During this reporting period, there was only one incident involving noncompliance with the CIA minimization procedures, which is a decrease from the [REDACTED] incidents that occurred during the previous reporting period, but in line with historic reporting. [REDACTED]

(~~S//NF~~) CIA's sole compliance incident involved the untimely destruction of data, [REDACTED] as is required by its minimization procedures.<sup>63</sup> CIA's Section 702 procedures require that CIA delete un-reviewed data five years from the expiration date of the relevant Section 702 certification. However, the relevant data was subsequently removed from CIA systems, and CIA made no use of the information that was improperly retained for the short period of time.

(~~S//NF~~) The joint oversight team believes that this CIA compliance incident, and other historical CIA, FBI, and NSA purge-related incidents indicate that the Government must remain vigilant to ensure the appropriate and timely removal of data. As with the prior Joint Assessment, the joint oversight team believes it is important for agencies to carefully consider the potential impacts on the purge process in designing and updating systems, including ensuring the appropriate time required for the deletion. The joint oversight team also believes that agencies must regularly monitor and reevaluate the functioning of relevant systems due to the fact that the identification and destruction of relevant data can be complex. Finally, the joint oversight team continues to remain focused on the purging of data by all three agencies. During this last reporting period, the joint oversight team continued to have meetings and/or conference calls with all three agencies as it pertained to their purging of data.

