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

Reporting Period: December 1, 2016– May 31, 2017

October 2018

[redacted]

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

OCTOBER 2018

TABLE OF CONTENTS

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

(U) FACT SHEET

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Joint Assessments

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as "Joint Assessments," and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of October 2018, eighteen Joint Assessments have been submitted.

(U) Joint Assessment Basics:

- *(U) Why is the Joint Assessment required?* The FISA Amendments Act of 2008 (50 U.S.C. § 1881(l)(1)) requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702.
- *(U) What period is covered by a Joint Assessment?* Each Joint Assessment covers a six-month period: December 1 – May 31 or June 1 – November 30.
- *(U) Who receives it?* Each Joint Assessment is submitted to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees.
- *(U) What is being assessed?* The Attorney General and the DNI jointly assess the Government's compliance with FISC-approved "targeting" and "minimization" procedures.

(U) Highlights from 18th Joint Assessment:

- *(U) No intentional violations*. Consistent with previous Joint Assessments, no instances of intentional circumvention or violation of those procedures were found during this reporting period.
- *(U) Continued focused efforts to implement Section 702 in a compliant manner.* This Joint Assessment reports that the agencies continued to implement the procedures in a manner that reflects a focused and concerted effort by Intelligence Community (IC) personnel to comply with the requirements of Section 702.
- *(U) Compliance incident rate remains low.* The compliance incident rate remained low, which is consistent with the compliance incident rate reported for other reporting periods. The majority of incidents were caused by a misunderstanding of the procedures, failure to conduct the required checks, technical issues, and inadvertent human errors.

- *(U) What are targeting procedures and minimization procedures?* Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information.

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

(*When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)*

- *(U) What compliance and oversight efforts underlie the Joint Assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, and constitutional requirements. A joint oversight team consisting of experts from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) oversee these measures. Each incident of non-compliance (i.e. compliance incident) is documented, reviewed by the joint oversight team, remediated, and reported to the FISC and relevant congressional committees. The Joint Assessment summarizes trends and assesses compliance (including calculating the compliance incident rate for the relevant reporting period) and may include recommendations to help prevent compliance incidents or increase transparency.

- *(U) What government agencies are involved with implementing Section 702?* The National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC). Each Joint Assessment discusses how these agencies implement the authority.

- *(U) Why is the Joint Assessment classified?* The Joint Assessment is classified to allow us to provide the congressional oversight committees a complete assessment of the Section 702 program, while at the same time protecting sources and methods. They are carefully redacted for public release in the interest of transparency.

- *(U) What is the format of the Joint Assessment?* The Joint Assessment generally contains an Executive Summary, five sections, and an Appendix. Beginning with the 16th Joint Assessment, this fact sheet has been included. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts, and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews of the targeting and minimization procedures. Section 4 describes compliance trends. The Joint Assessment describes the extensive measures undertaken by the Government to ensure compliance with court-approved targeting and minimization procedures; to accurately identify, record, and correct errors; to take responsive actions to remove any erroneously obtained data; and to minimize the chances that mistakes will re-occur.

- *(U) What are the types of compliance incidents discussed?* Generally, the Joint Assessment groups incidents into six or seven categories. Categories 1-4 (tasking incidents, detasking incidents, notification delays, and documentation errors) discuss non-compliance with targeting procedures. Category 5 discusses incidents of non-compliance with minimization procedures, such as erroneous queries of Section 702-acquired information using United States person identifiers. Sometimes a category discussing incidents of overcollection is included. Additionally, the last category is a catch-all category for incidents that do not fall into one of the other categories. The actual number of the compliance incidents is classified; the percentage breakdown of those incidents is unclassified and reported in the Joint Assessment. Additionally, because Section 702 collection occurs with the assistance of U.S. electronic communications service providers who receive a Section 702(h) directive, the Joint Assessment includes a review of any compliance incidents by such service providers.

(*When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)*

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

October 2018

Reporting Period: December 1, 2016 – May 31, 2017

(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 eighteenth joint compliance assessment of the Section 702 program. This assessment covers the period from December 1, 2016 through May 31, 2017 (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 (DOJ) submitted the Section 707 Report on September 7, 2017; 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 DOJ'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 (0.37%) of the overall collection activity. This represents a decrease from the last Joint Assessment's rate of 0.88% and still remains 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 represents 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")[1] 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 (DOJ) 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 18th joint compliance assessment under Section 702, covering the period December 1, 2016 through May 31, 2017 (hereinafter, the "reporting period").[2]

(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

[1] (U) On January 18, 2018, Congress reauthorized FAA with the FISA Amendments Reauthorization Act of 2017, with an effective date of December 31, 2017; it codified new requirements concerning Section 702. However, because the Act was signed into law after this current joint assessment's reporting period, any new requirements and how the government implements those requirements are not discussed in this joint assessment; they will be addressed in subsequent joint assessment(s), as appropriate.

[2] (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on September 7, 2017, as required by Section 707(b)(1) of FISA (hereafter Section 707 Report). This 18th Joint Assessment covers the same reporting period as the 18th Attorney General's Section 707 Report.

General's Acquisition Guidelines") were adopted by the Attorney General, in consultation with the DNI, on August 5, 2008.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information.[3] Four agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC).[4] An overview of how these agencies implement the authority appears in Appendix A of this assessment.

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

[redacted]

[4] (U) During this reporting period, NCTC was authorized by the FISC to receive unminimized Section 702 data. Specifically, in an opinion issued by the FISC on April 26, 2017, the FISC approved new minimization Section 702 procedures for NCTC (2016 NCTC Minimization Procedures). Both the FISC opinion and the 2016 NCTC Minimization Procedures were posted, in redacted form, on ODNI's website *IC on the Record* on May 11, 2017. The 2016 NCTC Minimization Procedures reflect that NCTC may now receive unminimized Section 702 information. Prior to the approval of the 2016 NCTC Minimization Procedures, NCTC was not authorized to receive unminimized Section 702 information pertaining to counterterrorism. However, under both the prior minimization procedures and the current procedures, NCTC ingests data from FBI systems that contain minimized Section 702 information. Because NCTC is not a law enforcement agency, it may not receive disseminations of Section 702 information that contain evidence of a crime, but which have no foreign intelligence value.

(U) In summary, the joint oversight team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period. As in the prior Joint Assessments, the joint oversight team has not found the compliance incidents that have been reported or otherwise identified during this reporting period to be an intentional or willful attempt to violate or circumvent the requirements of the Act.[5] 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, CIA, and NCTC[6] each handle Section 702-acquired data in accordance with their own minimization procedures.[7] 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.

---

[5] ~~(S//NF)~~ As reported to Congress in the 19th Semiannual Report of the Attorney General Concerning Acquisitions Under Section 702 of the Foreign Intelligence Surveillance Act, produced on March 5, 2018, NSD identified a compliance incident involving certain queries conducted by an FBI linguist. That Semiannual Report noted that the Government is investigating whether those noncompliant queries were conducted intentionally. The Government has completed its investigation. Although some of the noncompliant queries were conducted during the reporting period of this Joint Assessment, they were discovered by NSD and reported to the Court outside the period of this Joint Assessment. Now that the investigation is complete, NSD is in the process of updating the Court regarding this matter. Because the incident occurred outside the current reporting period and because the Government has yet to provide the Court with an updated report, this incident will be discussed in the next Joint Assessment.

