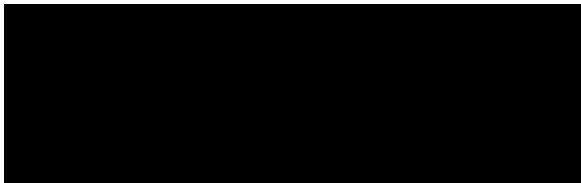




(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: June 1, 2015 – November 30, 2015

November 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

November 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	13
(U) VII. The Privacy and Civil Liberties Oversight Board	14
(U) Section 3: Trends in Section 702 Targeting and Minimization	16
(U) I. Trends in NSA Targeting and Minimization	16
(U) II. Trends in FBI Targeting	21
(U) III. Trends in CIA Minimization	23
(U) Section 4: Compliance Assessment – Findings	27
(U) I. Compliance Incidents – General	27
(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures	34
(U) III. Review of Compliance Incidents – CIA Minimization Procedures	48
(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures	48
(U) V. Review of Compliance Incidents – Provider Errors	51
(U) Section 5: Conclusion	51
(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

November 2016

Reporting Period: June 1, 2015 – November 30, 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 fifteenth joint compliance assessment of the Section 702 program. This assessment covers the period from June 1, 2015 through November 30, 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 as required by Section 707(b)(1) of FISA (hereinafter “the Section 707 Report”). The Department of Justice submitted the Section 707 Report on March 3, 2016; it covers the same reporting period as the Joint Assessment.

(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 (0.52%) of the overall collection activity. While this represents an increase from the last Joint Assessment’s rate of 0.35%, as well as from the other previous joint assessments’ rates, it still remains well below 1%. 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 fifteenth joint compliance assessment under Section 702, covering the period June 1, 2015 through November 30, 2015 (hereinafter, the “reporting period”).¹

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

An acquisition authorized under subsection (a)—

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

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

¹ (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on March 3, 2016, as required by Section 707(b)(1) of FISA (hereafter Section 707 Report). This fifteenth Joint Assessment covers the same reporting period as the fifteenth Attorney General’s Section 707 Report.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information.² Three agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA). An overview of how these agencies implement the authority appears in Appendix A of this assessment. The other agency involved in implementing Section 702 is the National Counterterrorism Center (NCTC), which has a limited role, as reflected in the “Minimization Procedures Used by NCTC in connection with Information Acquired by FBI pursuant to Section 702 of FISA, as amended.”³

(U) Section Two of this Joint Assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting and minimization procedures, as well as the Attorney General’s Acquisition Guidelines. Section Two also 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 concerted effort by agency personnel to comply with the requirements of Section 702 during this

2



³ (U) Under these limited minimization procedures, NCTC is not authorized to receive unminimized Section 702 data. Rather, these procedures recognize that, in light of NCTC’s statutory counterterrorism role and mission, NCTC has been provided access to certain FBI systems containing *minimized* Section 702 information, and prescribe how NCTC is to treat that information. For example, because NCTC is not a law enforcement agency, it may not receive disseminations of Section 702 information that is evidence of a crime, but which has no foreign intelligence value; accordingly, NCTC’s minimization procedures require in situations in which NCTC personnel discover purely law enforcement information with no foreign intelligence value in the course of reviewing minimized foreign intelligence information that the NCTC personnel either purge that information (if the information has been ingested into NCTC systems) or not use, retain, or disseminate the information (if the information has been viewed in FBI systems).

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 (a) inter and intra-agency communication, (b) training, and (c) systems used in the handling of Section 702-acquired communications, including those systems needed to ensure that appropriate purge practices are followed and that certain disseminated reports are withdrawn as 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 CIA⁴ each handle Section 702-acquired data in accordance with their own minimization procedures.⁵ 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 Office of Civil Liberties, Privacy and Transparency (ODNI CLPT),⁶ 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.

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

⁵ (U) Each agency's targeting and minimization procedures are approved by the Attorney General and reviewed by the Foreign Intelligence Surveillance Court. In 2015, 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"). Most recently, on August 11, 2016, the DNI released, in redacted form, NSA's, FBI's, and CIA's (as well as NCTC's) 2015 minimization procedures on ODNI's *IC on the Record* website as part of DNI's commitment to the IC's Principles of Transparency.

⁶ (U) CLPT was formerly called the Civil Liberties and Privacy Office (CLPO). Its name was changed to CLPT in June 2016. Although outside the reporting period for this current assessment, the name has nonetheless been updated herein.

(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 facilities⁷ (also referred to as selectors) 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,⁸ as well as the investigation and reporting of specific compliance incidents. During this reporting period, NSD and ODNI conducted the following onsite reviews at NSA:

Figure 1: (U) NSA Reviews

Date of Review	Taskings/Minimization Reviewed
August 28, 2015	June 1, 2015 – July 31, 2015
October 30, 2015	August 1, 2015 – September 30, 2015
December 16 and 22, 2015	October 1, 2015 – November 30, 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 onsite review, NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the review period to NSD and ODNI.⁹ Members of the joint oversight team initially review the tasking sheets, with ODNI team members sending any questions they may have concerning the tasking sheets to NSD, who then prepare a detailed report

⁷ (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 (i.e. selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described within this joint assessment, applies to the targeting of every communication facility regardless of the type of facility. A fuller description of the Section 702 targeting process may be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and is not attempting to make a substantive distinction between the two terms.

⁸ (U) NSA’s targeting procedures require that the onsite reviews occur approximately every two months.

⁹ (U) During this reporting period, NSA discovered that it had mistakenly not provided some of the required tasking documentation (i.e. tasking sheets) to NSD and ODNI, thereby resulting in compliance incidents, which are discussed below.

of the findings, including any questions and requests for additional information. NSD shares this report 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.

(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. The joint oversight team works with NSA to answer 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 the 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 oversight team reviews all approved United States person identifiers to ensure compliance with the minimization procedures.¹⁰ 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.¹¹

¹⁰ (U) Although outside this Joint Assessment's reporting period, on May 2, 2016, the DNI publicly released ODNI's third annual *Transparency Report[s]: Statistical Transparency Report Regarding Use of National Security Authorities* for calendar year 2015 (hereafter the *2015 Transparency Report*). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(A)), the *2015 Transparency Report* provided the "estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702" (emphasis added) for the entire calendar year of 2015.

¹¹ (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(B)), the *2015 Transparency Report* provided the "estimated number of queries concerning a known U.S. person used to retrieve the unminimized noncontents [(i.e. metadata)] information obtained under Section 702" (emphasis added) for the entire calendar year of 2015.

(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.¹² 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 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

Date of Visits	Minimization Reviewed
September 11, 2015	June 1, 2015 – July 31, 2015
November 4 and 17, 2015	August 1, 2015 – September 30, 2015
January 6 and 8, 2016	October 1, 2015 – November 30, 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

¹² (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.

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) CIA may receive [REDACTED]³ 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.¹⁴ 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.

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

¹³ (S//NF) [REDACTED]
[REDACTED] This footnote carried a different portion marking in prior joint assessments.

¹⁴ (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve CIA.

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

(S//NF) 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

Date of Visit	Targeting and Minimization Reviewed
August 19, 2015	June 2015 targeting decisions
September 16, 2015	July 2015 targeting decisions
November 9 and 10, 2015	August 2015 targeting decisions and June 1 through August 31, 2015, minimization decisions
November 17 and 18, 2015	September 2015 targeting decisions
December 10 and 11, 2015	October 2015 targeting decisions and September 1 through November 30, 2015, minimization decisions
January 11 and 12, 2016	November 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.¹⁵ The joint oversight team also reviews a sample of other files to 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.

¹⁵(S//NF) Supporting document includes, among other things, [REDACTED] The joint oversight team reviews every file identified by FBI [REDACTED]

(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 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 15 FBI field offices during this reporting period and reviewed cases involving Section 702-tasked facilities.¹⁶ ODNI joined NSD at a subset of these reviews; ODNI receives written summaries regarding all the reviews from NSD regardless of whether ODNI was in attendance or not. 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 in April 2016, which is outside this current Joint Assessment's reporting period.

~~(S//NF)~~ 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.

(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.¹⁷ 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.

¹⁶ ~~(S//NF)~~ During these field office reviews, NSD reviewed [REDACTED] involving Section 702-tasked facilities.

¹⁷ (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.

(U) IV. Joint Oversight of NCTC

(U) As noted above, NCTC is also involved in implementing Section 702, albeit in a limited role, as reflected in the “Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended.” Under these limited minimization procedures, NCTC is not authorized to receive unminimized Section 702 data, but NCTC has been provided access to certain FBI systems containing minimized Section 702 information. As part of the joint oversight of NCTC to ensure compliance with these procedures, NSD and ODNI conduct reviews of NCTC’s access, receipt, and processing of Section 702 information received from FBI. The most recent review occurred in May 2016, which is outside this current joint assessment’s reporting period.

(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 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, 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 the previous 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; during this reporting period, the CIA continued to implement this training required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. 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 continued to provide additional focused training at FBI field offices on the Section 702 minimization procedures, including training FBI field personnel, such as field office attorneys, on the attorney-client privileged communication provisions of FBI's minimization procedures.¹⁸ NSD's training at FBI field offices also included training on the new reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications.¹⁹ This new reporting requirement applies to queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a U.S. person that was reviewed by FBI personnel.

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

¹⁸ (U) This specific training began before and continued after the current reporting period of June 1, 2015 – November 30, 2015.

¹⁹ (U) On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, the FISC's *November 6, 2015 Memorandum Opinion and Order* on the ODNI's public website *IC on the Record*.

~~(S//NF)~~ This November 6, 2015 FISC opinion's formal, but classified, title is [REDACTED]

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) Specifically, the Board determined that PRISM collection (where the government sends a selector to a United States-based electronic communications service provider) and upstream collection are authorized by the statutory language of Section 702, and further concluded "that the core of the Section 702 program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence [. . .] – fits within the "totality of the circumstances" standard for reasonableness under the Fourth Amendment." *PCLOB's Section 702 Report* at 8-9. However, the Board also found that "[o]utside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness." *Id.* It enumerated specific areas "where operations of the Section 702 program could strike a better balance between privacy, civil rights, and national security" and recommended three revisions to the targeting and minimization procedures governing the Section 702 program. *See id.* at 134.

(U) In response to the *PCLOB's Section 702 Report*, the Government adopted all three recommended revisions to the relevant 2015 targeting and minimization procedures, which are detailed below. Subsequently, the FISC, after the appointment of an amicus curiae, found, in an opinion, that those revised procedures complied with Section 702 and were consistent with the requirements of the Fourth Amendment.²⁰

(U) The PCLOB recommended that NSA's targeting procedures be "revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector [i.e. facility] is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court." *PCLOB's Section 702 Report* at 134 (Recommendation 1). The joint oversight team worked with NSA to appropriately modify its targeting procedures, including engaging with the PCLOB regarding the proposed revisions, which resulted in those recommendations being implemented in revised targeting procedures that were submitted to the FISC. Additionally, the joint oversight team advised NSA on appropriate supplemental written guidance and training for its personnel, which will continue to be the subject of continued oversight by NSA's internal compliance personnel and the joint oversight team.

(U) The PCLOB also recommended that FBI's procedures "be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination

²⁰ (U) These procedures were filed with the FISC as part of the 2015 Certifications renewal application, which the FISC approved on November 6, 2015. As noted above, the FISC's *November 6, 2015 Memorandum Opinion and Order* was publicly released on ODNI's *IC on the Record* website in April 2016.

of Section 702 data in connection with non-foreign intelligence criminal matters.” *PCLOB’s Section 702 Report* at 137 (Recommendation 2). Again, the joint oversight team worked with FBI to implement this recommendation and engaged with the PCLOB regarding the proposed revisions. These revisions were submitted to the FISC in the form of revised minimization procedures. As discussed above, in its *November 6, 2015 Memorandum Opinion and Order*, the FISC imposed a reporting requirement for queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a U.S. person that was reviewed by FBI personnel.

(U) Additionally, the PCLOB also recommended that “[t]he NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if it is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA.” *PCLOB’s Section 702 Report* at 139 (Recommendation 3). The joint oversight team worked with the relevant agencies to implement this recommendation and engaged the PCLOB regarding the proposed revisions. The revisions to these agencies’ minimization procedures were submitted to, and approved by the FISC, and will continue to be the subject of oversight by the joint oversight team.

(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.

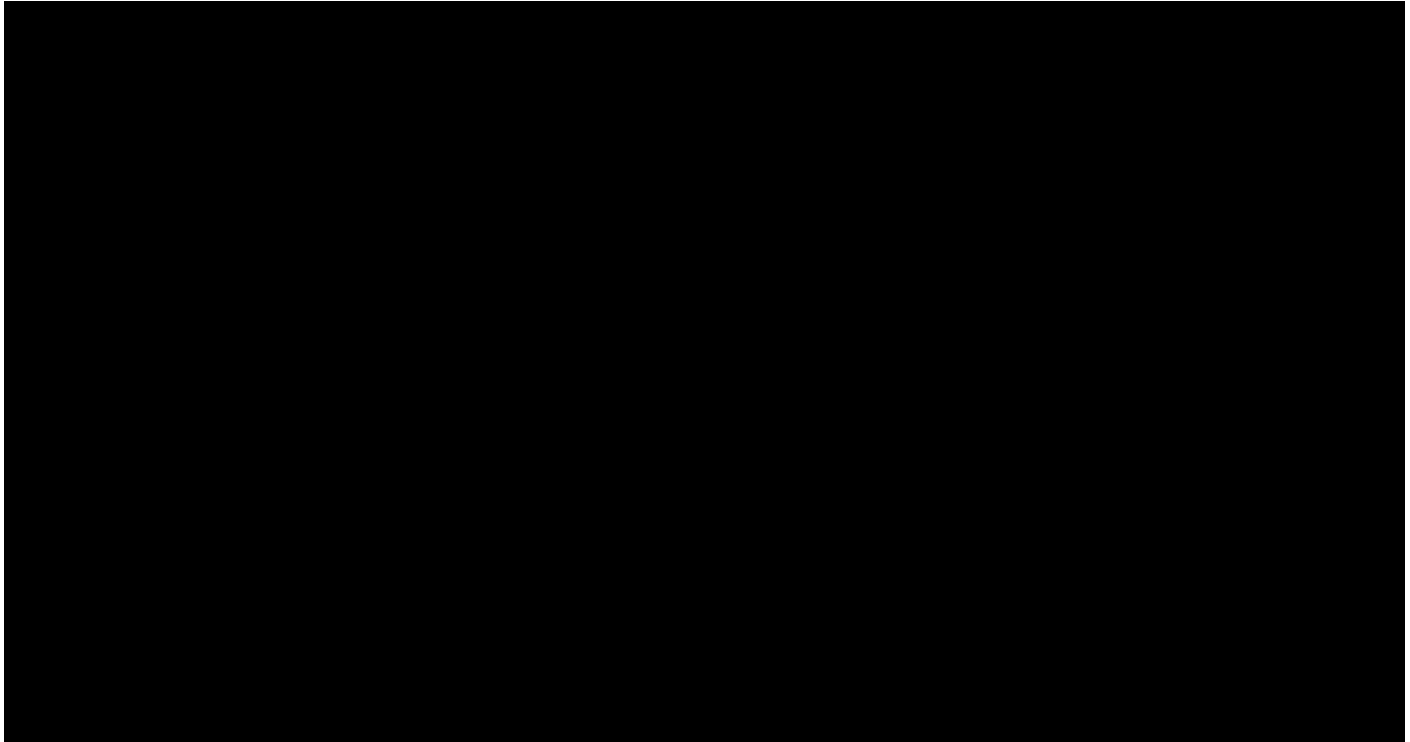
(U) I. Trends in NSA Targeting and Minimization

(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,²¹ the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.²²

²¹ (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 by ODNI, most recently in its *2015 Transparency Report*. Previously, ODNI released transparency reports on June 26, 2014, (the *2013 Transparency Report*) and on April 22, 2015 (the *2014 Transparency Report*). The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified number provided in the Transparency Reports estimate the number of Section 702 *targets*. As noted in 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*, whereas the Transparency Reports estimate the number of targets affected by Section 702 *during the calendar year*.