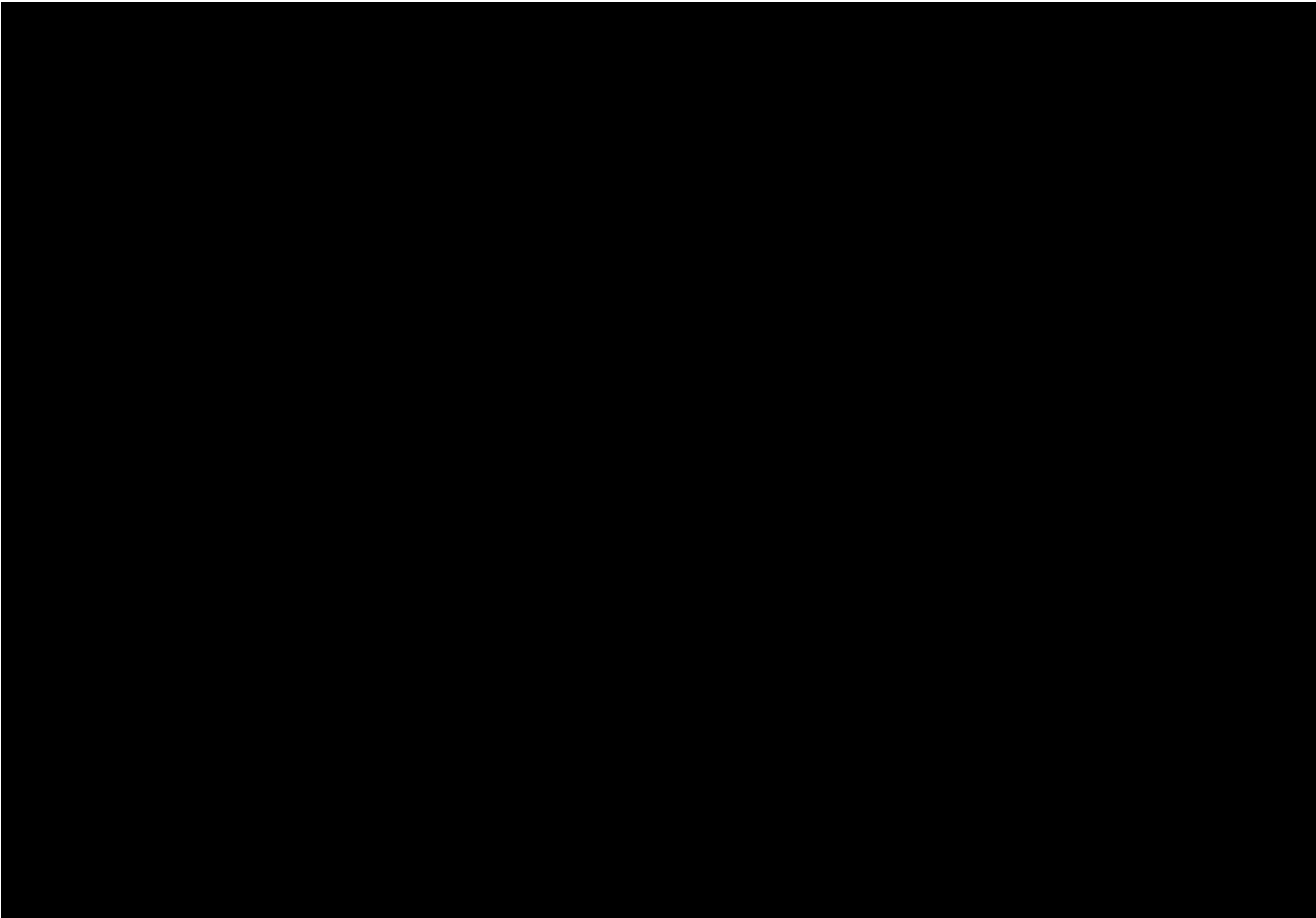
---

<sup>62</sup> (~~U//FOUO~~) This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

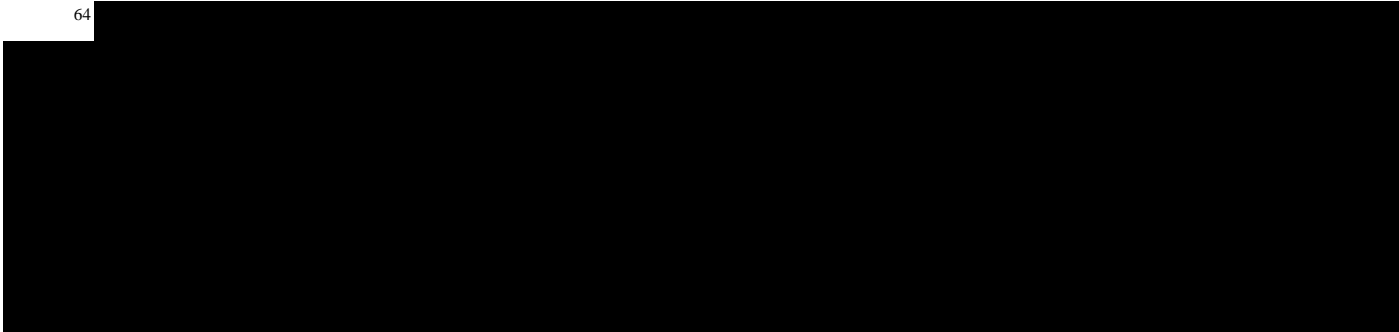
<sup>63</sup> [REDACTED]

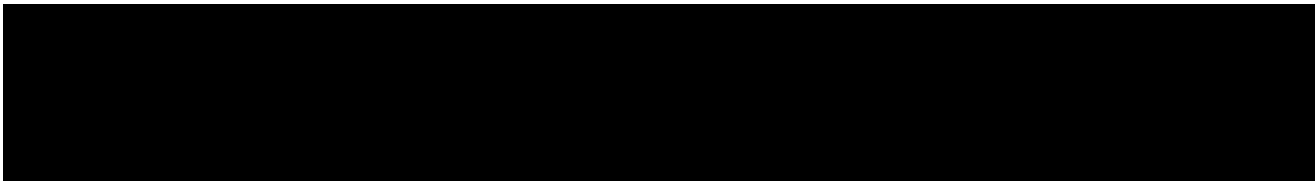
**(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures**

(U) There were a minimal number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period. As a percentage of FBI's targeting actions during the reporting period, the FBI targeting compliance incident rate during this reporting period decreased from 0.03% to 0.02%. The targeting incidents in this reporting period that did occur were process issues that were narrow in impact, and none involved the targeting of an individual who was in fact a United States person or person located in the United States.