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

[7] (U) Each agency's Section 702 targeting and minimization procedures are approved by the Attorney General and reviewed by the FISC. On May 11, 2017, the DNI released, in redacted form, the current 2016 minimization procedures for NSA, FBI, CIA, and NCTC, as well as the current 2016 targeting procedures, in redacted form, for NSA and FBI. These procedures are posted on ODNI's *IC on the Record* website. Past years' versions of the minimization procedures were previously released and remain on *IC on the Record* as part of the DNI's commitment to the IC's Principles of Transparency.

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

(U) I. Joint Oversight of NSA

(U) Under the process established by the Attorney General and Director of National Intelligence's certifications, all Section 702 targeting is initiated pursuant to the NSA targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities[8] (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,[9] as well as the investigation and reporting of specific compliance incidents. During this reporting period, NSD and ODNI conducted the following onsite reviews at NSA:

Figure 1: (U) NSA Reviews

Date of Review	Taskings/Minimization Reviewed
February 24, 2017	December 1, 2016 – January 31, 2017
April 28, 2017	February 1, 2017 – March 31, 2017
June 16, 2017	April 1, 2017 – May 31, 2017

(U) Figure 1 is UNCLASSIFIED.

(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 reporting period. These reports

[8] (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 in 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.

[9] (U) The NSA targeting procedures require that the onsite reviews occur approximately every two months.

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 reporting period to NSD and ODNI. 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 prepares a detailed report 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 to ascertain the basis for NSA's foreignness determinations. The joint oversight team also reviews whether the tasking was in conformance with the targeting procedures and statutory requirements. 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 the NSA Office of Compliance for Operations (formerly known as the NSA's Signals Intelligence Directorate (SID) Office of Oversight and Compliance),[10] 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 currently reviews all of the serialized reports (ODNI reviews 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) NSA's Section 702 minimization procedures provide that any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures,[11] which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information, as defined in FISA. With respect to queries of Section 702-acquired *content* using a

[10] (U) NSA's SID Oversight & Compliance office was replaced by NSA's Office of Compliance for Operations (OCO) on August 31, 2016, as part of NSA's internal reorganization.

[11] (U) NSA released these internal procedures in response to a Freedom of Information (FOIA) case filed in the U.S. District Court, Southern District of New York, ACLU v. National Security Agency, et al. (hereafter the ACLU FOIA), and they were posted, in redacted form, on ODNI's *IC on the Record* on April 11, 2017.

United States person identifier, the joint oversight team reviews all approved United States person identifiers to ensure compliance with NSA's minimization procedures.[12] 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.[13]

(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.[14] 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.

(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 includes the results of those visits in the bimonthly NSA review reports discussed above.

---

[12] (U) On May 2, 2017, the DNI publicly released ODNI's fourth annual Transparency Report[s]*: Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016* (hereafter the *2016 Transparency Report*). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(A)), the *2016 Transparency Report* provided the "estimated number of search terms concerning a known United States person used to retrieve the unminimized contents of communications obtained under Section 702" (emphasis added) for the entire calendar year of 2016.

[13] (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(B)), the *2016 Transparency Report* provided the "estimated number of queries concerning a known United States person used to retrieve the unminimized noncontents [(i.e. metadata)] information obtained under Section 702" (emphasis added) for the entire calendar year of 2016.

[14] (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, 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.

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
March 9 and 10, 2017	December 1, 2016 – January 31, 2017
May 8 and 10, 2017	February 1, 2017 – March 31, 2017
June 28 and 30, 2017	April 1, 2017 – May 31, 2017

(U) Figure 2 is UNCLASSIFIED.

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

(U) As a part of the onsite reviews, the joint oversight team examines documents related to CIA's retention, dissemination, and querying of Section 702-acquired data. The team reviews a sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with CIA 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. In addition, NSD and ODNI review CIA's written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications to assess whether those queries were compliant with CIA's minimization procedure requirements that such queries are reasonably likely to return foreign intelligence information, as defined by FISA. [15]

~~(S//NF)~~ CIA may receive [redacted][16] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. Additionally, and 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 those visits are included in the bimonthly NSA review reports discussed previously. CIA

[15] ~~(S//NF)~~ As of [redacted] CIA had [redacted], such that NSD and ODNI will be able to review CIA's written foreign intelligence justifications for queries using United States person identifiers of the noncontents of unminimized Section 702-acquired communications. NSD and ODNI's assessments of such queries will be included in future joint assessments, as appropriate.

[16] [redacted]

has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those 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.[17] 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 those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(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. Those acquisitions must be conducted pursuant to FBI's Section 702 targeting procedures.

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

~~(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 those 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 at FBI headquarters of FBI's compliance with its targeting procedures and bimonthly reviews at FBI headquarters of FBI's compliance with its minimization procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section

[17] (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.

707(b)(1)(F) of FISA. For this reporting period, onsite reviews at FBI Headquarters were conducted on the following dates:

Figure 3: (U) FBI Reviews

Date of Visit	Targeting and Minimization Reviewed
February 7 and 8, 2017	December 2016 targeting decisions
March 15 and 16, 2017	January 2017 targeting decisions
April 11 and 12, 2017	February 2017 targeting decisions and December 1, 2016 through February 28, 2017, minimization decisions
May 3 and 4, 2017	March 2017 targeting decisions
June 20 and 21, 2017	April 2017 targeting decisions and March 1 through May 31, 2017, minimization decisions
June 27 and 28, 2017	May 2017 targeting decisions

(U) Figure 3 is UNCLASSIFIED.

(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.[18] 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.

(U) At the FBI reviews, 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 by the relevant FBI headquarters unit of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States person information.

(U) In addition to conducting minimization reviews at FBI headquarters, during this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention, query, and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During those field office reviews, NSD reviewed a sample of retention decisions made by FBI personnel in Section 702 cases and a sample of disseminations of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons. NSD also reviewed a sample of queries by FBI personnel in FBI systems that contain raw (unminimized) FISA-acquired information, including Section 702-acquired information. Those reviews ensure that the queries complied with the requirements in FBI's FISA minimization procedures, including its Section 702 minimization procedures. In addition, as a result of a Court-ordered reporting requirement in the

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

FISC's *November 6, 2015 Memorandum Opinion and Order*[19] for queries conducted after December 4, 2015, NSD reviews those queries to determine if any such queries were conducted solely for the purpose of returning evidence of a crime. If such a query was conducted, NSD would seek additional information as to whether FBI personnel received and reviewed Section 702-acquired information of or concerning a United States person in response to such a query. Pursuant to the FISC's opinion and order, such queries must subsequently be reported to the FISC.

(U) As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at 14 FBI field offices during this reporting period and reviewed cases involving Section 702-tasked facilities.[20] ODNI joined NSD at a subset of those reviews; ODNI received written summaries regarding all of the reviews from NSD regardless of whether ODNI was in attendance. Those 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 those activities complied with applicable minimization procedures. The last annual process review occurred in March 2017.

~~(S//NF)~~ As further described in detail in Appendix A, FBI nominates potential Section 702 targets to NSA. [redacted] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those 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.[21] Those 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. Compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

---

[19] (U) The FISC's November 6, 2015 Opinion and Order approved the 2015 FISA Section 702 Certifications. On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, this *Opinion and Order* on the ODNI public website *IC on the Record*.

~~(S//NF)~~ The title of the FISC's November 6, 2015 opinion is [redacted]

[20] ~~(S//NF)~~ During those field office reviews, NSD reviewed [redacted] cases involving Section 702-tasked facilities.