²² (U) One of the reporting periods in which the total number of facilities under collection decreased occurred prior to 2010 and is not reflected in the below chart.

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



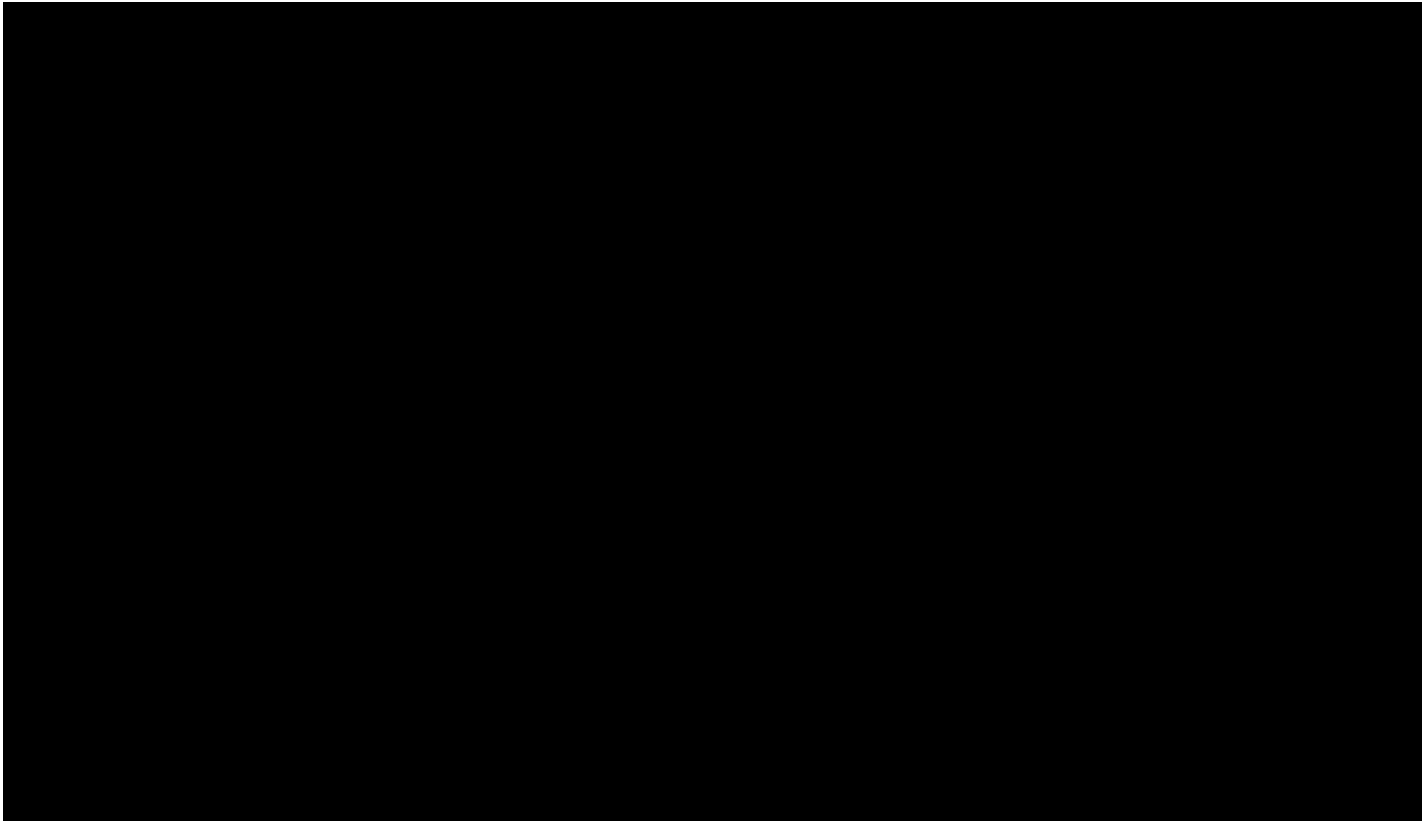
~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [REDACTED] facilities were under collection pursuant to the applicable certifications on any given day during the reporting period.²³ This represents a 2.9% increase from the approximately [REDACTED] facilities under collection 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.²⁴ Classified Figure 5 charts the total monthly numbers of newly tasked facilities since September 2010.

²³ ~~(S//NF)~~ The applicable certifications for this reporting period were [REDACTED]

²⁴ (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.

Figure 5: ~~(TS//SI//NF)~~ New Taskings by Month (Yearly Average for 2010 through 2014)



~~(TS//SI//NF)~~ Specifically, NSA provided documentation of [REDACTED] new taskings during the reporting period. This represents a 14.0% 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 eleven 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 eleven months of 2015 compared to 2014.

~~(TS//SI//NF)~~ NSA tasked an average of [REDACTED] electronic communications accounts each month in 2014. During the first eleven months of 2015, NSA tasked an average of [REDACTED] electronic communication accounts (a [REDACTED] increase from 2014's monthly average).

25

[REDACTED]

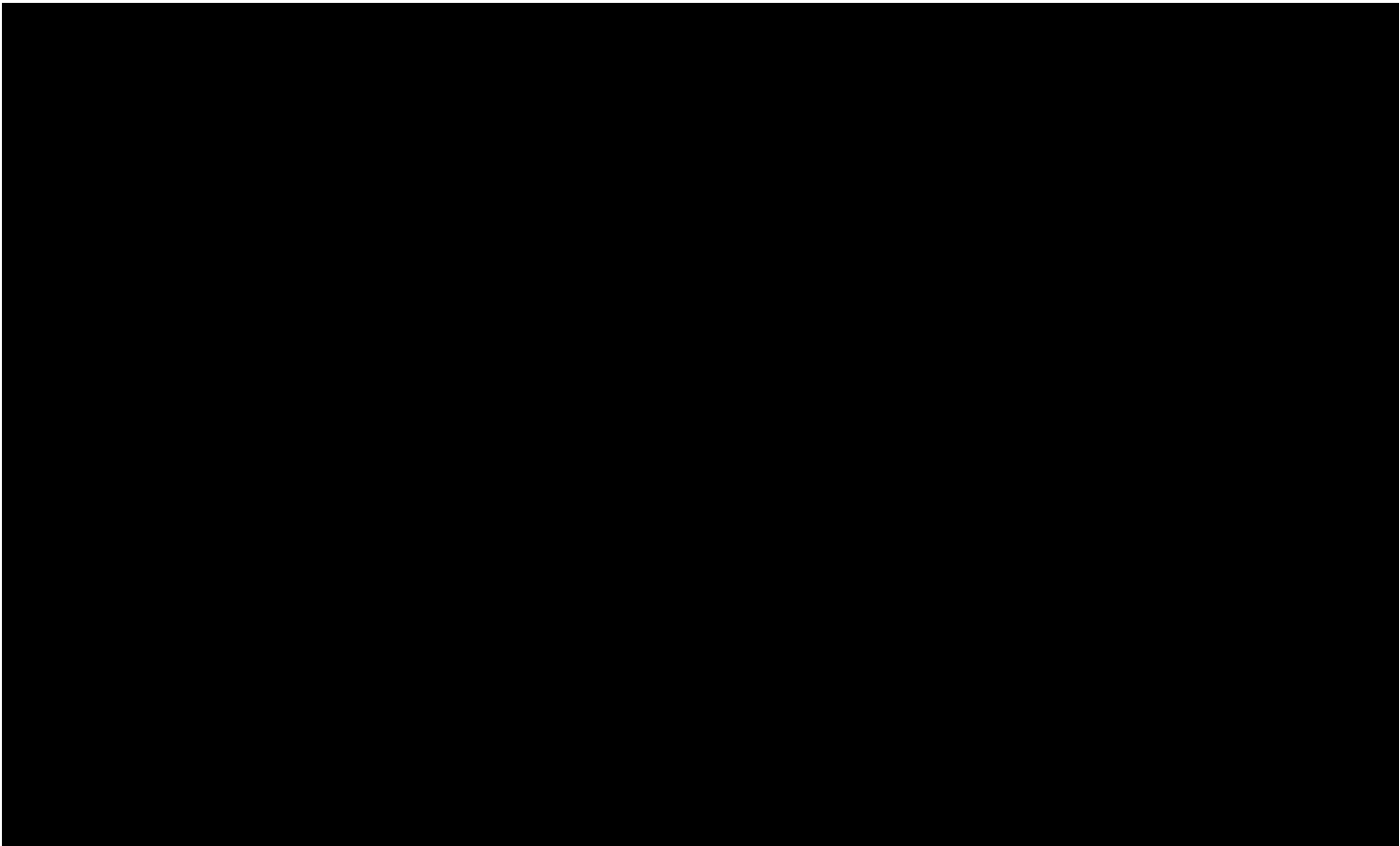
(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data, and provided NSD and ODNI access to all reports NSA identified as containing United States person information.²⁶ Figure 6 contains 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.²⁷ The number of serialized reports NSA has identified as containing United States person information slightly decreased this reporting period, compared to the prior reporting period.²⁸

²⁶ (U) Previous joint assessments referred to these reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. However, given that Section 702 of FAA replaced the PAA in 2008, the government no longer disseminates minimized information that was previously acquired pursuant to PAA. However, Figure 6 provides a trend analysis over a longer period of time and may include reports containing minimized PAA-acquired information in addition to minimized Section 702-acquired information.

²⁷ (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.

²⁸ (U) In the *2015 Transparency Report*, in response to the *PCLOB's 702 Report Recommendation 9(5)*, NSA publicly released the number of Section 702 reports that contained U.S. person information for calendar year 2015, including delineating the number of times the U.S. person information was masked versus unmasked in those disseminated reports.

Figure 6: ~~(S//NF)~~ Total Disseminated NSA Serialized Reports Based Upon Section 702-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-acquired data. This represents a 6.2% increase from the [REDACTED] such serialized reports NSA identified in the prior reporting period. Figure 6 reflects NSA reporting over the last nine reporting periods; the fact that reporting based on Section 702 -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-acquired data.²⁹ The percentage of reports containing United States person information was lower this reporting period (9.0%), than the 9.7% and 9.8% reported in the two prior reporting periods.

²⁹ ~~(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(1)(3) that is provided to Congress.

(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.³⁰ 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.³¹

(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 portion³² were rejected on the basis that they were ineligible for Section 702 collection.

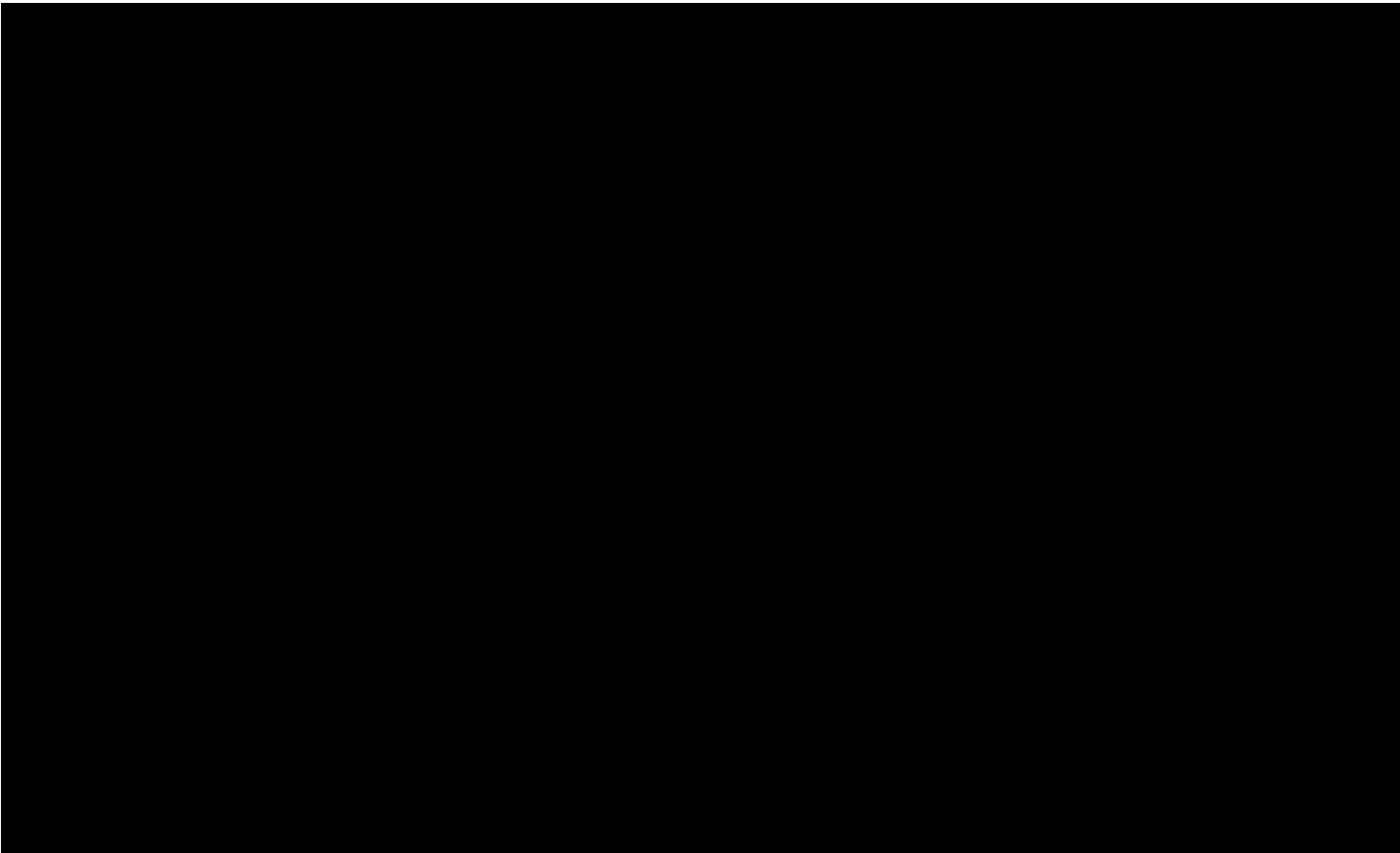
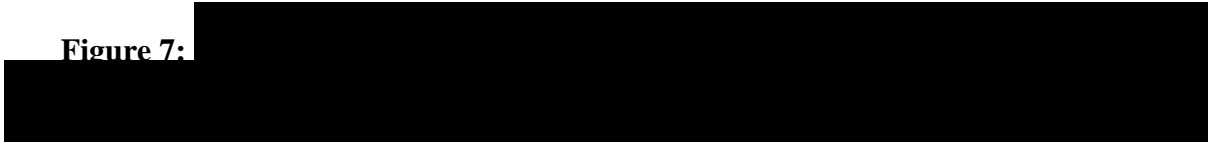
(U) Between 2010 and December 2014, the *yearly average* of designated facilities approved by FBI steadily increased. Between January and November 2015, the *number* of designated facilities approved by FBI *each month* has varied. NSD and ODNI have continued to track the number of facilities approved by FBI in 2015 and will incorporate this information into future Joint Assessments.