64





(U) One of the minimization errors involved the improper querying of raw Section 702-acquired data.<sup>65</sup> Here, NSD's oversight review revealed that on multiple occasions over an approximate three-week period, an FBI employee conducted queries using United States person identifiers of at least three other FBI personnel and the FBI employee's own identifier. Although the searches were for official work-related purposes, the queries were not conducted in an effort to find and extract foreign intelligence information or evidence of a crime, as required by FBI's minimization procedures. Subsequently, FBI reminded the employee of the minimization procedures' requirement concerning queries. FBI also provided additional, formalized retraining to relevant personnel to remind them of the appropriate Section 702 query requirements.

(~~S//NF~~) [redacted] minimization errors involved the improper dissemination of United States person information. [redacted] For example, [redacted] the FBI disseminated the names of United States [redacted] NSD and ODNI determined that it was unreasonable to conclude the dissemination of the United States person identities [redacted] met the appropriate standard. In prior Section 707 Reports, the Government has reported [redacted] in which NSD and ODNI assess that FBI had improperly disseminated United States person information. *See, e.g.*, March 2014 Section 702 Report. [redacted]



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

(~~S//NF~~)<sup>66</sup> During this reporting period, there were [redacted] incidents (as opposed to one incident during the last reporting period) of noncompliance by an electronic communication service provider with a Section 702(h) directive. Given that errors by the service providers can result in the acquisition of United States person information, the Government must actively monitor the acquisitions that the providers transmit to the Government. The joint oversight team believes that the historically low number of compliance incidents caused by service providers reflect, in part, the service providers' commitment to comply with the law while protecting their customers' interests. However, the low number of these incidents also reflects continued efforts by the Government and service providers to ensure that lawful intercept systems are effective and compliant with all applicable law and other requirements. The Government must continue to work with the service providers to prevent future incidents of non-compliance.

<sup>65</sup> [redacted]

<sup>66</sup> (~~U//FOUO~~) This paragraph carried a different portion marking in prior joint assessments. As noted in footnote 9 above, we are continuing to review the information in this paragraph to determine the proper portion marking, but, in the meantime, the portion-marking of this paragraph has been upgraded.

**(U) SECTION 5: CONCLUSION**

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

# APPENDIX A



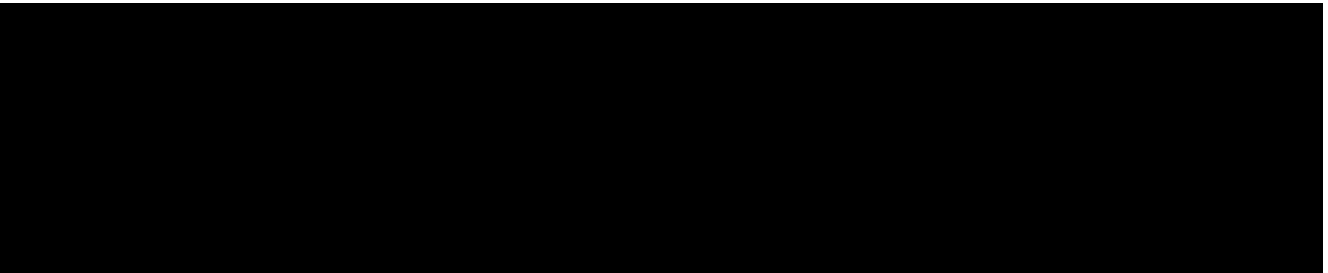
## APPENDIX A

### (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).<sup>1</sup> As required by Section 702, those targets must be non-United States persons<sup>2</sup> reasonably believed to be located outside the United States.

~~(S//NF)~~ During this reporting period, NSA conducted foreign intelligence analysis to



<sup>1</sup> (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).

<sup>2</sup> (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 section 101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

3

4

(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 receive or 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 NSA's FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a "selector") is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.<sup>5</sup> In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA "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//NF)~~ Once information is collected from these tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.<sup>6</sup>