[21] (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 previously played a more limited role in implementing Section 702, 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." For the majority of this reporting period, under these limited minimization procedures, NCTC was not authorized to receive unminimized Section 702 data, but NCTC had access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism. 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 minimized Section 702 information received from FBI. NSD conducted the most recent review at NCTC for this reporting period in May 2017.

~~(S//NF)~~ As referenced in footnote 4, during this reporting period, NCTC was authorized to receive unminimized Section 702 information pertaining to counterterrorism. NCTC's processing, retention, and dissemination of such information is subject to its 2016 Minimization Procedures. Unlike [redacted] NCTC does not directly engage in targeting or acquisition, nor does it nominate potential Section 702 targets [redacted] NCTC may receive [redacted] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to NCTC's minimization procedures. NCTC has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Because NCTC now acquires unminimized Section 702 information, the joint oversight team conducts onsite visits at NCTC, and the results of those visits are included in bimonthly NCTC review reports. The onsite reviews focus on NCTC's application of its Section 702 minimization procedures. In July 2017, which is outside this reporting period, NSD and ODNI conducted the first onsite review at NCTC to assess NCTC's handling of unminimized Section 702-acquired communications pursuant to its 2016 Section 702 minimization procedures. The July 2017 onsite review at NCTC will be discussed in a subsequent joint assessment, as appropriate.

(U) As a part of the onsite review, the joint oversight team examines documents related to NCTC's retention, dissemination, and querying of Section 702-acquired data. The team reviews all communications acquired under Section 702 that have been minimized and retained by NCTC, irrespective of whether it contains United States person information. Reviewers ensure that communications have been properly minimized and discuss with personnel issues involving the proper application of NCTC's minimization procedures. The team also reviews all NCTC disseminations of information acquired under Section 702. In addition, NSD and ODNI review NCTC's written foreign intelligence justifications for all queries of the content of unminimized Section 702-acquired communications.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with NCTC's minimization procedures or other agencies' procedures in which NCTC is involved.[22] Investigations are coordinated through the NCTC Compliance and Transparency Group and NCTC Legal, a forward deployment component of the DNI Office of General Counsel (DNI OGC), and when necessary, may involve requests for further

[22] (U) Insofar as NCTC 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 NCTC.

information; meetings with NCTC Legal, analytical, and/or technical personnel; or the review of source documentation. All compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(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 those 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. Additionally, NSD and ODNI conduct weekly telephone calls with NSA to address outstanding compliance matters and work through the process of understanding those matters and reporting incidents to the FISC.

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

(U) VI. Training

(U) In addition to specific instructions to personnel directly involved in 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 updated in November 2016.[23] All NSA personnel who require access to Section 702 data are required to complete this course on an annual basis in order to gain and/or maintain that access. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders and compliance advisories to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. Those training reminders and compliance advisories are e-mailed to individual analysts and targeting adjudicators and maintained on internal agency websites[24] where

[23] (U) The transcript associated with this training, dated August 2016, was posted, in redacted form, on *IC on the Record* on August 22, 2017, in response to the aforementioned ACLU FOIA case titled, *OVSC1203: FISA Amendments Act Section 702* (Document 17, NSA's Training on FISA Amendments Act Section 702).

[24] (U) These documents were posted, in redacted form, on ODNI's *IC on the Record* on August 23, 2017, in response to the aforementioned ACLU FOIA case: *NSA's 702 Targeting Review Guidance* (Document 10), *NSA's 702 Practical Applications Training* (Document 11), *NSA's 702 Training for NSA Adjudicators* (Document 12), and *NSA's 702 Adjudication Checklist* (Document 13).

personnel can obtain information about specific types of Section 702-related issues and compliance matters.

(U) 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 required training program for anyone handling raw Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Furthermore, CIA has issued guidance to its personnel about how to properly conduct United States person queries that are reasonably likely to return foreign intelligence information, *see USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data*.[25]

(U) FBI has similarly continued implementing its online training programs regarding Section 702 nominations, minimization, and other related requirements. Completion of those 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 on the attorney-client privileged communication provisions of FBI's minimization procedures.[26] NSD training at FBI field offices also included training on the reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications. As discussed above, this 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 United States person that was reviewed by FBI personnel.

(U) NCTC provides training on the NCTC Section 702 Minimization Procedures to all of its personnel who may have access to raw Section 702-acquired information. NCTC uses a training tracking system through which NCTC can verify that its users have received the appropriate Section 702 training before being given access to raw Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed raw Section 702-acquired information in its system to confirm that those personnel who access raw Section 702-acquired information had received training on the NCTC Section 702 Minimization Procedures.

(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

[25] (U) In response to the aforementioned ACLU FOIA case, CIA's guidance document was posted, in redacted form, on ODNI's *IC on the Record* on April 11, 2017, *see* ACLU April 2017 Production 5, Document 15 "CIA's United States Person Query Guidelines for Personnel."

[26] (U) This specific training began before and continued after the current reporting period of December 1, 2016 – May 31, 2017.

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,[27] 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.[28]

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

(U) Figure 4 is classified TOP SECRET//SI//NOFORN

[27] (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 the ODNI most recently in its *2016 Transparency Report*. The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified numbers provided in the Transparency Report estimate the number of Section 702 *targets*. As noted in the Transparency Report, the number of 702 'targets' reflects an estimate of the number of known users of particular facilities, subject to intelligence collection under those Certifications. The classified number of facilities account for those facilities subject to Section 702 acquisition *during the current six month reporting period*, whereas the Transparency Report estimates the number of targets affected by Section 702 *during the calendar year*.

[28] (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 Figure 4.

~~(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.[29] This represents a 27.4% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period.[30] [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.[31] Classified Figure 5 charts the total monthly numbers of newly tasked facilities since 2010.

Figure 5: ~~(TS//SI//NF)~~ New Taskings by Month (Yearly Average for 2011 through Nov. 2016)

[redacted]

(U) Figure 5 is classified TOP SECRET//SI//NOFORN.

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

[30] [redacted]

[31] (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 facilities that had been previously tasked for collection, were detasked, and then retasked.

~~(S//SI//NF)~~ Specifically, NSA provided documentation of [redacted] new taskings during the reporting period. This represents a 33.8% increase in new taskings from the previous reporting period. [redacted]

~~(S//SI//NF)~~ NSA tasked an average of [redacted] telephony facilities during the first eleven months of 2016. From December 2016 through May 2017, NSA has tasked an average of [redacted] telephony facilities. This represents [redacted] increase in the average monthly telephony facilities when compared to the first eleven months of 2016.

~~(S//SI//NF)~~ NSA tasked an average of [redacted] electronic communications accounts during the first eleven months of 2016. From December 2016 through May 2017, NSA tasked an average of [redacted] electronic communication accounts ([redacted] increase from the January through November 2016 monthly average).

(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.[32] Figure 6 contains the classified number of serialized reports and reports identified as containing United States person information over the last ten reporting periods. The NSD and ODNI review revealed that the United States person information was at least initially masked in the vast majority of circumstances.[33] The number of serialized reports NSA has identified as containing United States person information increased after slightly decreasing for the prior two reporting periods.

[32] (U) Previous joint assessments referred to those 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.

[33] (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 meets the applicable standards in NSA's minimization procedures.

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

(U) Figure 6 is classified SECRET//NOFORN.

~~(S//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 13.7% increase from the [redacted] serialized reports NSA identified in the prior reporting period. NSA attributes this increase, in part, to its expanded use of Section 702 [redacted] which have produced reportable foreign intelligence information. Figure 6 reflects NSA reporting over the last ten reporting periods; this is the first and only decrease for these ten reporting periods.