30

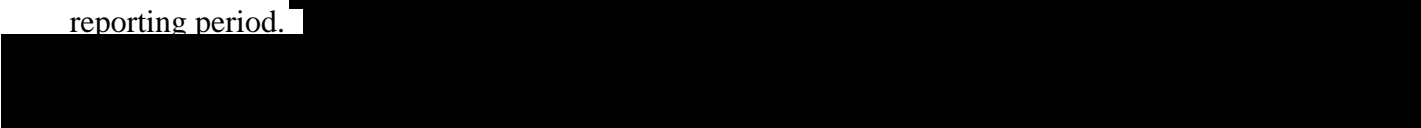
31

32

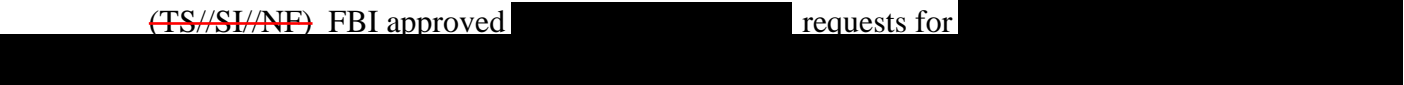
Figure 7:



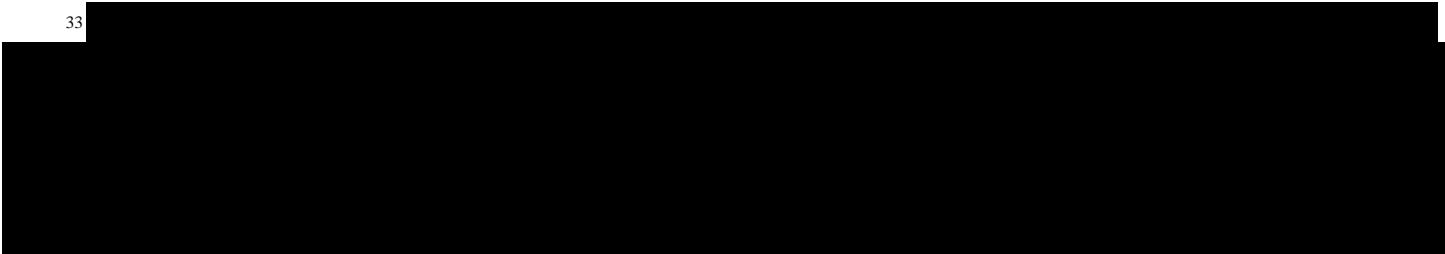
(TS//SI//NF) Specifically, FBI reports that NSA designated [redacted] accounts [redacted] [redacted] during the reporting period – an average of [redacted] designated accounts per month. This is a [redacted] increase from the [redacted] accounts designated in the prior six-month reporting period.

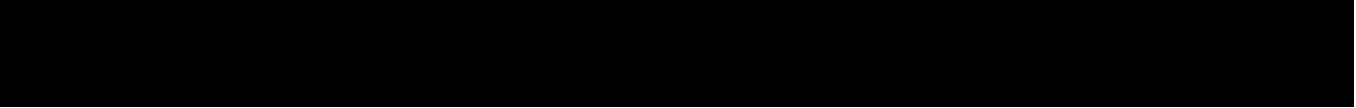


(TS//SI//NF) FBI approved [redacted] requests for [redacted]



33



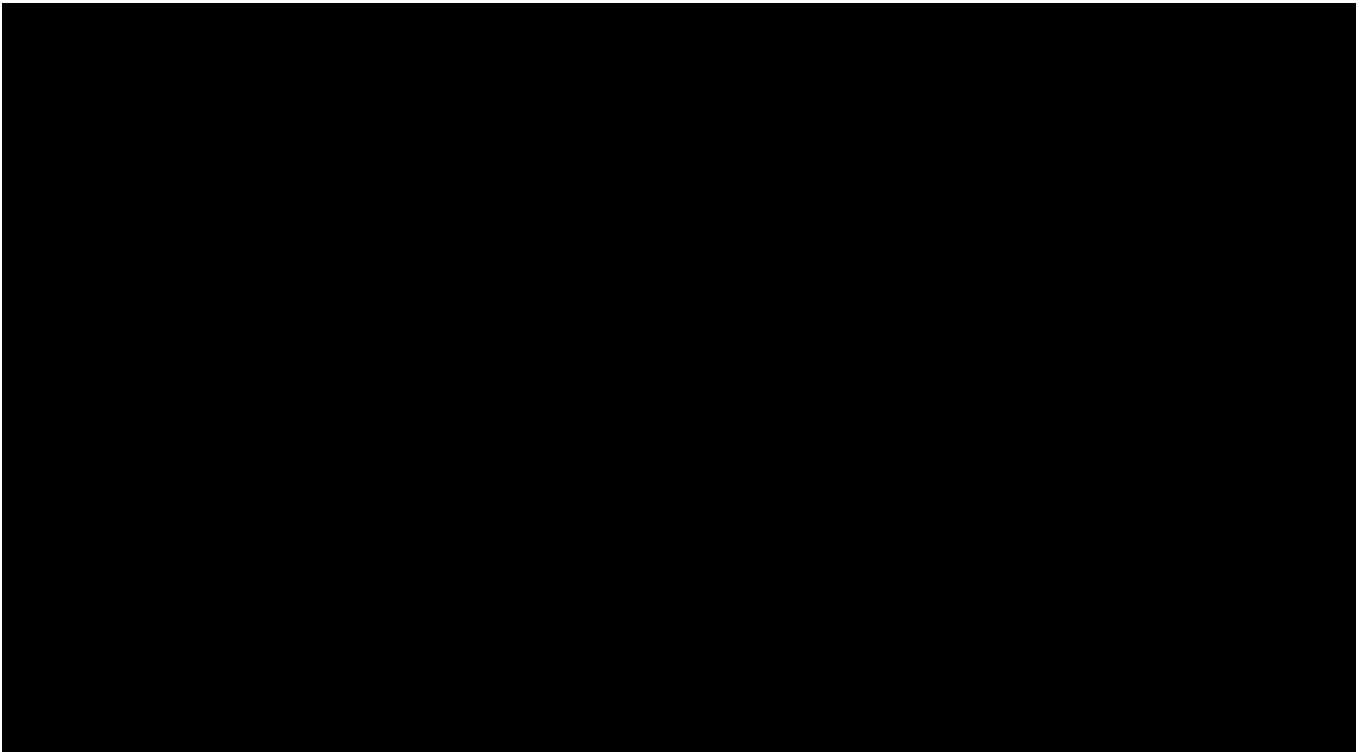


(U) As indicated in the prior Joint Assessment, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its dissemination of Section 702-acquired information from FBI Headquarters to FBI field offices. NSD conducts oversight reviews at multiple FBI field offices each year, some of which ODNI attends, 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(1)(3)(i).

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

(U) CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Classified Figure 8 compiles the number of such disseminations of reports containing United States person information identified in the last nine reporting periods (June-November 2011 through the current period of June-November 2015). In the first six reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the seventh, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the last two reporting periods, the number of CIA-identified disseminations containing United States person information again 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] SD and ODNI, however, review all [redacted] containing Section 702-acquired information 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.³⁴ Classified Figure 9 details the total number of files that were either retained or transferred, as well as the number of those

³⁴ ~~(S//NF)~~ [redacted] In making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

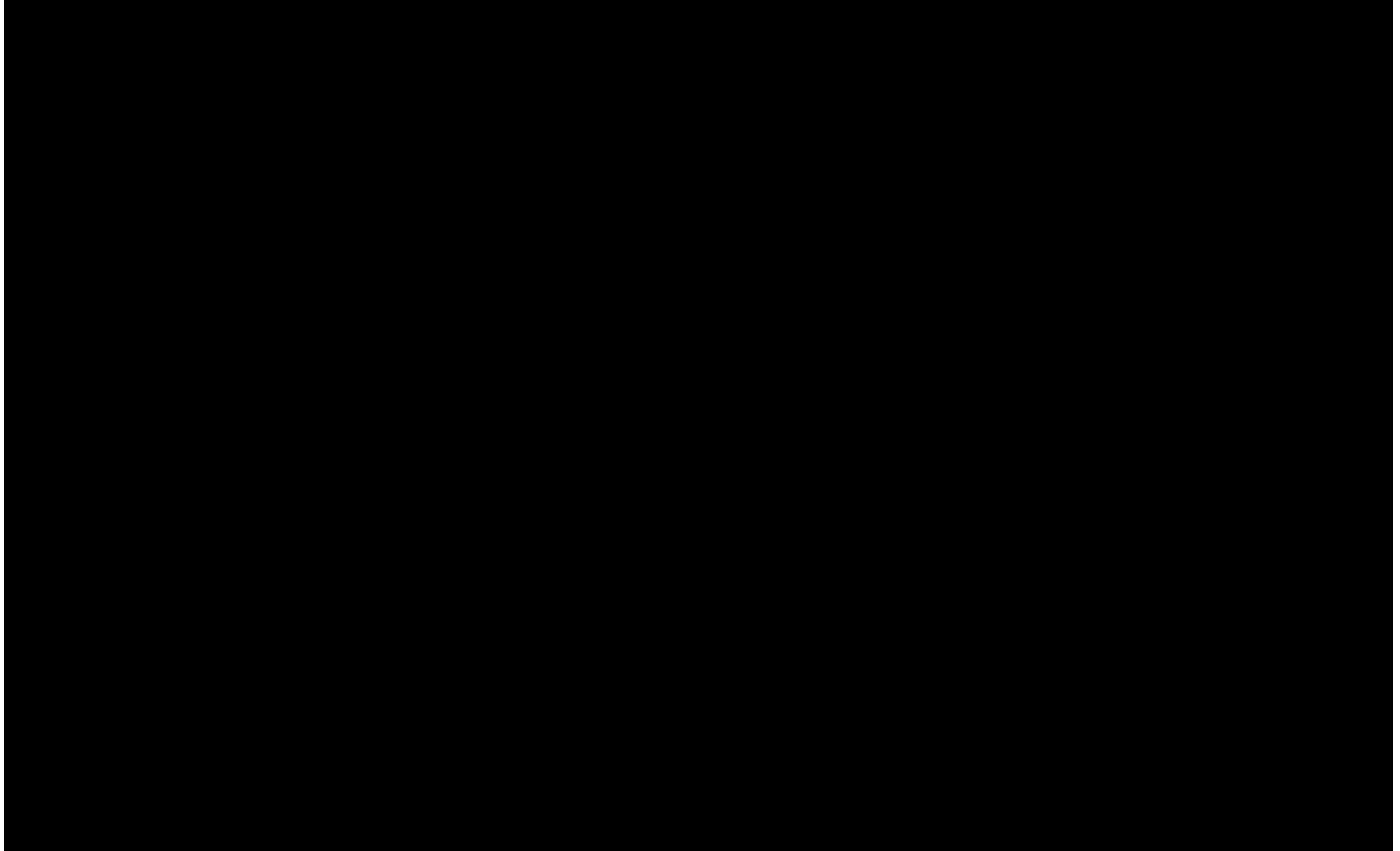
retained or transferred files that contain identified United States person information.³⁵ Beginning in the middle of the reporting period covered by the thirteenth Joint Assessment (dated September 2015), CIA began reporting the number of files CIA transferred to systems with broader access, instead 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 June 2015 through November 2015. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.³⁶ 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.

³⁵ (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.

³⁶



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 or retained [REDACTED] [REDACTED] of which were identified by CIA as containing a communication with potential United States person information. This is a [REDACTED] decrease in the number of files transferred or retained, when compared to the previous reporting period when [REDACTED] [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.³⁷ During this reporting period, there was one identified incident of noncompliance with CIA's minimization procedures, and no identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

³⁷ (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 day³⁸ during the reporting period:

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

Compliance incidents during reporting period (June 1, 2015 – November 30, 2015)	[REDACTED]
Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.53%

(U) The compliance incident rate continues to remain low, well below one percent. The compliance incident rate of 0.53% represents an increase from the 0.35% compliance incident rate in the prior reporting period, however, this increase is largely attributable to two types of errors discussed further below.³⁹ The number of notification delays remained low 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 0.50% which is still higher than the prior period’s 0.32%. This information is explained below and detailed in Figure 11.

(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.⁴⁰

³⁸ ~~(S//NF)~~ [REDACTED] he Attorney General’s Section 707 report provides further details with respect to any particular incident.