(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

<sup>5</sup>

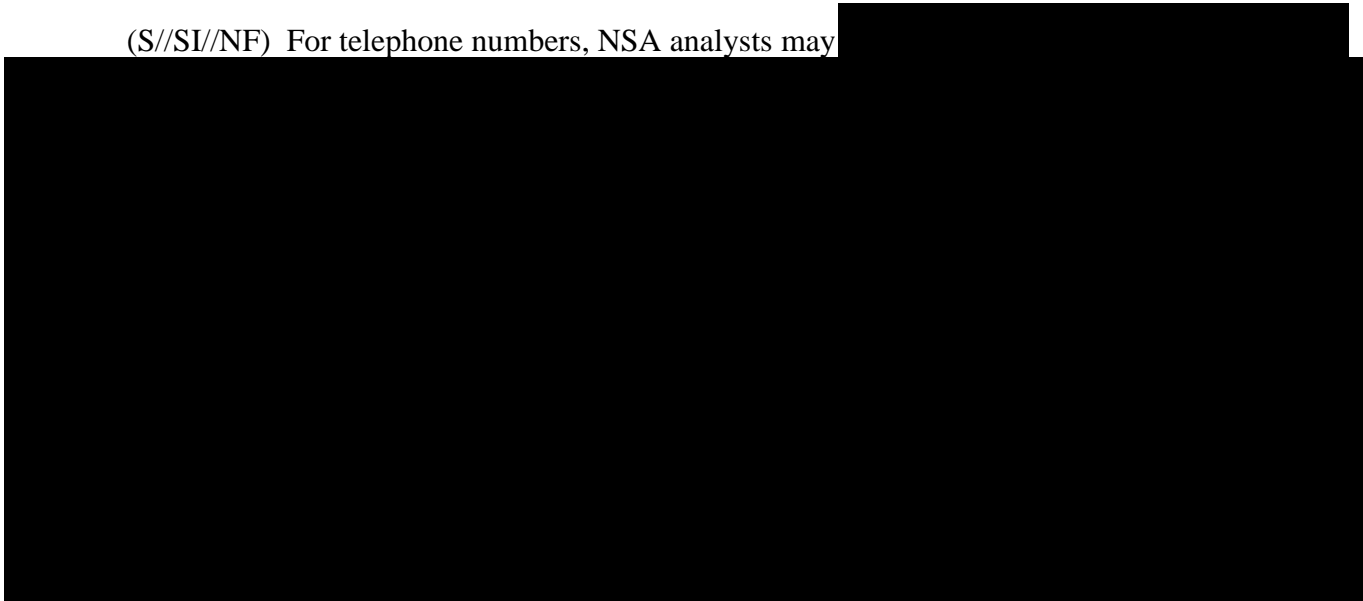
<sup>6</sup> (S//NF) As noted in the Section 707 Report, with respect to ongoing acquisitions from certain electronic communication service providers,

believed to be located outside the United States, the post-targeting analysis conducted on the facilities, and the documentation required.