~~(S//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.[34] The percentage of reports containing United States person information was slightly higher this reporting period (8.5%) than the 8.4% reported in the previous reporting period and similar to the 8.5% and 9.0% reported in the two prior reporting periods.

[34] (U) 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 United States person was derived. Accordingly, the references to United States person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.

(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.[35] 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.[36]

(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 the NSA targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion[37] were rejected on the basis that they were ineligible for Section 702 collection.

(U) Between 2011 and December 2013, the yearly average of designated facilities approved by FBI steadily increased. The yearly average of designated facilities approved by FBI in 2014 slightly decreased, and then increased again in 2015 and in the first eleven months of 2016. Between December 2016 and May 2017, 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 2017 and will incorporate this information into future Joint Assessments.

35 [redacted]

36 [redacted]

37 [redacted]

[redacted]

(U) Figure 7 is classified SECRET//NOFORN.

~~(S//SI//NF)~~ Specifically, FBI reports that NSA designated [redacted] accounts [redacted] during the reporting period – an average of [redacted] designated accounts per month. This is a [redacted]

~~(S//NF)~~ FBI approved [redacted] requests [redacted]

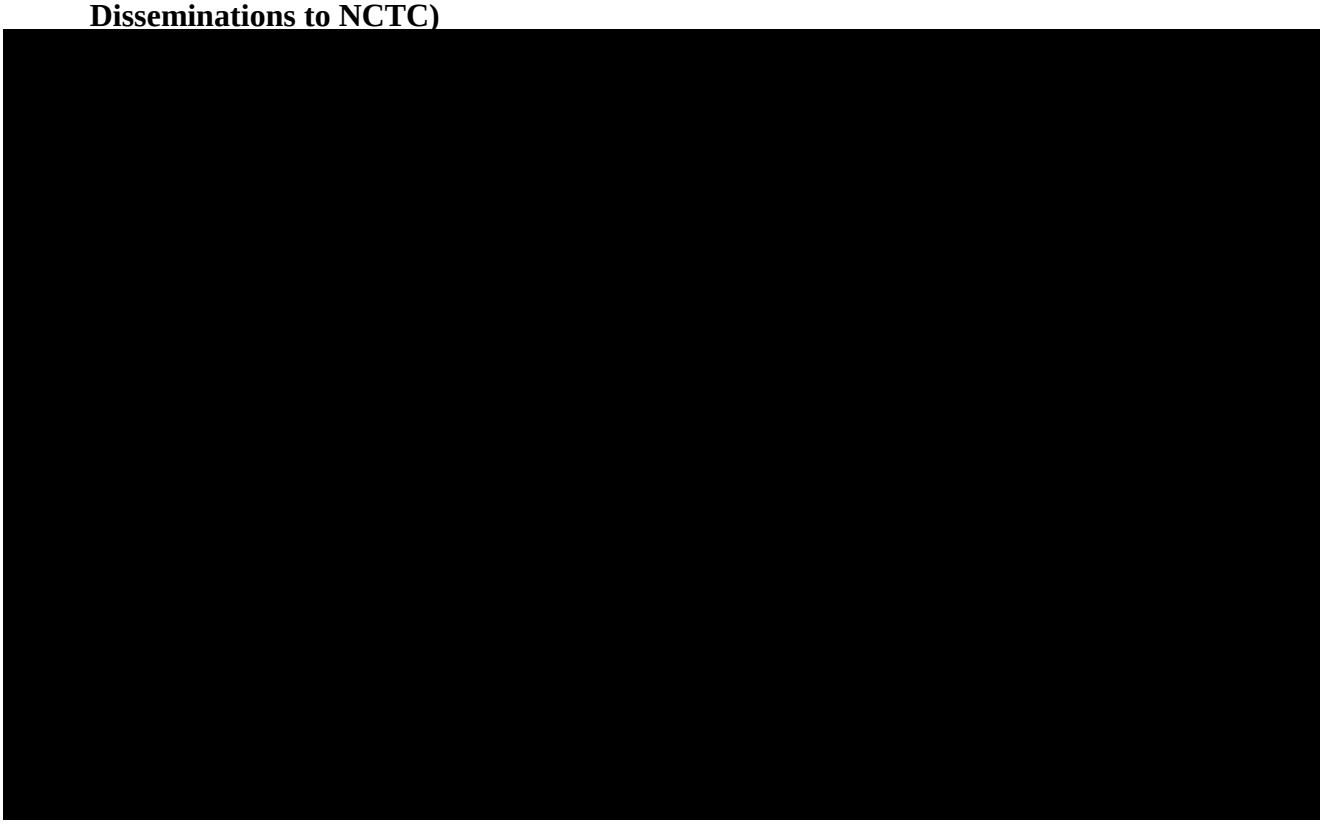
(U) As indicated in prior Joint Assessments, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its

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(l)(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 ten reporting periods (June 2012 – November 2012 through the current period of December 2016 – May 2017). In the first four reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the fifth reporting period, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the sixth and seventh reporting periods, the number of CIA-identified disseminations containing United States person information again decreased. In the eighth and ninth reporting periods, the number of CIA-identified disseminations containing United States person information increased. In this reporting period, the number of CIA-identified disseminations containing United States person information decreased.

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



(U) Figure 8 is classified SECRET//NOFORN.

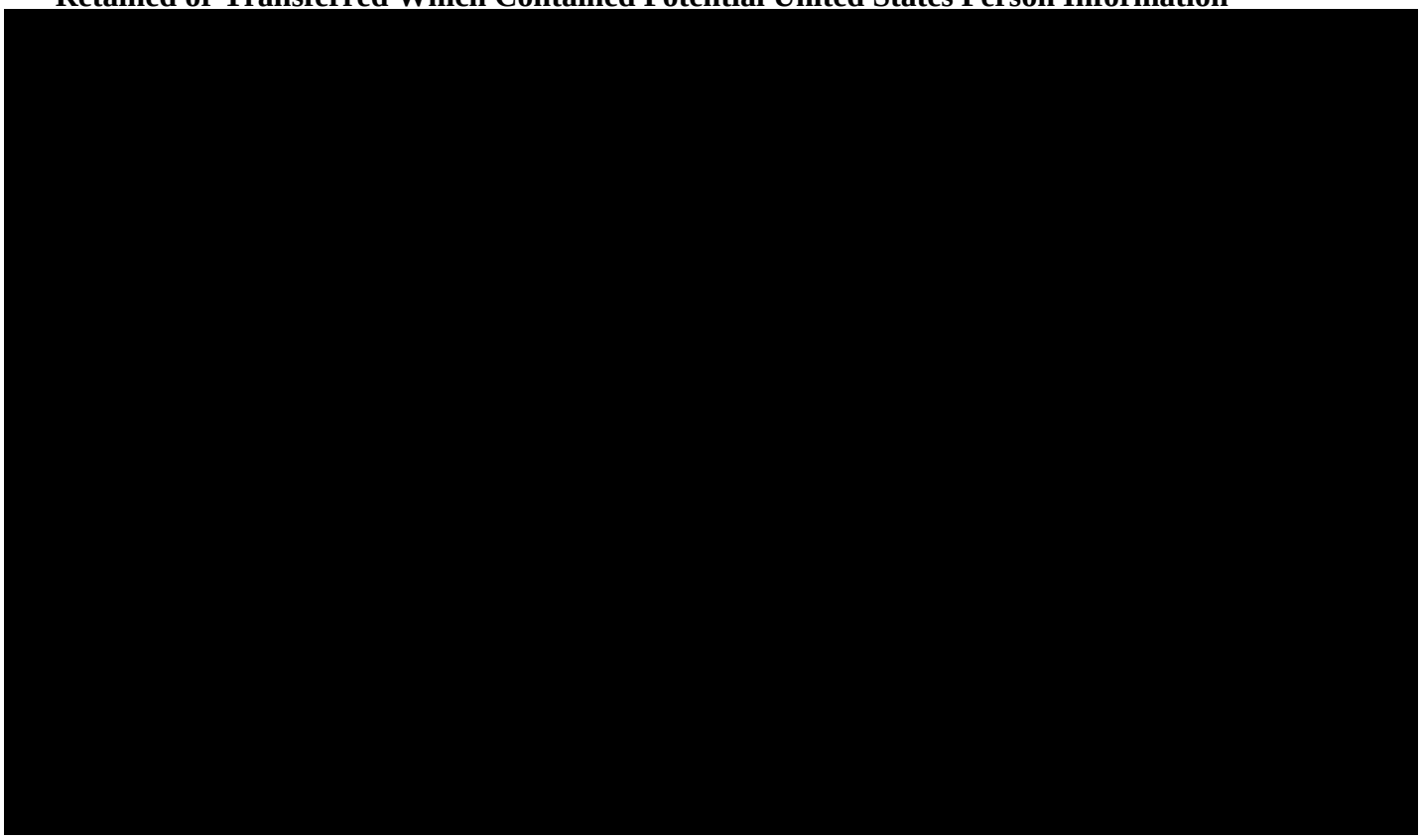
~~(S//NF)~~ During this reporting period, CIA identified disseminations of Section 702-acquired data containing minimized United States person information. This is a decrease from the such disseminations CIA made in the prior reporting period. and as reported in prior Joint Assessments, CIA also permits some personnel with NSD and ODNI, however, review all 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. The CIA minimization procedures must be applied to those files before they are retained or transferred to systems with broader access.[38] Classified Figure 9 details the total number of files that were either retained or transferred, as well as the number of those