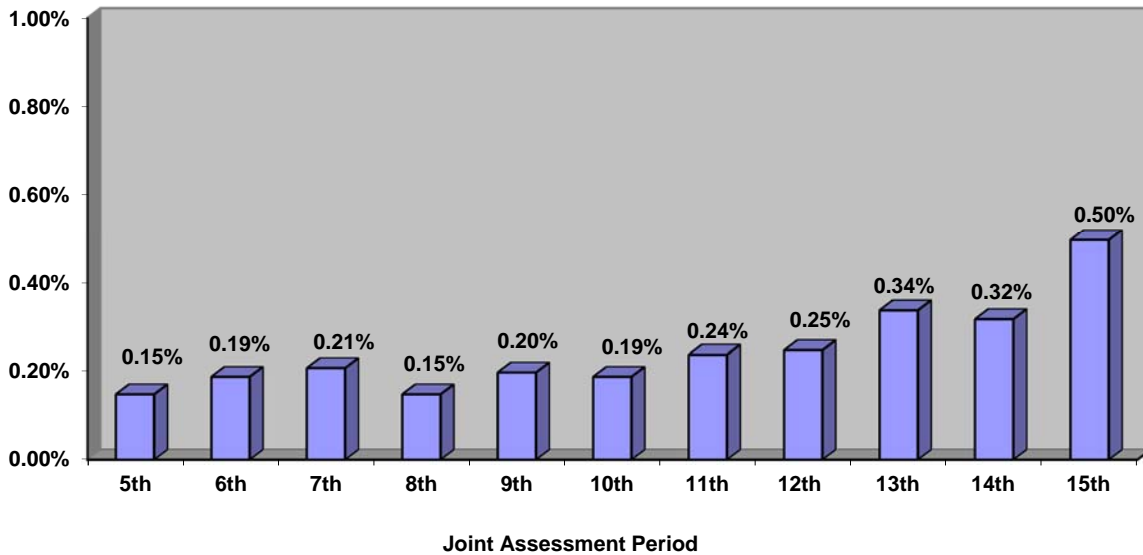
[REDACTED]

³⁹ [REDACTED]

⁴⁰ (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 0.50%, which is higher than what was reported in the prior reporting period (0.32%) but 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. In addition, although there was an increase in the compliance incident rate this period, NSA has taken steps to address some of the causes of these incidents, which are discussed further below.

(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.⁴¹
- (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.

⁴¹ (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

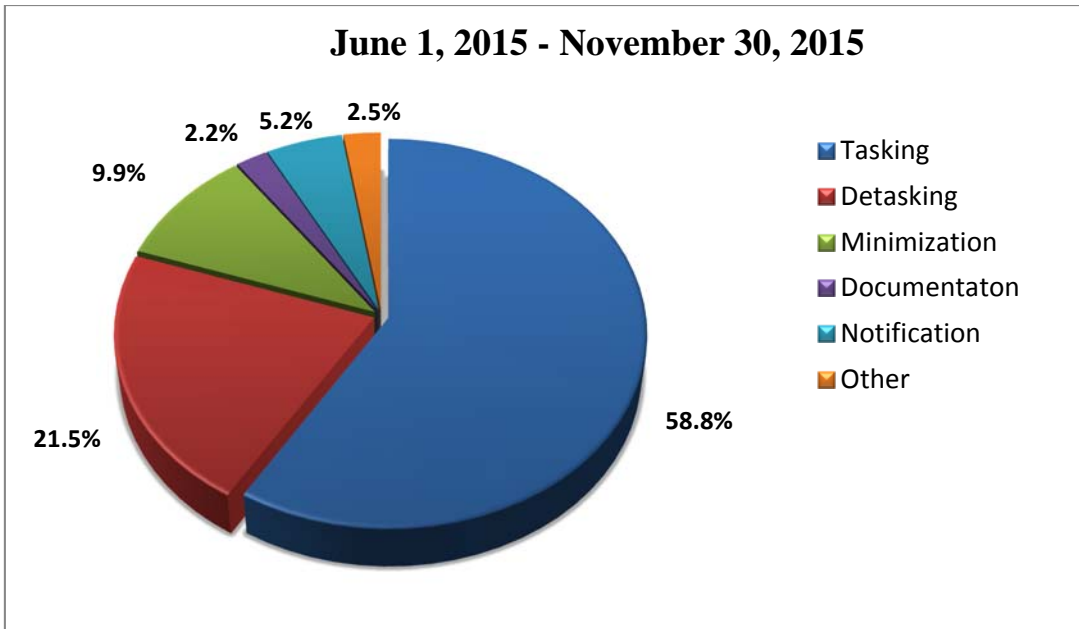
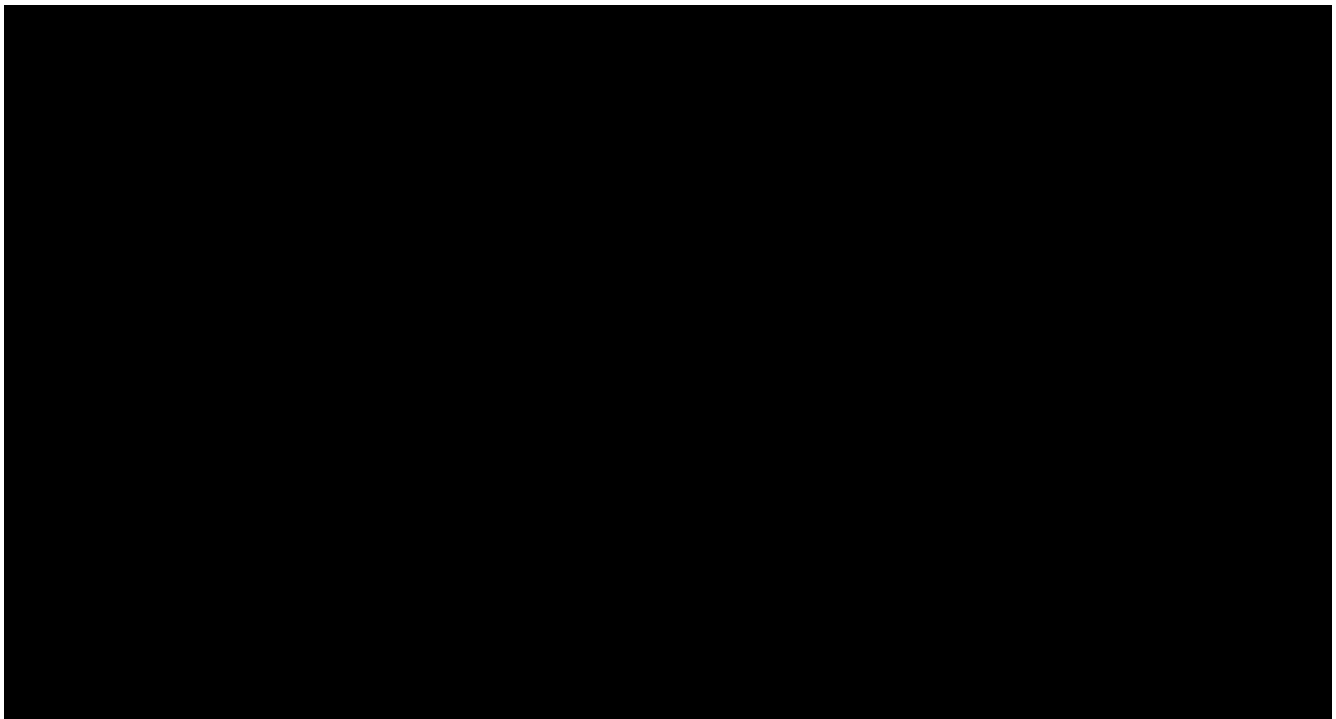


Figure 12B: ~~(S//NF)~~ Number of Compliance Incidents Involving the NSA Targeting and Minimization Procedures



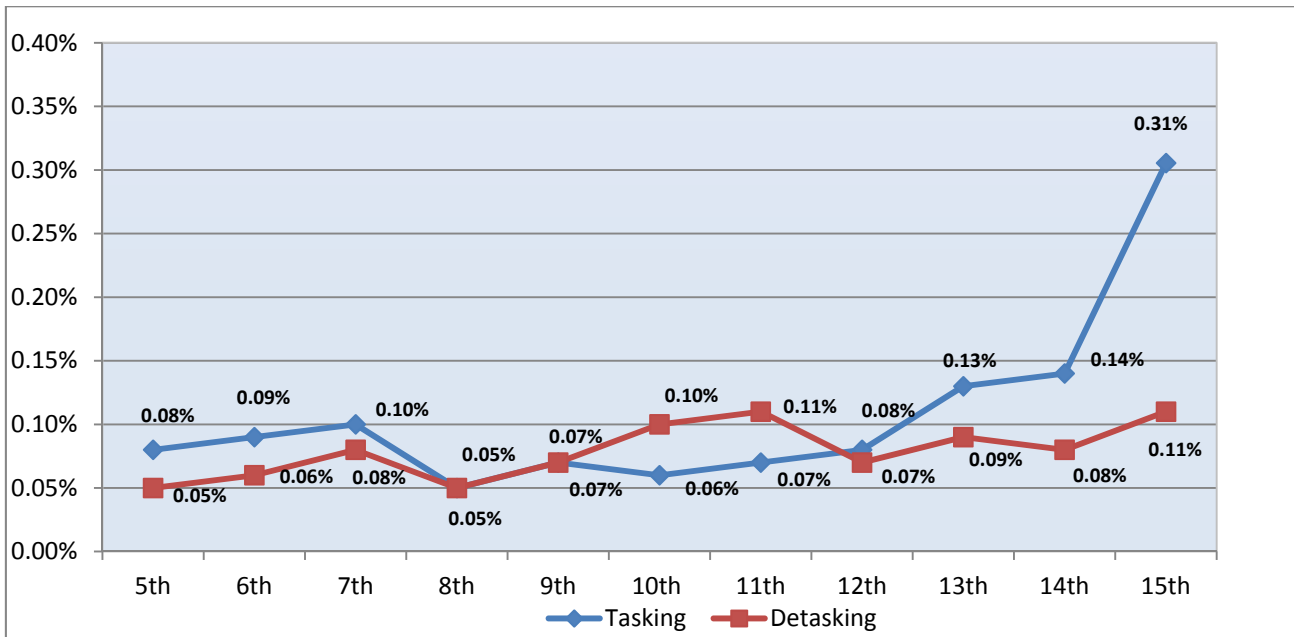
(U) As Figures 12A and B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, has been substantially reduced. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, incidents of noncompliance with minimization procedures 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]; detasking incidents increased [REDACTED]; minimization incidents increased [REDACTED]; documentation incidents decreased [REDACTED],⁴² and “other” category incidents decreased [REDACTED]. The number of notification delays decreased [REDACTED]. Additionally, as with the previous reporting period, there were no overcollection incidents in the current reporting period.

(U) The following chart, Figure 13, depicts the compliance incident rates, as compared to the average facilities on task, for tasking and detasking incidents over the previous reporting periods. 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.

⁴² ~~(S//NF)~~ The joint oversight team is examining whether it should revise the counting of documentation errors to address NSA’s revised targeting procedures. The targeting procedures approved by the FISC in November 2015 included a new documentation requirement that NSA provide a written explanation of the basis for the assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked. The revised targeting procedures with this new documentation requirement was made pursuant to a PCLOB recommendation, as discussed above. An update will be provided in the subsequent joint assessment as appropriate.

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.⁴³ The percentage of compliance incidents involving such detasking incidents has remained consistently low.⁴⁴

(U) With respect to FBI’s targeting and minimization procedures, incidents of non-compliance with the FBI targeting procedures decreased from the rate of 0.01% in the prior reporting period to a rate below 0.01% in the current reporting period.⁴⁵ The total number of

43

44 (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 the different incident rates are statistically significant, and note that the incident rate is consistently quite low.

45

identified minimization errors also remains low.⁴⁶ The joint oversight team assesses that FBI's overall compliance with its targeting and minimization procedures is a result of FBI's training and the processes it has designed to effectuate its procedures.

(U) Furthermore, there was one incident during this reporting period that involved CIA's minimization procedures, which is the same amount of 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)~~ Finally, there were no incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents a decrease from the [REDACTED] incidents 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.

(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 oversight team believes that analyzing the trends of these incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance. 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.

46 [REDACTED]

(U) In the subsections that follow,⁴⁷ this Joint Assessment examines some of the underlying causes of incidents of non-compliance, focusing on incidents in this period that contributed to the increased compliance incident rate of 0.53%. In the previous reporting period, the compliance incident rate was 0.35%, which was consistent with the historical compliance incident rate. While the current incident rate still remains well under 1%, the joint oversight team found its increase significant and ultimately determined that the overall incident rate was significantly impacted by two types of tasking errors. This Joint Assessment first begins by examining these two subsets of tasking incidents that contributed to a majority of the tasking errors, even though the majority of these tasking errors did not impact United States persons. This Joint Assessment then focuses on examining and explaining incidents that have the greatest potential to impact United States persons' privacy interests, even though those incidents represent a minority of the overall incidents.

(U) A. Errors That Resulted in the Increased Number of Tasking Incidents

(U) During this reporting period, the joint oversight team attributed the overall increase in incidents to an increase in two particular types of tasking incidents caused by agency personnel misapplying the requirements of NSA's targeting procedures; these accounted for 72% of all tasking incidents.⁴⁸ First, 49% of tasking incidents were caused by one particular target office misunderstanding the requirements of the targeting procedures.⁴⁹ Second, 23% of tasking errors involved NSA failing to conduct a necessary foreignness check (i.e. checking that a targeted user is reasonably believed to be located outside the United States) prior to tasking a facility or NSA allowing too long of a delay between the necessary foreignness check and the actual tasking of the facility.⁵⁰

(U) 1. Incidents that Contributed to 49% of the Tasking Errors Due to a Misunderstanding by a Single NSA Targeting Office

(U) As noted above, 49% of the tasking errors identified during this reporting period were attributed to a misunderstanding by a single target office. The joint oversight team discovered this incident⁵¹ as part of its bi-monthly oversight review of newly tasked facilities, all of which are reviewed by NSD. NSD requested that NSA provide additional information about the connection between the targeted users of certain tasked facilities and the particular certification under which those facilities were tasked. After additional research, NSA advised that this particular target office

⁴⁷ (U) While ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may nonetheless change with each joint assessment depending on the incidents that occurred in each reporting period and their respective underlying causes.