**(U) A. Pre-Tasking Location**

**(U) 1. Telephone Numbers**

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



**(U) 2. Electronic Communications Identifiers**

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



<sup>7</sup>

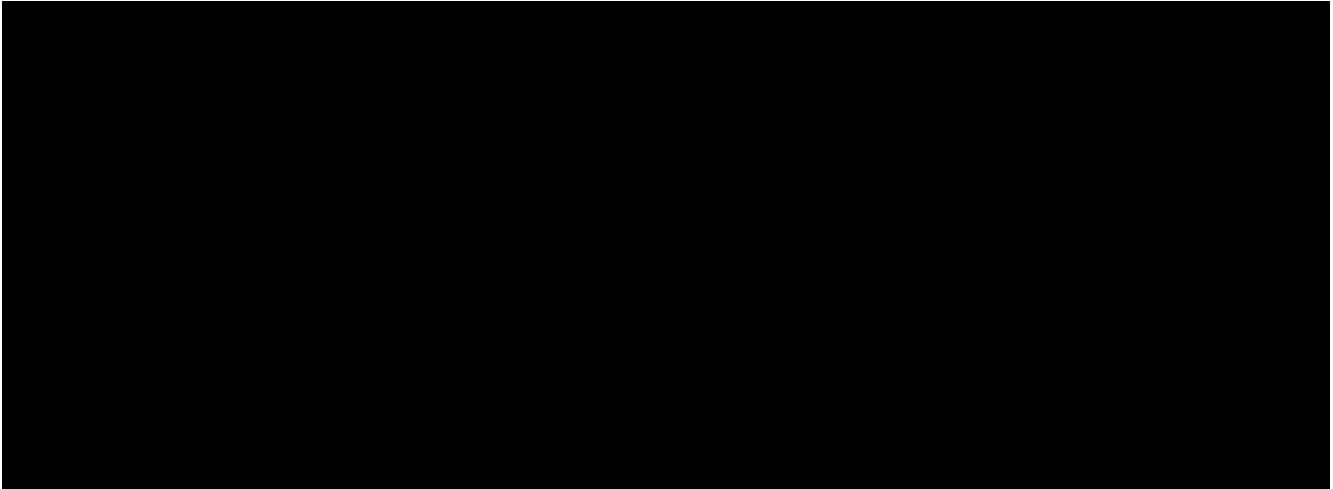


<sup>8</sup> (U) Analysts also check this system as part of the “post-targeting” analysis described below.

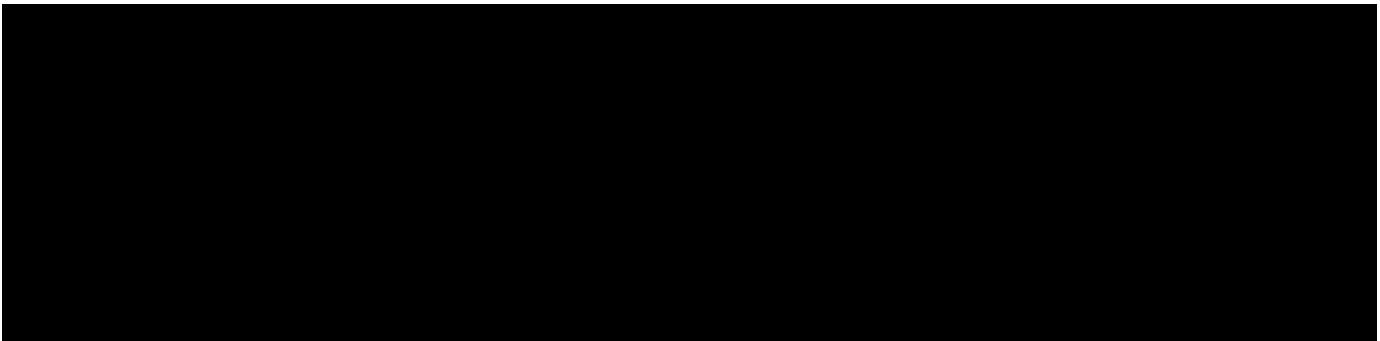
<sup>9</sup>



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



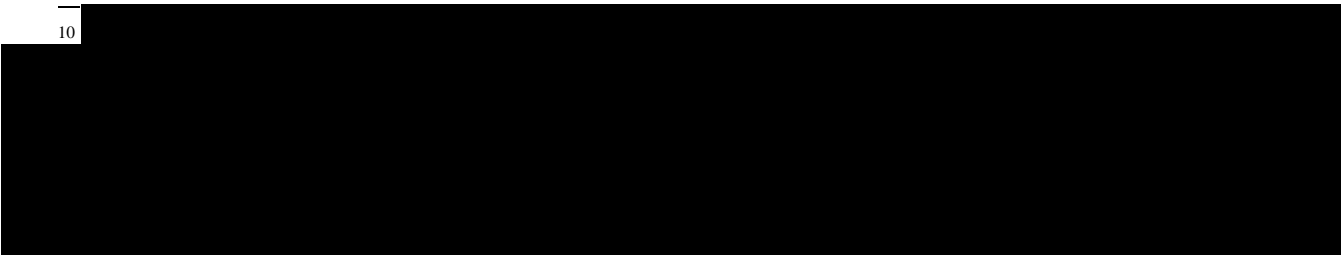
**(U) C. Post-Tasking Checks**



~~(S//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],<sup>11</sup> 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 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

10



<sup>11</sup> ~~(S//NF)~~ NSA's automated notification system to ensure analysts have reviewed collection is currently implemented only for [REDACTED], not [REDACTED] NSA is attempting to develop a similar system for [REDACTED]

sent to the tasking team, as well as to their management, who then have the responsibility to follow up.

**(U) D. Documentation**

(U) 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.