[38] In making those 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.[39] Beginning in the middle of the reporting period covered by the 13th 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 December 2016 through May 2017. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.[40] 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.

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



(U) Figure 9 is classified SECRET// NOFORN.

[39] (U) As reported in the 11th 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.

[40]

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

(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes. 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 for this period, 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 is 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.[41] During this reporting period, there were [redacted] identified incidents of noncompliance with CIA's minimization procedures. There were no identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

(U) Figure 10 puts those compliance incidents in the context of the average number of facilities subject to acquisition on any given day[42] during the reporting period:

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

	[redacted]
Compliance incidents during reporting period (December 1, 2016 – May 31, 2017)	
Number of facilities on average subject to acquisition during the reporting period	
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.37%

(U) Figure 10 is classified TOP SECRET//SI//NOFORN.

(U) The compliance incident rate continues to remain below one percent, with the current rate of 0.37% representing a decrease from the 0.88% compliance incident rate in the prior reporting period.[43] The number of notification delays decreased during this reporting period, but remained higher than the number reported for several periods prior to the June 1, 2016 through November 30, 2016 reporting period. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is 0.33%. This information is explained below and detailed in Figure 11.

(U) While the incident rate remains well below one percent, 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

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

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

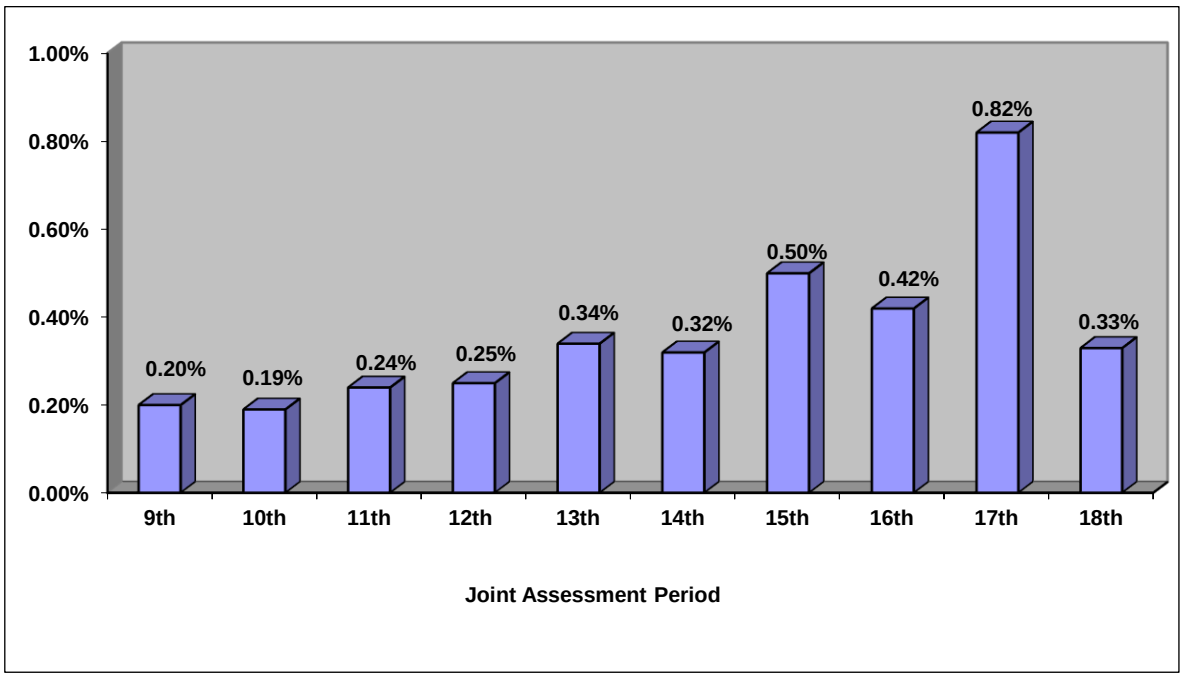
[redacted]

[43] (U) As explained in the previous joint assessment, the prior 0.88% compliance incident rate was largely attributed to an increase in two types of incidents. If those two types of incidents had not been included in that reporting period, the previous compliance incident rate would have been 0.40% (as opposed to 0.88%).

delays (described further below) may occur with frequency, but have limited significance with respect to United States person information.[44]

(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 notification delays. Figure 11 shows that 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) Figure 11 is UNCLASSIFIED.

(U) As Figure 11 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.33%, which is lower than what was reported in the prior reporting period (0.82%), and still below 1%. While the underlying causes of the compliance incident rate are discussed later in this assessment, as the DNI explained on June 7, 2017, during an open hearing in front of the Senate Select Committee on Intelligence, ODNI and DOJ's reviews have revealed an extremely low incident rate. The DNI explained that, while mistakes have occurred, "any system with zero compliance incidents is a broken compliance system because humans make mistakes." The DNI emphasized that when the government finds compliance incidents, those incidents are reported and corrected.

[44] (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 the consistently low compliance incident rate of less than 1% is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures.