⁴⁸

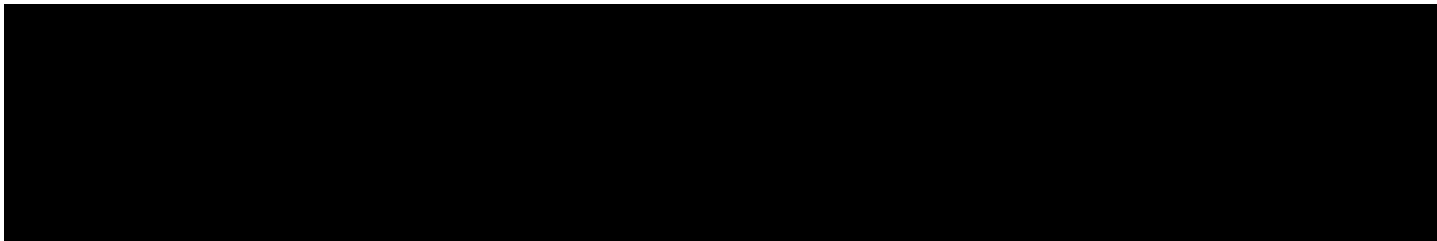
⁵⁰

⁵¹

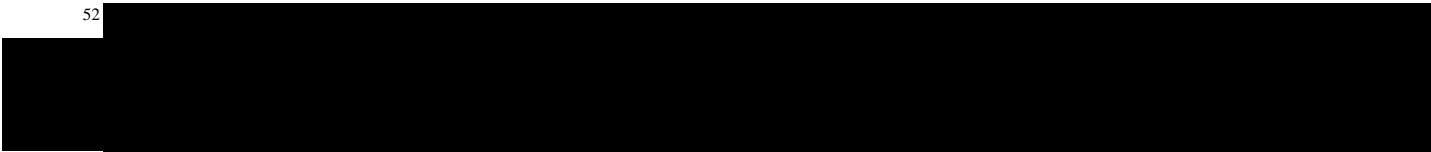
had erroneously tasked those facilities under circumstances in which it did not have sufficient information to assess that the user would possess, receive, and/or communicate foreign intelligence information about the certification under which those facilities were targeted.⁵² While NSA analysts in this office believed that the targeted users were appropriately connected to the certification under which they were tasked, those analysts erroneously failed to utilize additional NSA resources to support their assessment and, therefore, could not reasonably determine, as required by the targeting procedures, whether or not targeting those facilities would likely produce the requisite foreign intelligence information. As a result of this incident, NSA required the target office to retake the NSA's formal Section 702 online training course, and NSA issued guidance to all personnel involved in the Section 702 targeting process regarding the requirement in the targeting procedures that NSA must reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or likely communicate foreign intelligence information.

(U) 2. Incidents that Contributed to 23% of the Tasking Errors Due to Failing to Conduct the Required and Timely Foreignness Checks

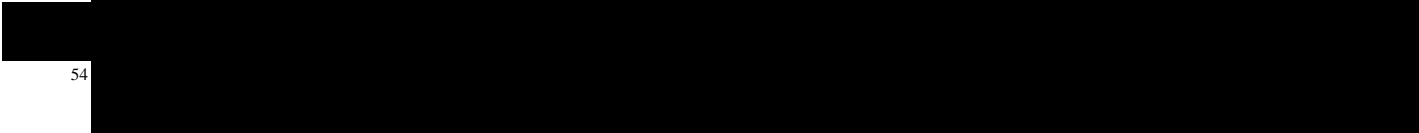
(U) In 23% of the tasking incidents,⁵³ NSA did not properly establish a sufficient basis to assess that the target was located outside the United States because NSA analysts either failed to conduct the required foreignness check or failed to conduct the required foreignness check in a timely manner. Even though these types of errors accounted for 23% of the tasking incidents during this reporting period, it was a decrease in these types of errors compared to the last reporting period (which was 56%).⁵⁴ In all of these incidents during the current reporting period, NSA advised that there was no indication that the selectors were used by a United States person or by someone in the United States. NSA further advised that the relevant personnel were reminded of the Section 702 tasking requirements. Additionally, in an attempt to reduce these types of tasking errors in the future, NSA conducted refresher training, beginning in October/November 2015, for all NSA targeting adjudicators about the required pre-tasking checks. The joint oversight team continues to work with NSA to ensure that appropriate additional training efforts are utilized to further reduce these types of tasking incidents.



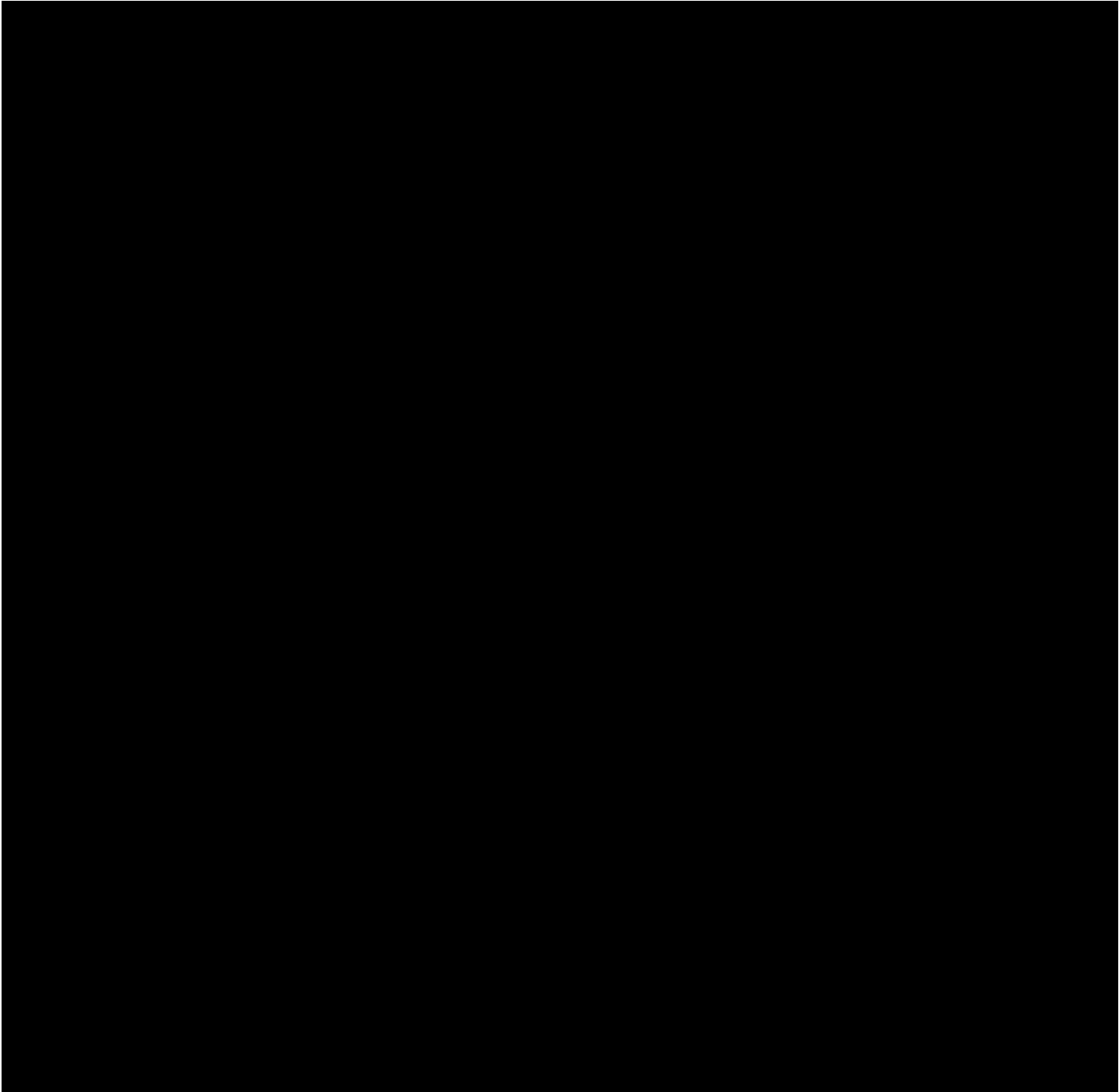
52



53

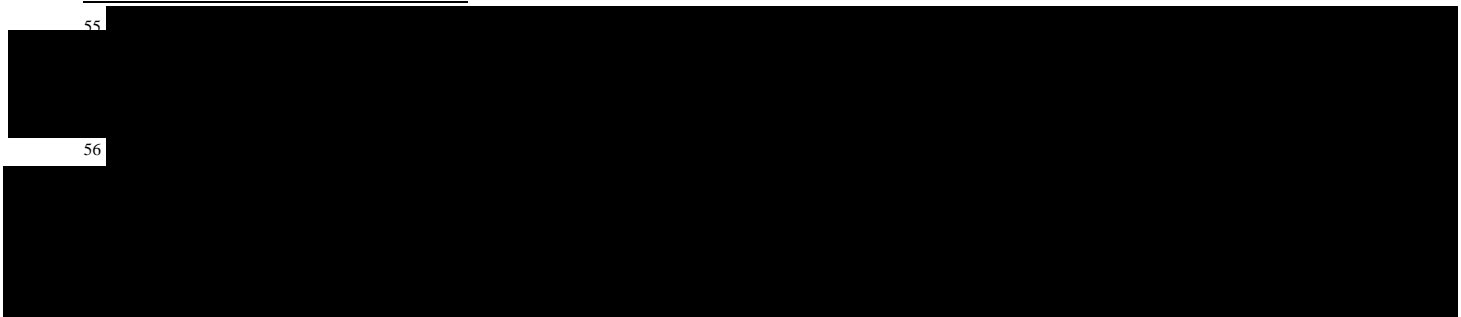


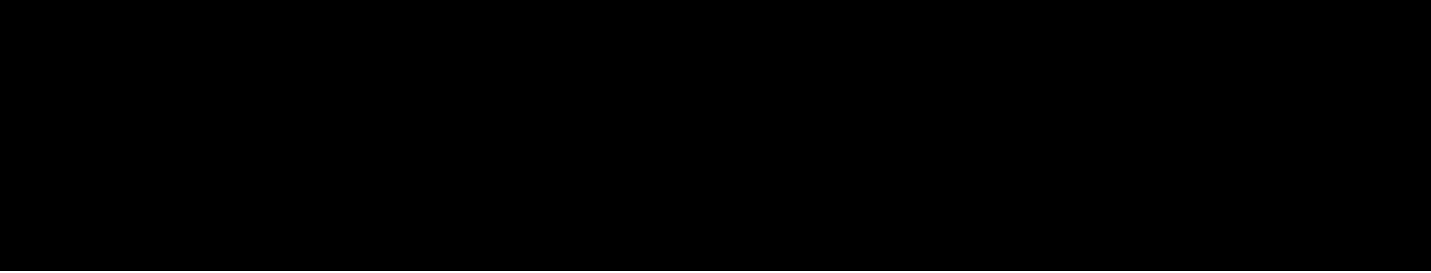
54



55

56



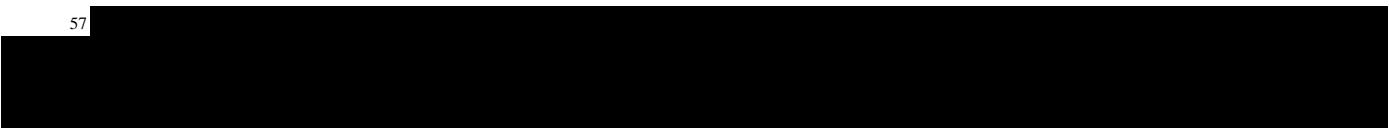


(U) C. Compliance Incidents Related to Incomplete Purges

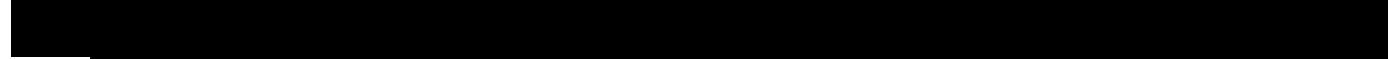
(U) During this reporting period, there was an increase in the number of incidents involving the incomplete purge of information as required by NSA’s Section 702 minimization procedures, whereas in the previous reporting period no such incidents occurred.⁵⁷ While this number of incidents is not entirely in line with historic reporting, as discussed further below, some of the incidents were the result of NSA proactively conducting purge verification assessments and are not further analyzed or discussed below (although the Section 707 report provides a detailed discussion of such).⁵⁸ However, discussed below, are those purge incidents where NSA’s technical processes for identifying data subject to purge were not fully detecting all collection that needed to be purged or were not completely purging the required information.⁵⁹ Furthermore, two additional incidents (discussed below) involved incomplete purges in specific systems – these two incidents had more substantial implications than other incidents and were the subject of multiple filings and compliance hearings before the FISC in connection with the 2015 Section 702 Certification renewal.⁶⁰

(U) The first step in any required purge is to identify what data must be purged. In some instances, NSA’s technical processes failed to properly identify the data required to be purged or failed to fully detect all of the data required to be purged (i.e. incomplete purges), which resulted in compliance incidents due to the incomplete removal of data subject to purge. To address these purge incidents affected by technical processes, NSA undertook activities to: (a) verify that data required to be purged has been removed from the applicable NSA systems⁶¹ (i.e. purge verification assessments) and (b) identify and resolve issues with its purge process when incomplete purges are identified. For example, NSA has continued to conduct purge verification assessments by comparing a sample of data that was added to NSA’s Master Purge List (MPL)⁶² between a certain

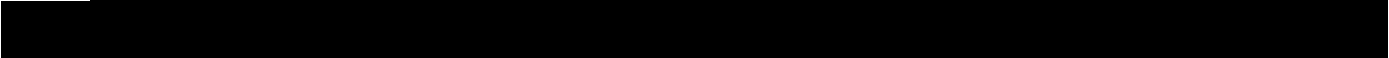
57



58



59



60

⁶¹ (U) These applicable NSA systems are known as SIGINT Collection Source Systems of Record (SC-SSRs). Any system designated by NSA as an SC-SSR must employ a purge protocol to verify that information is purged when the system receives a request to destroy SIGINT information that NSA is not authorized to retain.

⁶² (U) The Section 707 report provides further details as to the operation of the MPL.

date range with the data in an NSA system. The purpose is for NSA to identify whether the underlying data has in fact been purged from NSA's systems as required. In addition, NSA performed a full comparison of the MPL with the data in NSA's SC-SSRs. As a result of this MPL comparison process, NSA has identified incomplete purges in some of its SC-SSRs.⁶³ NSA has been able to identify causes for these incomplete purges and has worked to develop solutions to address the root causes.

(U) Two incidents involving incomplete purges had more substantial implications than the other purge incidents.⁶⁴ These two incidents were the subject of multiple filings and compliance hearings before the FISC in connection with the 2015 Section 702 Certification renewal and were addressed by the FISC in its *November 6, 2015 Memorandum Opinion and Order*.