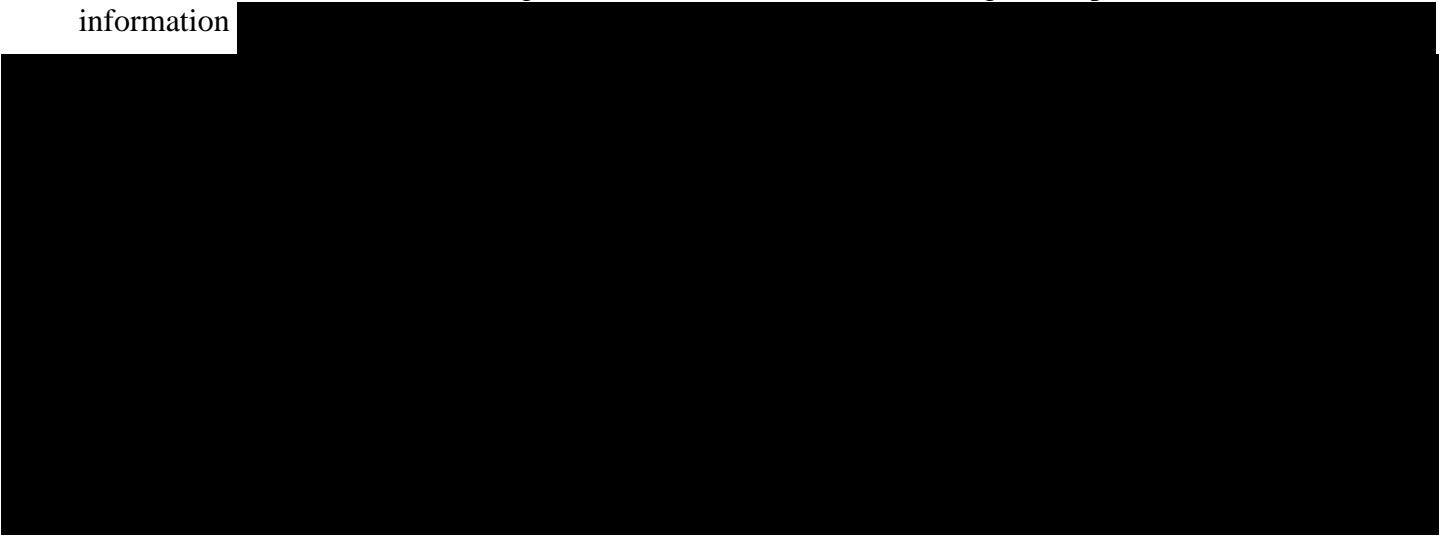
(S//NF) NSA has [REDACTED] an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. [REDACTED] to assist analysts as they conduct their work. This tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain 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]

[REDACTED] The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields [REDACTED] each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

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

(S//NF) [REDACTED]  
[REDACTED] Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the record or records relied upon by the analyst, [REDACTED] the analyst's foreignness explanation, the targeting rationale, [REDACTED] These records, referred to as "tasking sheets," are reviewed by the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

(S//NF) The source records cited on these tasking sheets are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations recorded on the tasking sheets. Other source records may consist of “lead information” from other agencies, such as disseminated intelligence reports or lead information



**(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 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 OGC. SID Oversight and Compliance conducts spot checks of targeting decisions and disseminations to ensure compliance with procedures. SID also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

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

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

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

## (U) II. Overview - CIA

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

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

one of the Section 702(g) certifications. [REDACTED]

[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]

(U) The FISA Program Office was established in December 2010 [REDACTED]

[REDACTED] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts [REDACTED]. The primary responsibilities of the FISA Program Office are to [REDACTED]

---

12 [REDACTED]



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 FISA compliance program is managed by its FISA Program Office in coordination with CIA OGC. CIA provides small group training to personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination and minimization questions. Identified incidents of noncompliance with the CIA minimization procedures are generally reported to NSD and ODNI by CIA OGC.

**(U) III. Overview - FBI**


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

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process intelligence targets to NSA for the acquisition of in-transit communications


information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to NSA for tasking.

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 FBI must then apply its own additional procedures, which require FBI to review NSA's conclusion of foreignness

(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.



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



~~(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 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]

[REDACTED] XTS has the lead responsibility in FBI for [REDACTED] s 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 to NSA for [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.