(U) B. Categories of Compliance Incidents

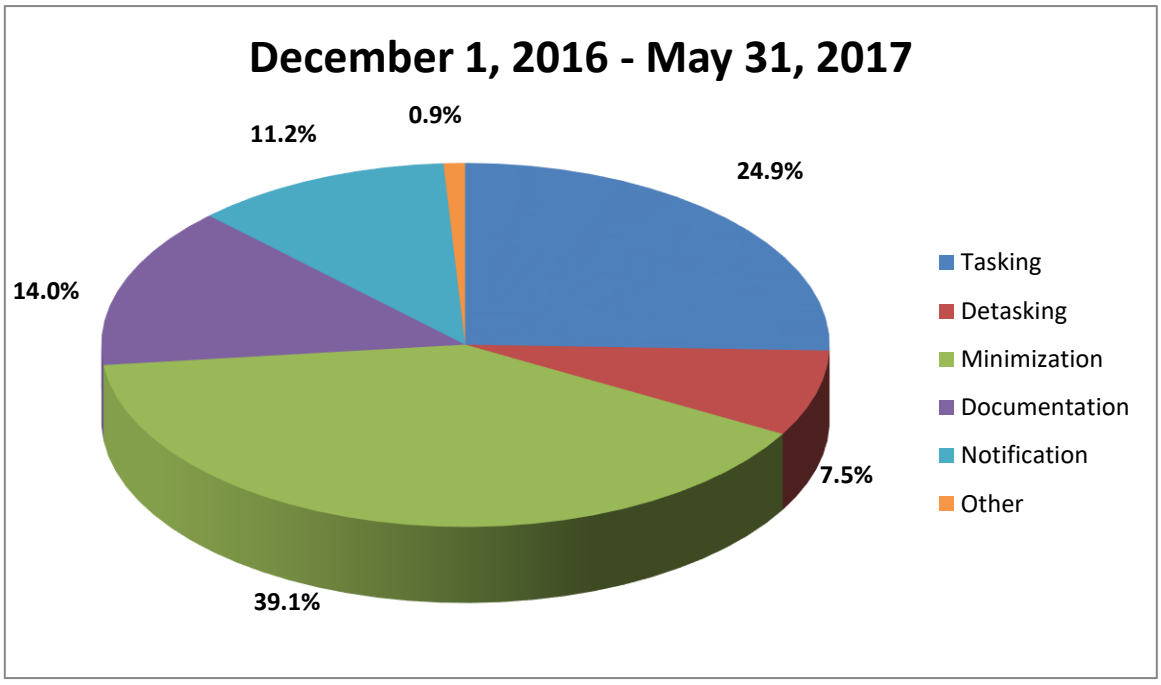
(U) Most of the compliance incidents occurring during the reporting period involved non-compliance with the NSA's targeting or minimization procedures. This largely reflects the centrality of NSA's targeting and minimization efforts in the Government's implementation of the Section 702 authority. The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

- (U) *Tasking Issues.* This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.
- (U) *Detasking Issues.* This category involves incidents in which the facility was properly tasked in accordance with the targeting procedures, but errors in the detasking of the facility caused noncompliance with the targeting procedures.
- (U) *Overcollection*. This category involves incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection."
- (U) *Notification Delays*. This 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.
- (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.

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



(U) Figure 12A is UNCLASSIFIED

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

[redacted]

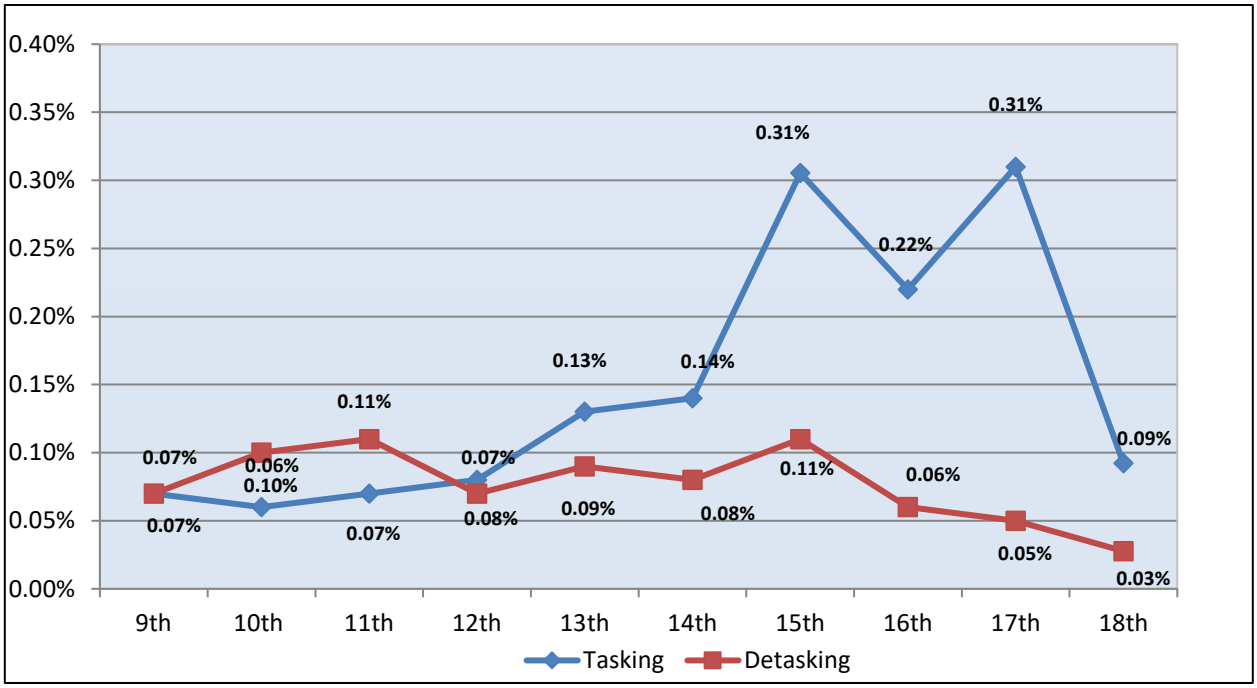
(U) Figure 12B is classified SECRET//NOFORN

(U) As Figures 12A and 12B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, remains low. 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 decreased from [redacted] detasking incidents decreased [redacted] minimization incidents decreased from [redacted] documentation incidents slightly increased [redacted] and "other" category incidents decreased from [redacted] The number of notification delays decreased [redacted] There were zero overcollection incidents in this period, which is less than the single overcollection incident reported for the prior period.

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

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



(U) Figure 13 is UNCLASSIFIED.

(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.[45] The tasking compliance incident rate involving facilities used by United States persons was less than 0.01%, which was substantially lower than the overall tasking incident compliance rate. 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.[46] The percentage of compliance incidents involving such detasking incidents has remained consistently low.[47] The detasking compliance incident rate involving facilities used by United States persons was also less than 0.01%.

(U) With respect to FBI's targeting and minimization procedures, the total number of identified targeting and minimization errors also remained low, as consistent with past reporting periods.[48] Classified Figure 14 shows the classified number of incidents for the last several reporting periods. 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.

[45] (U) As discussed in detail in the 15th Joint Assessment, the significant increase in tasking errors during that reporting period was substantially caused by one particular NSA targeting office's misunderstanding of the requirements of the targeting procedures. As a result, that particular targeting office was required to retake the formal NSA Section 702 online training. *See* the 15th Joint Assessment, pp. 35 – 36. As detailed in the 17th Joint Assessment, the increase in tasking errors was not caused by a single targeting office's misunderstanding of the rules, but a number of the tasking errors consisted of a common fact pattern.

[46] [redacted]

[47] (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 the different incident rates are statistically significant and note that the incident rate is consistently quite low.

[48] [redacted]

Figure 14: ~~(S//NF)~~ Number of Compliance Incidents Involving the FBI Targeting and Minimization Procedures

(U) Figure 14 is classified SECRET//NOFORN.