(U) In the first incident, the Government explained that two particular NSA Mission Management Systems (MMS)⁶⁵ had not historically conducted required purges of records from those systems. The first MMS had been marking and limiting access to Section 702-acquired data subject to purge. However, this MMS had not deleted or aged-off the data subject to purge; furthermore, domestic communications that had been marked for deletion in other systems and added to NSA's MPL had not been historically purged from this MMS.⁶⁶ NSA re-designed this MMS so that it would properly remove records subject to purge going forward. Additionally, NSA completed the removal in this MMS of historic Section 702-acquired data subject to purge and the historic domestic communications that had been marked for deletion and added to the MPL. However, NSA continues to work to develop a technical solution for this MMS to age-off applicable Section 702-acquired information.

(U) In the same incident, the Government explained that that a second MMS had been improperly purging information and that the incomplete purges potentially affected information collected pursuant to Section 702.⁶⁷ NSA identified a system error in this second system as the cause for these incomplete purges. To remedy this error, NSA redesigned this second MMS to compare, on a daily basis, data in its system with all identifiers listed on the MPL. Thus, records associated with object identifiers listed on the MPL in purge state are now being appropriately deleted from this second MMS. This second MMS had also failed to properly age-off FISA-acquired information. This system now ages off data older than one year and no longer contains FISA-acquired information. The joint oversight team assesses that this incident highlights the importance for agency personnel to ensure that databases used to store Section 702 FISA-acquired information are configured appropriately to meet purge, deletion, and age-off requirements. This incident also demonstrates the need to have agency personnel work with the joint oversight team to

63

64

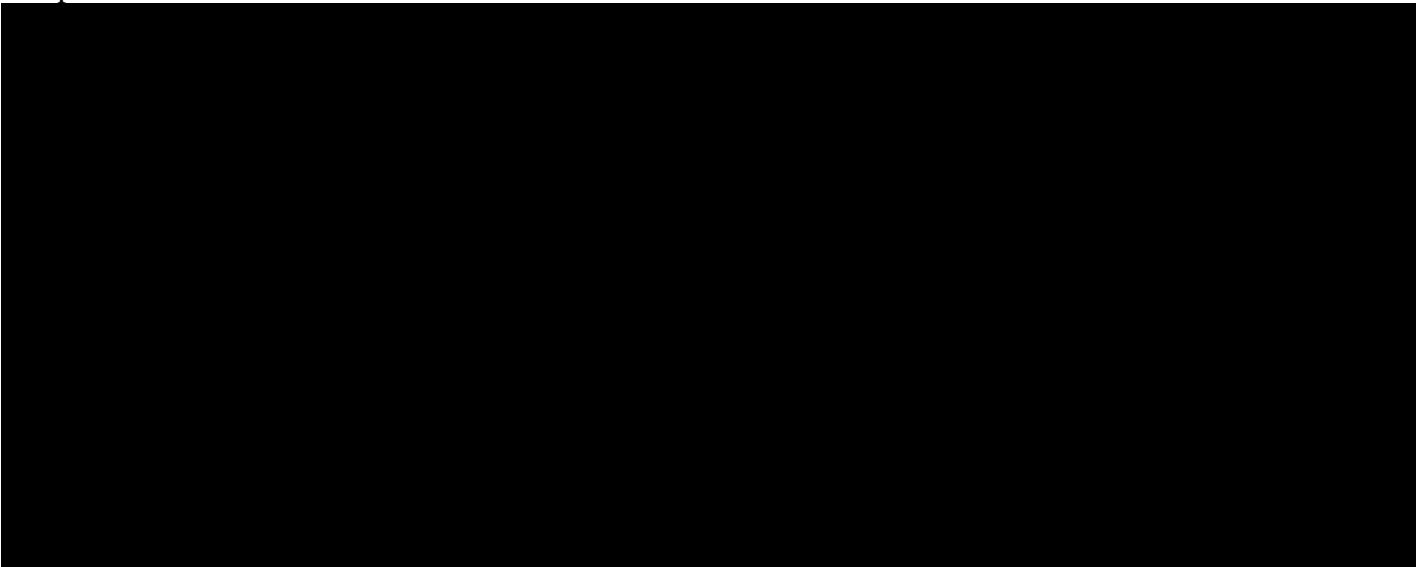
65

66

67

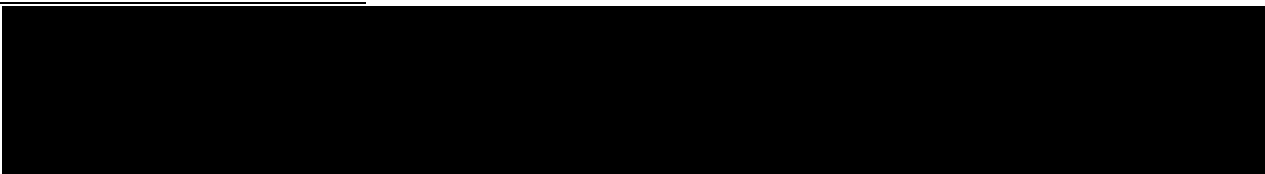
try to address potential issues in systems before those systems actually contain Section 702-acquired information.

(U) In the second more substantial incident,⁶⁸ the Government reported that Section 702-acquired information subject to purge or age-off was being erroneously kept in two other NSA MMS (separate systems from those detailed above).⁶⁹ Here, the first MMS is used in the *pre*-tasking process where NSA analysts most commonly use it as part of a determination of whether a facility can be properly tasked under Section 702. The second MMS is used in the *post*-tasking process where NSA analysts use it to perform checks to identify indications that a Section 702 target may be located in the United States. If these systems do not function properly, NSA analysts may not have the appropriate information at hand to fulfill the requirements of its targeting procedures to ensure that NSA reasonably believes the tasked facility is used by a non-United States person located outside the United States.



(U) Following a hearing during which the FISC addressed this particular incident, the FISC required the Government to justify the retention and use of data that was otherwise subject to purge in these two MMS databases.⁷⁰ After receipt of the Government's justification, the FISC addressed this matter in its *November 6, 2015 Memorandum Opinion and Order*. The FISC agreed that NSA's Section 702 minimization procedures do not prohibit NSA from keeping data in these two MMS databases that is derived from domestic communications placed on the MPL (i.e. subject to purge) for the purpose of collection avoidance. However, the FISC voiced concern as to whether the retention of other categories of information subject to purge in those two MMS databases comply with NSA's targeting and minimization procedures and, thus, ordered additional Government reporting on this topic. Subsequently, the Government reported that NSA would delete from these two MMS databases all data collected as a result of unauthorized electronic surveillance as well as all other categories of information subject to purge pursuant to its targeting and

68
69
70



minimization procedures. NSA detailed for the FISC a three-phase plan to effectuate required age-off, historic purge and prospective compliance with purge requirements.

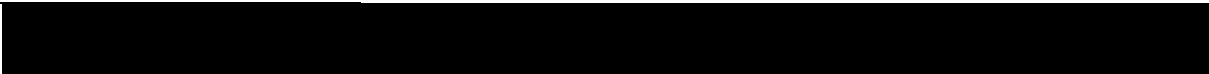
(U) The joint oversight team believes that these compliance incidents and other historical CIA, FBI, and NSA purge-related incidents indicate that the Government must remain vigilant to ensure the appropriate and timely removal of data. As with prior Joint Assessments, the joint oversight team believes it is important for NSA to carefully consider the potential impacts on the purge process when NSA designs and updates its systems. Because the identification and destruction of relevant data can be complex, the joint oversight team also believes that NSA must continue to regularly monitor and re-evaluate the functioning of relevant systems. Finally, the joint oversight team continues to remain focused working with all three agencies to ensure the appropriate purging of data. For example, during this last reporting period, the joint oversight team continued to have conference calls and in-person meetings with NSA and FBI as it pertained to their purging of data.

(U) D. Effect of Other Technical Issues

(U) There were a small number of compliance incidents resulting from technical issues (other than the purge incidents discussed above) during this reporting period. Technical issues potentially have larger implications than other incidents because technical issues: often involve more than one facility; can remain undetected and uncorrected for a long period of time; and can proliferate dramatically in a short time period, including across numerous interconnected systems. 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.

(U) Specifically, the technical issues that resulted in delayed detaskings were caused by data becoming corrupted, data not being properly processed due to a server backlog, and system errors.⁷¹ In these instances, the technology and systems failed to function as designed, and, thus, the systems failed. This resulted in delayed detasking incidents, whereby NSA was unable to timely detask facilities. NSA subsequently corrected these technical issues. Additionally, none of the users of the facilities at issue were believed to be United States persons.

71



(U) In another incident, NSA discovered that, due to a technical issue, (1) one NSA system failed to generate the tasking record (i.e. tasking sheet) for NSD and ODNI to review to ensure NSA compliance with NSA targeting procedures, and (2) an NSA system failed to receive tasking information that enables NSA to conduct required post-tasking analysis.⁷² Once a facility has been appropriately tasked, NSA has the obligation to ensure, post-tasking, that the facility remains appropriately tasked - i.e. that NSA reasonably believes that the non-United States person user of the tasked facility continues to be located outside the United States and that the tasking will provide foreign intelligence information. NSA subsequently provided the tasking sheets to the joint oversight team who is reviewing them to determine that the facilities contained on those sheets were appropriately tasked. This technical issue was corrected in October 2015.

(U) E. Effect of Human Errors⁷³

(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 4% of the tasking errors made in this reporting period, which is a decrease from the previous reporting period, in which typographical errors accounted for 8% of the tasking errors.⁷⁴ Furthermore, no such incidents 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 delays⁷⁵ from this reporting period were the result of inadvertent errors, such as an NSA analyst detasking some, but not all, of a target's facilities that required detasking.⁷⁶ As discussed below, approximately 21% of the

72

⁷³ (U) This section discusses other human errors that caused compliance incidents unrelated to the significant number of tasking errors discussed in an earlier section.

74

⁷⁵ (~~U//FOUO~~) This percentage is consistent with the percentage of these types of detasking delays reported in the prior Joint Assessment.

76

detasking delays were the result of faulty analysis or misunderstanding of procedures.⁷⁷ 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 purged.

(U) NSA's minimization procedures prescribe rules for using United States person identifiers to query Section 702-acquired data including that: (a) the queries be designed in a manner "reasonably likely to return foreign intelligence information;" (b) the queries are first approved in accordance with NSA's internal procedures; and (c) the queries of Internet communications acquired through NSA's upstream collection techniques are prohibited. During this reporting period, approximately 56% of the minimization procedures errors involved non-compliance with the minimization rules regarding queries (whereas it was approximately 78% in the previous reporting period).⁷⁸ As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization procedures

(U) Specifically, during this reporting period, just over half of the query incidents involved overly broad queries.⁷⁹ These overly broad query errors are typically traceable to a typographical or comparable error in the construction for the query. For example, an overly broad query can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overly broad results as a result of the query. As with previous reporting periods, there were no incidents of an analyst purposely running a query for non-foreign intelligence purposes against Section 702-acquired data identified during the reporting period.

(U) The remaining query incidents involved NSA analysts: (a) using United States person identifiers which had not been approved pursuant to NSA's internal procedures to query Section 702-acquired data; (b) exceeding the scope of the authorization provided under NSA's internal procedures; and/or (c) using approved United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques. For example, in one incident, a NSA analyst received the appropriate approval to use a United States person identifier to query Section 702-acquired data (excluding upstream). However, due to a misunderstanding, the analyst continued to use the United States person identifier as a query term past the approval's expiration date. NSA discovered the error over three months later; the NSA target office discontinued the queries the same day the error was discovered. NSA advised that all results from the unauthorized use of the United States person identifier as a query term were deleted. NSA further advised that the relevant personnel were reminded of the Section 702 query requirements.

77

78

79

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

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

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

~~(S//SI//NF)~~ In prior Joint Assessments, the joint oversight team suggested that NSA consider making changes to its tasking tool and query tool.⁸⁰ Specifically, the joint oversight team proposed two changes be made to NSA's tasking tool. NSA subsequently implemented both proposed changes and modified its tasking tool. First, NSA's tasking tool was configured in such a manner that [REDACTED] could 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.⁸¹ NSA modified its tasking tool so that [REDACTED] now require the analysts to consciously and manually change the instruction before further targeting. NSA believes that this change will result in a decrease in the unintentional retasking of facilities [REDACTED]s. Second, in processing [REDACTED] requests from CIA and FBI, detasked facilities previously could have been erroneously retasked without application of the NSA targeting procedures unless NSA personnel verified that the facility [REDACTED] was currently subject to Section 702 acquisition; one such error occurred during this reporting period.⁸² To resolve this issue, NSA modified its targeting tool to

⁸⁰ (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 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 (hereafter the *HPSCI October 2015 letter*). This *HPSCI October 2015 letter* also requested that the report evaluate "the possibility of including additional [REDACTED] mechanisms for analyzing the foreignness of a target pre- and post-tasking."

(U) On February 16, 2016, ODNI provided HPSCI with a report in response to the *HPSCI October 2015 letter*. The ODNI report, *Assessment of Oversight and Compliance with Targeting Procedures* (hereafter the *ODNI February 2016 report*), evaluated the process by which IC elements task foreign intelligence targets under Section 702, including *providing* an update on the status of proposed modifications DOJ and ODNI suggested in previous Joint Assessments that NSA make to its tools related to tasking and querying.

81

82

prevent those types of [REDACTED] tasking requests to proceed; now the modification requires a NSA employee to [REDACTED] specify that a tasking request is being requested pursuant to Section 702. This modification was completed in January 2016.⁸³

(U) While modifying NSA's tasking tool would have prevented these two methods of erroneously retasking facilities, these modifications would eliminate only 2% of the tasking errors that occurred in this reporting period. Such modifications would have eliminated 5% and 8% of tasking errors in the prior two reporting periods, respectively. Thus, these types of modifications could potentially reduce the already very small overall compliance incident rate.

(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.⁸⁴ In response to this recommended modification, NSA developed a potential solution and plans to test and implement it during calendar year 2016. Specifically, the solution being developed for NSA data repositories containing unevaluated and unminimized Section 702 information will require analysts to document whether the query being executed 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.⁸⁵

~~(U)~~ Additionally, 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's Section 702 Report Recommendation 9(4)*. In the Section 707 Report, the Department of Justice reports (a) the number of metadata queries that use a United States person identifier and (b) the number of United States person identifiers approved for content queries. [REDACTED]

[REDACTED] NSA subsequently declassified these numbers relating to calendar year 2015 metrics so as to report those numbers publicly as part of ODNI's *2015 Transparency Report*.

⁸³ (U) As it pertains to recommended modifications to NSA's tasking tool, the *ODNI February 2016 report* indicated that NSA was reviewing the recommendation and planned to engage in further discussions with DOJ and ODNI. The above information updates the information in the *ODNI February 2016 report*.