~~(S//NF)~~ There were [redacted] incidents during this reporting period that involved CIA's minimization procedures; [redacted] incidents were also reported in 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 zero incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents a decrease from the [redacted] 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 those 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 those incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-compliance with the NSA's minimization procedures involving the unintentional improper dissemination, retention, or querying of Section 702 information.

(U) The NSA compliance incident rate for this reporting period, excluding FBI and CIA compliance incidents, is 0.36%[49] and represents a substantial decrease from the compliance incident rate of the previous reporting period. In the subsections that follow,[50] this Joint Assessment examines some of the underlying causes of incidents of non-compliance focusing on incidents that have the greatest potential to impact United States persons' privacy interests, albeit that those incidents represent a minority of the overall incidents. Different types of communication issues, technical and system errors, and human errors are detailed and discussed below. The joint oversight team believes that analyzing the trends of these incidents, especially in regards to their causes, help the agencies focus resources, avoid future incidents, and improve overall compliance.

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

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

(U) Some incidents, however, did involve United States persons during the recent reporting period. As noted above, both the tasking compliance incident rate and detasking compliance incident rate involving facilities used by United States persons was less than 0.01% during this reporting period. For tasking and detasking incidents, United States persons were primarily impacted by (1) tasking errors that led to the tasking of facilities used by United States persons, and (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person. United States persons were also impacted by minimization errors during this reporting period, which are detailed below. While the number of incidents involving United States persons remains low, due to their importance, these incidents are highlighted in this subsection. The Section 707 Report provides further details regarding each individual incident and how any

[49] (U) The overall compliance incident rate for this reporting period is 0.37%.

[50] (U) Although ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may change with each joint assessment, depending on the incidents that occurred during that reporting period and the respective underlying causes.

erroneously acquired, disseminated, or queried United States person information was handled through various purge, recall, and deletion processes.

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

(U) Only 3% of the total number of tasking errors identified during this reporting period involved instances where facilities used by United States persons were tasked pursuant to Section 702.[51] These incidents represent isolated instances of insufficient due diligence and did not involve an intentional effort to target a United States person.

(U) All of the tasking errors in this reporting period impacting United States persons involved the tasking of facilities where the Government knew or should have known that at least one user of the facility was a United States person.[52] The majority of these tasking errors involved targeting analysts not considering the totality of circumstances known to the Government prior to targeting pursuant to Section 702.[53] One tasking error was of a somewhat different nature. In that incident, an NSA analyst tasked a facility pursuant to Section 702 based on an erroneous analysis of data acquired from the intended target's Section 702-tasked facility.[54]

[51] (U) Note that this is 3% of *all* tasking incidents. As described above, the overall tasking compliance incident rate involving United States persons was less than 0.01%.

[52] [redacted]

[53] [redacted]

[54] [redacted]

(U) (2) Delays in Detasking Impacting United States Persons

(U) The majority of the detasking incidents involved non-United States persons who either traveled to the United States, appeared to have traveled to the United States, or involved a non-resolvable unexplained indication of an account appearing to be accessed from within the United States. Only 17% of the total number of detasking delays involved facilities used by a United States person.[55] As discussed in further detail below, the detasking delay incidents impacting United States persons in this reporting period were caused by human errors: miscommunication, misunderstandings of the detasking requirements, and analysts' faulty analysis of information that erroneously led them to continue to assess that the target was a non-United States person located outside the United States.

~~(TS//SI//NF)~~ Of the detasking delays involving facilities used by United States persons,[56] ncidents involved a misunderstanding of the detasking requirements.

~~(TS//SI//NF/FISA)~~ Other incidents were the result of faulty analysis that led to delays in detasking facilities used by United States persons.[59]

[55] (U) Note that this is 17% of *all* detasking incidents. As described above, the overall detasking compliance incident rate involving United States persons was less than 0.01%.

[56]

[57]

[58]

[59]

[60]

[redacted]

~~(TS//SI//NF)~~ One delayed detasking incident that impacted a United States person was the result of intra-agency and inter-agency miscommunication. [redacted]

(U) B. Effect of Human Error

(U) (1) Errors That Can Be Addressed Through Training

(U) Unlike in the immediately prior section, which focused exclusively on incidents impacting United States persons, this section addresses incidents that impacted both United States persons and non-United States persons. As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established 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 11% of the tasking errors made in this reporting period, which is an increase from the previous reporting period, in which

typographical errors accounted for 6% of the tasking errors.[61] Approximately 27% of the detasking delays 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[62] or, as explained above in the examples of detasking delays, were the result of misunderstanding the rules and inadvertent miscommunication, all of which can be and are addressed through remedial training efforts. As with other compliance incidents, any data acquired as a result of such tasking and detasking errors is required to be purged.

(U) Other types of errors can also be addressed and alleviated through training – in particular certain types of tasking errors. Specifically, during this reporting period, a number of incidents involved the failure to conduct necessary foreignness checks prior to the tasking of a facility. Approximately 40% of the tasking errors in this reporting period involved instances in which NSA did not take sufficient pre-tasking steps to try to find information regarding the location of the targeted user or otherwise did not properly establish a sufficient basis to assess that the targeted user was outside the United States. The two most common examples include situations in which the analyst did not conduct a necessary pre-tasking check or there was too long of a delay between the necessary pre-tasking checks and the actual tasking of the account.[63] In all of these incidents, NSA advised that there is no indication that these facilities were used by a United States person or by someone in the United States. After discussing these incidents with NSA compliance personnel, NSA advised that they have met in person with target offices to reiterate *NSA's 702 Targeting Review Guidance* regarding foreignness checks.[64] NSA also held training in 2016 for Section 702 adjudicators who review proposed taskings, and during that training, NSA reminded them of the need to conduct the relevant foreignness checks prior to tasking and to ensure that the checks are done within 7 days of approving a tasking. NSA has also posted guidance on this issue on several NSA internal webpages to reach as wide an audience as possible. The joint oversight team assesses that these types of tasking errors are easily preventable and recommends that NSA continue to reinforce this issue with analysts and adjudicators as part of regular training.

(U) Of all the tasking errors, approximately 9% of those incidents were caused by the incorrect processing of tasking requests. Specifically, errors arose where an analyst requested administrative updates to the tasking record, and the request inappropriately triggered retasking the facility without NSA appropriately applying its targeting procedures.[65] In order to address these types of incidents, NSA updates its adjudication guidance as needed, including in February 2017 to

[61] [redacted]

[62] [redacted]

[63] [redacted]

[64] (U) *See* NSA's documents posted, in redacted form, on ODNI's *IC on the Record* on August 23, 2017, in response to the ACLU FOIA: *NSA's 702 Targeting Review Guidance* (Document 10), *NSA's 702 Practical Applications Training* (Document 11), *NSA's 702 Training for NSA Adjudicators* (Document 12), and *NSA's 702 Adjudication Checklist* (Document 13).

[65] [redacted]

all adjudicators to address administrative updates and how to prevent this type of incident from occurring. Specifically, NSA reminded all adjudicators to check the tasking history for each facility to verify that the facility is currently tasked to Section 702 prior to making changes to the tasking, such as reassigning the facility to a different analyst.

~~(S//NF)~~ Approximately 14% of the total number of NSA compliance incidents was the result of documentation errors.[66] The NSA targeting procedures require that NSA's documentation concerning each tasked facility contain a citation to the source of information upon which the determination that the user of that facility was reasonably believed to be located outside the United States was made (the "foreignness determination") and identify the foreign power or foreign territory about which NSA expects to obtain foreign intelligence information pursuant to the tasking. The targeting procedures also require NSA to 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 that foreign power or foreign territory. In addition, NSA must document which certification under which the facility is tasked. In all of these incidents, while the actual tasking of each facility was appropriate, the analyst failed to sufficiently document this information on the tasking sheet.