⁸⁴ [REDACTED]

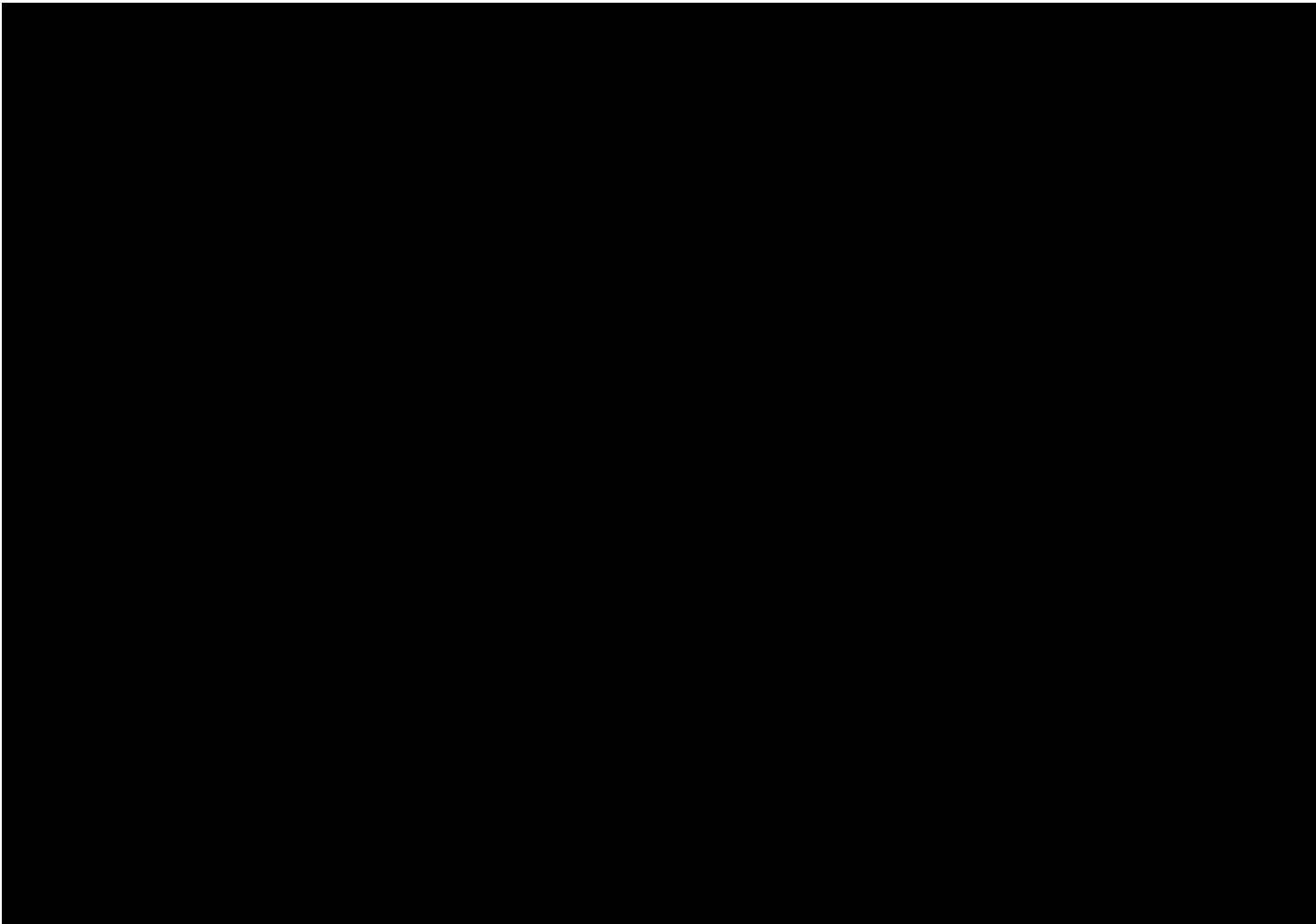
⁸⁵ (U) As it pertains to recommended modifications to NSA's query tool, the *ODNI February 2016 report* indicated that NSA planned to test and implement this recommendation during calendar year 2016 and also explained how the new modified compliance control mechanism would function.

(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 (including the incident described above where one office misunderstood or misapplied the targeting procedures resulting in a significant number of tasking incidents from a single office)⁸⁶ were attributable, to varying degrees, to a misunderstanding or misapplication of these rules. The overall number of such incidents compared to the number of targeting, detasking, and minimization decisions made by Government personnel remains very low, and the particular aspects of the procedures misunderstood or misapplied were diverse. The below-described incidents are examples of agency personnel misapplying the requirements of NSA's targeting or minimization procedures, which resulted in either the inadvertent targeting of a U.S. person or the dissemination of information of or concerning a U.S. person that did not meet the requirements in the minimization procedures.

(U) For example, in two incidents, NSA personnel did not understand what efforts they were required to undertake to ascertain whether a targeted user was a United States person prior to tasking. These errors resulted in United States persons being erroneously tasked; however, upon discovering the tasking errors, NSA detasked the users' facilities and ensured that all necessary purge requirements were completed. NSA further advised that the relevant personnel have been reminded of the Section 702 tasking requirements. In a third incident, an analyst did not understand the minimization requirements with regard to disseminating information concerning a United States person.

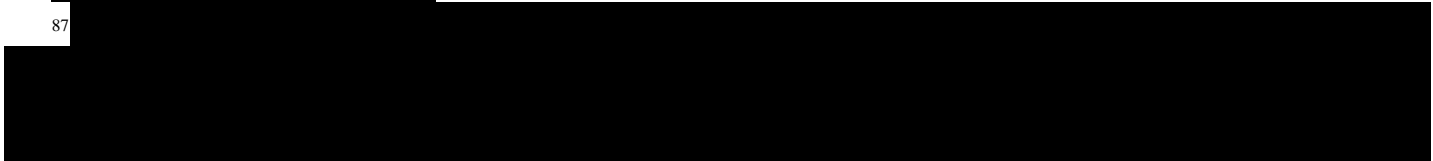
86



(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) G. 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 6% (down from the prior reporting period's 15%) of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.⁸⁸ 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.

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

~~(S//NF)~~ During this reporting period, there was only one incident involving noncompliance with the CIA minimization procedures, which is the same number that occurred during the previous reporting period. [REDACTED]

(U) CIA's sole compliance incident involved the untimely destruction of Section 702-acquired data as is required by its minimization procedures.⁸⁹ CIA's Section 702 Minimization Procedures require that CIA delete unminimized communications that may contain United States person information no later than five years from the expiration date of the Section 702 certification authorizing the collection. In this incident, the applicable data that was required to be deleted was not deleted due to a technical issue and that data remained in one of CIA's systems for less than two weeks past the deletion deadline. CIA advised that it made no use of the information that was improperly retained for the short period of time.

(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

⁸⁸ [REDACTED]

⁸⁹ [REDACTED]

period decreased from 0.01% to almost zero. The one targeting incident in this reporting period was a process issue that was narrow in impact, and did not involve the targeting of a United States person or person located in the United States.⁹⁰

~~(S//NF)~~ The minimal number of incidents involving noncompliance with FBI's minimization procedures resulted from misapplication or misunderstanding of the procedures by FBI employees and from technical issues.⁹¹ For example, one of the minimization incidents involved the improper querying of Section 702-acquired data which was caused by an FBI employee misunderstanding the rule.⁹² Specifically,

[REDACTED]

Subsequently, FBI reminded the employee of the minimization procedures' requirement concerning queries.

[REDACTED]

90

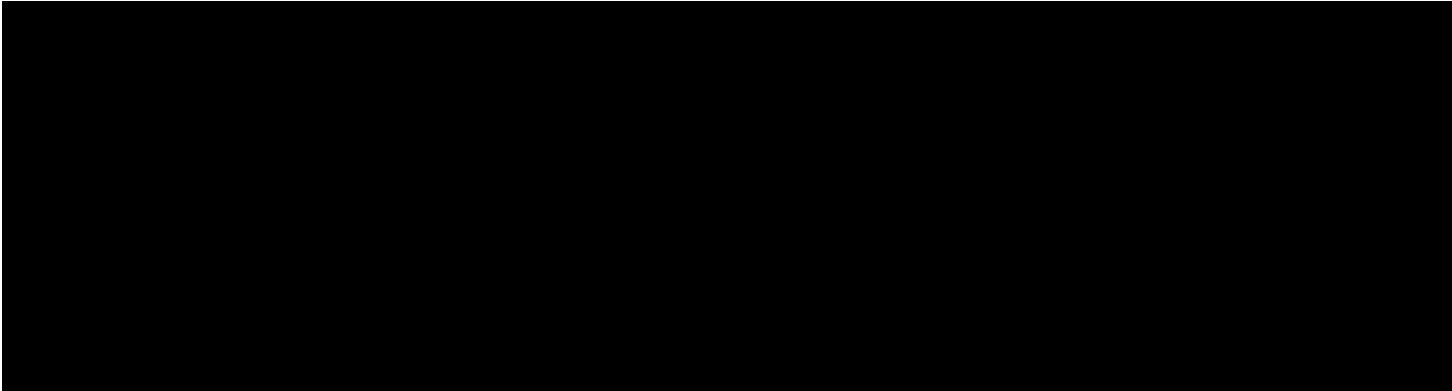
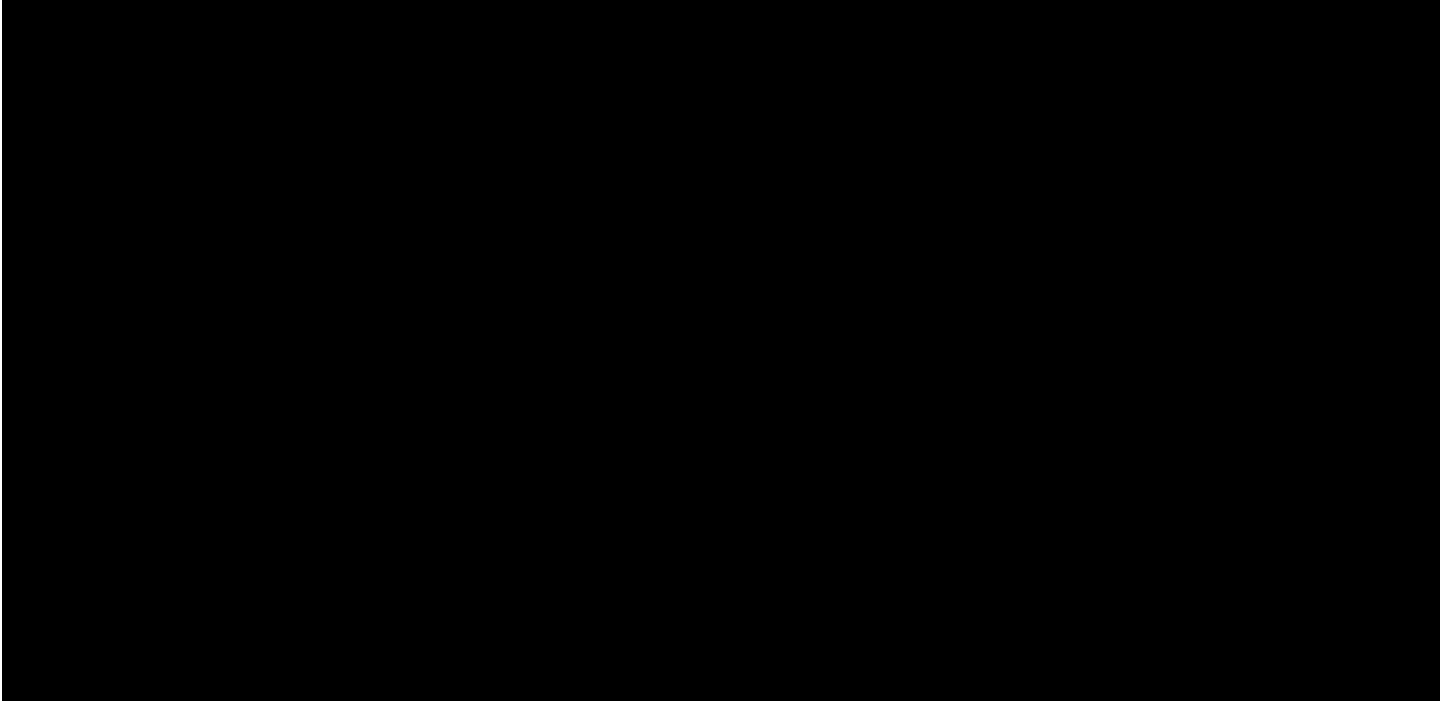
[REDACTED]

91

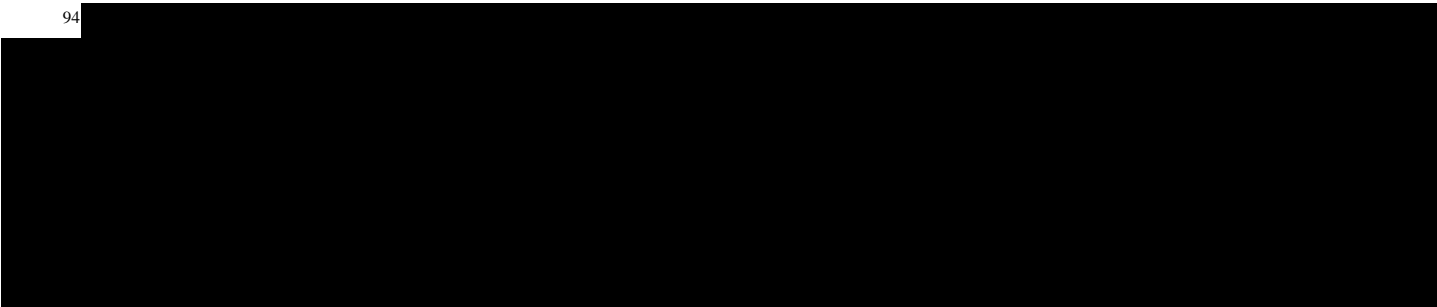
92

93

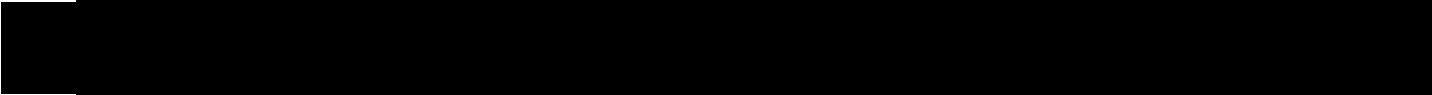
[REDACTED]



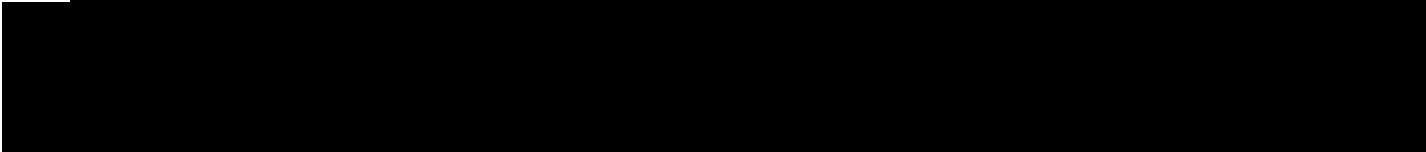
94




95



96





(U) The previous joint assessment discussed two minimization errors that involved the improper dissemination of United States person information.⁹⁷ While no such errors of this type occurred during this current reporting period, the previous joint assessment explained that FBI had recalled five of the seven improper disseminations and further explained that, at that time, FBI was continuing to discuss the remaining two improper disseminations with NSD. This discussion between FBI and NSD continued through this and subsequent reporting periods.

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

(U) During this reporting period, there were no incidents (as opposed to minimal incidents during the last reporting period)⁹⁸ 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.

(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

97



98

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

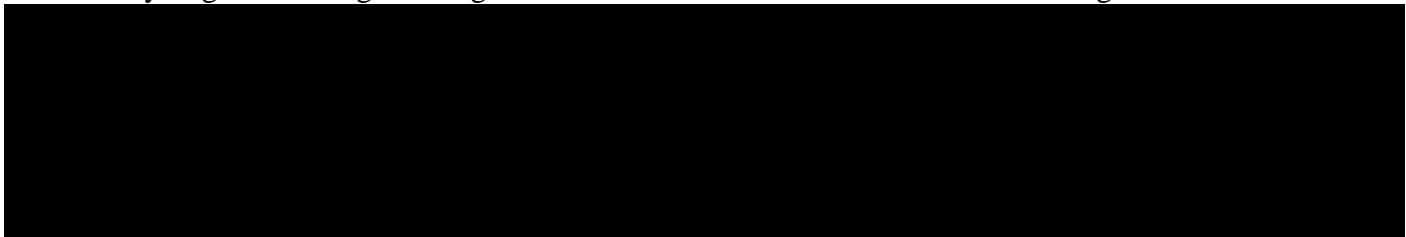
APPENDIX A

(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).¹ As required by Section 702, those targets must be non-United States persons² reasonably believed to be located outside the United States.

(~~S//NF~~) During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:



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

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

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

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in 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.⁵ 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.

(U) Once information is collected from these tasked facilities, it is subject to FISC-approved minimization procedures. NSA’s minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA’s minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA’s targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.⁶

(U) NSA’s targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably

⁵

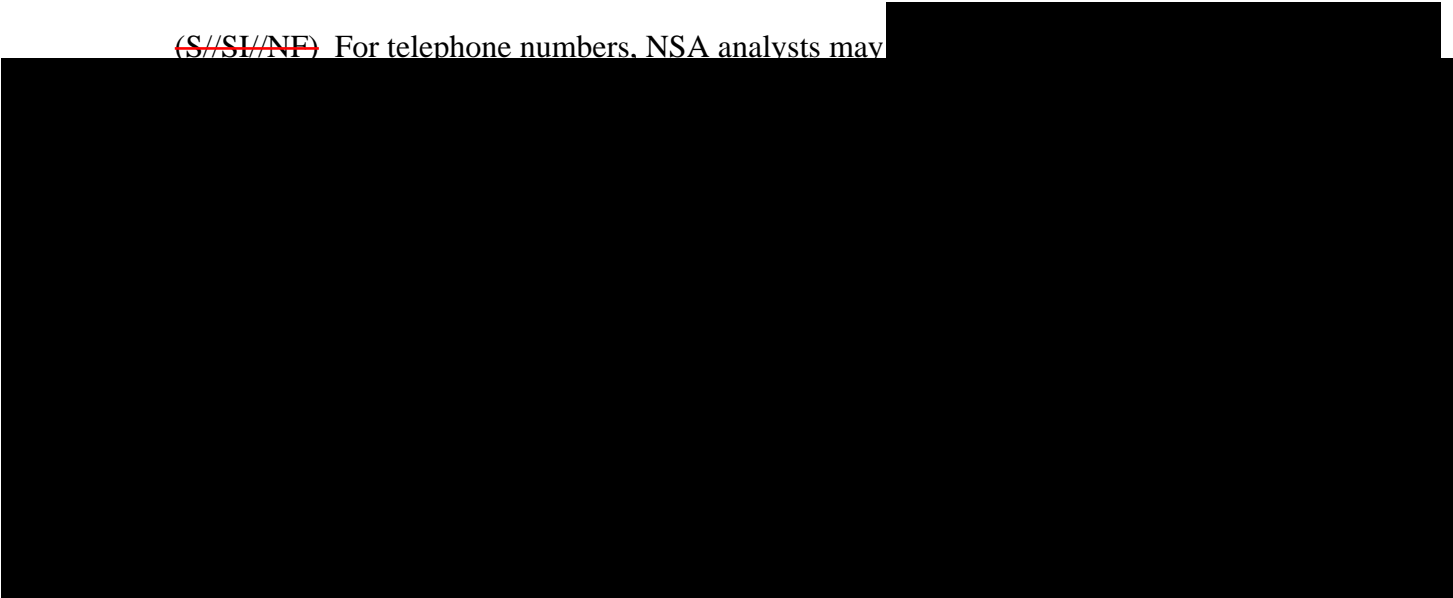
⁶ ~~(S//NF)~~ As noted in the Section 707 Report, with respect to ongoing acquisitions from certain electronic communication service providers

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



7



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

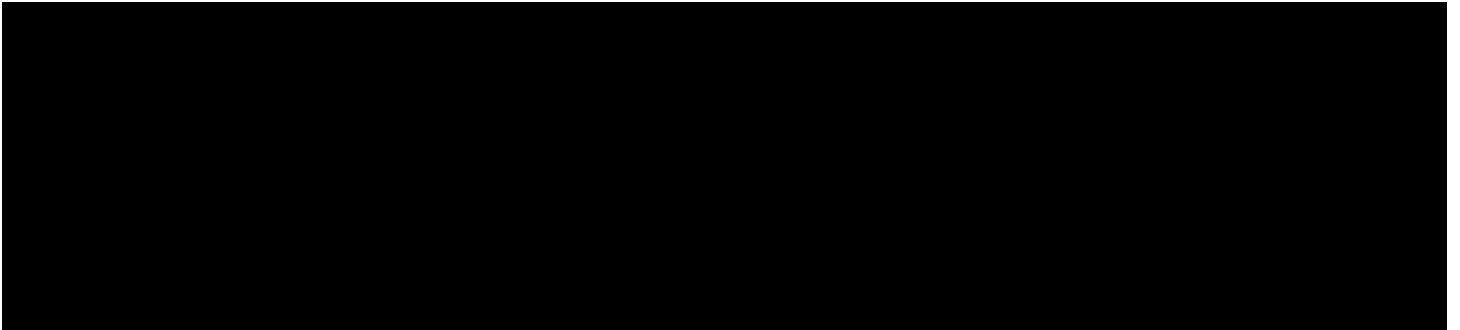
9



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



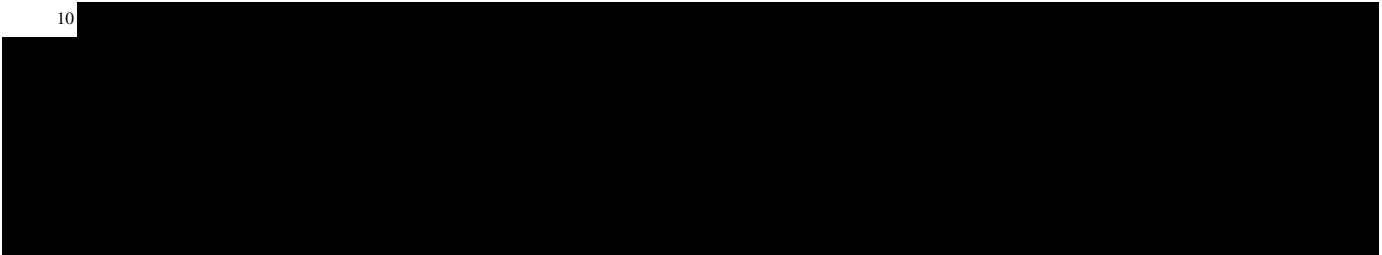
(U) C. Post-Tasking Checks



~~(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],¹¹ a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm 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]

[REDACTED] Should traffic not be viewed in at least once every 30 days, a notice is

¹⁰



¹¹ ~~(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

(~~S//NF~~)¹² 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's targeting procedures also require analysts to identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information and provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory.

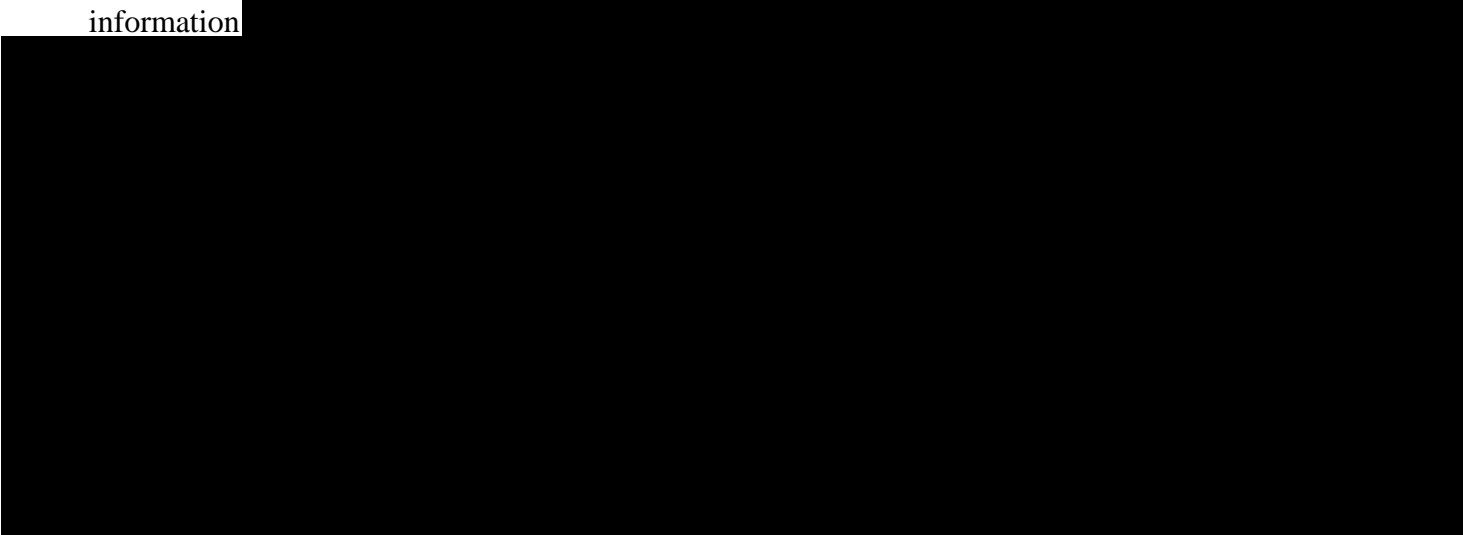
(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user 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]

¹² (~~U//FOUO~~) This paragraph was erroneously marked (U) in the previous joint assessment (i.e. the 14th Joint Assessment) but was appropriately marked (~~S//NF~~) in prior joint assessments.

█ 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, █ the analyst's foreignness explanation, the targeting rationale, █. 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 biannually.

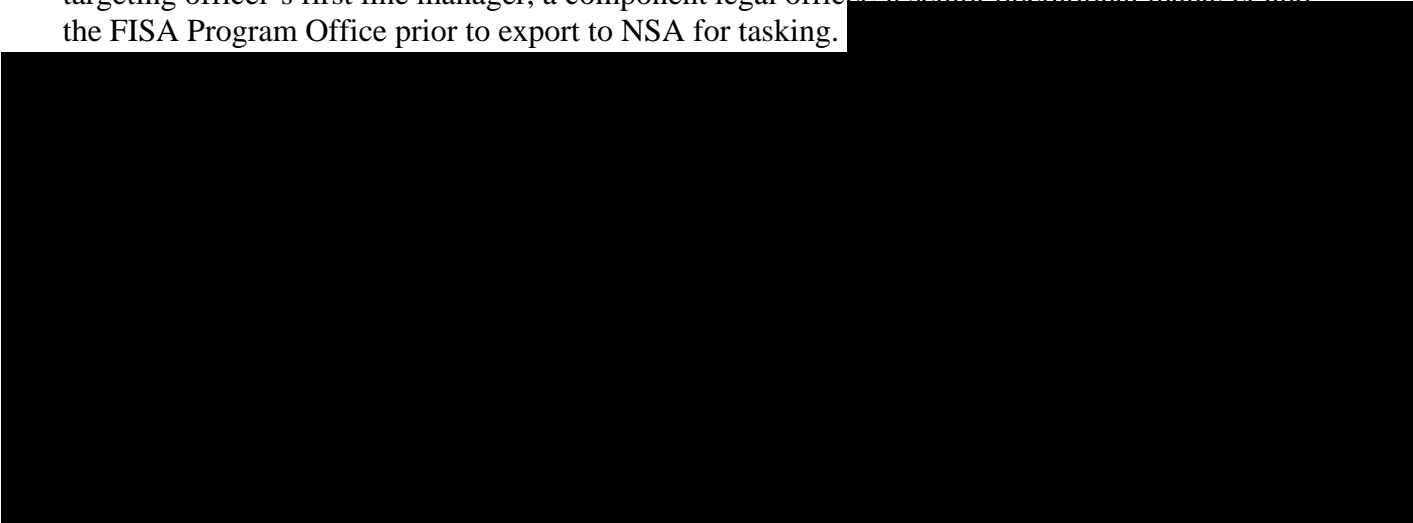
(U) **II. Overview - CIA**

(U) **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.



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.



(S//NF) 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 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 to [REDACTED] intelligence targets to NSA for the acquisition of in-transit communications.

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

[REDACTED] The FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a

United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate [REDACTED], FBI must then apply its own, additional procedures, which require FBI to review NSA's conclusion of foreignness [REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

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

[REDACTED]

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

[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] TS has the lead responsibility in FBI for [REDACTED] requests [REDACTED]. XTS personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests [REDACTED]. XTS also has the lead responsibility for facilitating FBI's nominations to NSA [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]. In addition, NSD conducts training on the Section 702 minimization Procedures at multiple FBI field offices each year.

~~(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.