(U) Additionally, during the reporting period, the joint oversight team noted a number of compliance incidents resulting from instances in which NSA neglected to provide the required notice to NSD and ODNI within the specified timeframe required by the targeting procedures. Reporting delays accounted for 11% of all incidents during the reporting period.[67] NSA advised that the number of compliance incidents resulting from reporting delays was due to reorganization and personnel changes within NSA. NSA's OCO has implemented additional safeguards to ensure that all new analysts are appropriately trained in the Incident Reporting Tool (IRT) and that IRT checks were conducted regularly to ensure that notices were reviewed in a timely manner. NSA also increased its incident reporting staff, began cross-training personnel in different authorities, and revised its standard operating procedures to streamline incident reporting. Reducing the number of reporting delays is a priority for NSD and ODNI, and the joint oversight team continues to discuss additional steps NSA can take to reduce these notification delays.

(U) (2) Minimization Errors That Can Be Addressed Through Training and Technical Improvements

(U) During this reporting period, NSA's minimization procedures included three types of restrictions on querying raw Section 702 collection.

66 [redacted]

67 [redacted]

1) NSA's Section 702 minimization procedures require that queries of raw Section 702 collection *must be designed in a manner "reasonably likely to return foreign intelligence information."* For example, if a query is determined to be overly broad under this standard (*e.g.*, typographical or comparable error in the construction of the query term),[68] it constituted a compliance incident, regardless of whether the query term used a non-United States person identifier or a United States person identifier.

2) Although NSA's Section 702 minimization procedures permit queries of raw Section 702 collection using United States person identifiers, such queries *must be approved in accordance with NSA's internal procedures*. If an NSA analyst used a United States person identifier that had not been approved pursuant to NSA's internal procedures to query Section 702-acquired data, it constituted a compliance incident.

3) NSA's Section 702 minimization procedures in effect during the majority of this reporting period *prohibited using United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques*. If an NSA analyst used a United States person identifier to query Internet communications acquired through NSA's upstream collection techniques, it constituted a compliance incident.

(U) As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization procedures. During this reporting period, out of all of NSA's total minimization errors, approximately 92.4% involved improper queries,[69] of which:

- approximately 68.9% involved United States person queries (i.e., queries that involved using a United States person identifier without approval as required by NSA's internal procedures or using a United States person identifier to query NSA's upstream collection)[70] and

- approximately 23.5% involved overly broad queries.[71]

As with previous reporting periods, there were no incidents of an NSA analyst intentionally running improper queries.

[68] (U) 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.

[69] (U) In the previous reporting period, approximately 99% of NSA's minimization procedures errors involved improper queries.

[70] [redacted]

[71] [redacted]

(U) As a result of its review of NSA's compliance with the procedures approved by the Court in the 2002 Raw Take Order, NSA's Office of the Inspector General (OIG) discovered a number of potentially improper queries conducted by NSA personnel between June 1, 2016, and August 31, 2016, using United States person identifiers in upstream collection.[72] Because NSA's OIG discovered these potentially improper queries during the current reporting period, they are discussed in this joint assessment; however, the queries were conducted outside the current reporting period. After the OIG notified NSA's Office of Compliance for Operations (OCO) of these queries, which were outside the scope of the OIG review, OCO conducted further analysis and found additional improper queries. At this time, the NSA OIG has completed the investigative portion of the Raw Take Order review and issued its report. NSD is in the process of reviewing this report to determine the scope of the improper queries, which ones had previously been reported by NSA, and the associated root cause(s).

(U) In another incident, a discrete category of information collected pursuant to NSA's Section 702 upstream collection techniques was inadvertently not labeled as upstream collection.[73] As a result, it is likely that, even if analysts took the appropriate actions to limit queries to Section 702 downstream collection, queries including United States person identifiers would have run against this limited set of mislabeled communications acquired through NSA's upstream collection techniques. NSA corrected the labeling error in May 2016, but failed to report it to NSA compliance personnel at that time. NSA subsequently reported it to NSD, and it was reported to the FISC.

(U) Additionally, during this reporting period, there was a series of other incidents that involved NSA improperly querying Section 702-acquired data using United States person identifiers in two NSA systems that are used to determine the location of the user of the facilities queried.[74] NSA uses those systems, for example, as part of the due diligence requirement to ensure that Section 702 targets are non-United States persons located outside the United States. These systems search information acquired pursuant to multiple FISA and non-FISA authorities, including NSA's Section 702 collection (which at the time the queries took place included upstream collection). Consequently, queries using known United States person identifiers should not have been conducted in those particular systems.[75] Subsequently, the improper queries and results were deleted, and no

72 [redacted]

73 [redacted]

74 [redacted]

75 [redacted]

results were included in disseminated reports. NSA advised that the relevant personnel have been reminded to exercise care when performing queries of United States person identifiers and using these two systems. Additionally, as is the case with all identified compliance incidents, those incidents were reported to the FISC, and to Congress in the Section 707 report.

(U) Prior to the above-described incidents, NSA issued a compliance advisory that advised NSA personnel, as part of the due diligence requirement, to check the location of the users of any identifiers proposed for queries. However, the NSA guidance did not differentiate between United States person identifiers and non-United States person identifiers. In early 2017, NSA issued an updated compliance advisory instructing personnel not to use the two particular systems to conduct queries using known United States person identifiers.[76] As a result of the initial compliance advisory discussed above, the government assesses it is likely that at least one of those two systems, which pre-dates the second one, was regularly used to conduct queries using United States person identifiers. Despite NSA's efforts to ensure all analysts were aware of the updated 2017 compliance advisory, it remains possible for an analyst to inadvertently query United States person identifiers in those particular systems.

(U) C. Inter-Agency and Intra-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. However, the joint oversight team assesses that there remains room for continued improvement: approximately 13% of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.[77] Those detasking delays typically

[redacted]

76 [redacted]

77 [redacted]

involved travel or possible travel of non-United States persons to the United States. Only one incident is attributable to a communication issue that resulted in a tasking error and that incident did not involve a United States person.[78]

(U) D. Incidents Resulting from Technical Issues

(U) A number of compliance incidents resulted from technical issues 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. Accordingly, 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. As a result of those 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 determined that the historically limited number of overcollection incidents was the result of the efforts of all of the involved agencies. Although technical issues can potentially have larger implications, that potential was largely avoided during this reporting period.

(U) Specifically, the technical issues that resulted in delayed detaskings were caused by system errors and a system processing problem.[79] In all of the instances involving system errors or system processing problems, the technology and systems failed to function as designed, and, thus, the systems failed, resulting in delayed detasking incidents whereby NSA was unable to timely detask facilities. NSA subsequently corrected those technical issues.

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

(U) During this reporting period, there were [redacted] incidents involving noncompliance with the CIA minimization procedures. Those incidents involved inadvertent instances of CIA not completely removing Section 702-acquired information that was supposed to be deleted and failing to properly track certain United States person queries so that those queries could subsequently be reviewed by the joint oversight team.

~~(S//NF)~~ Specifically, there were [redacted] involving noncompliance with the CIA minimization procedures. In [redacted], CIA discovered that it inadvertently deleted a portion of a CIA system used [redacted] and minimization of FISA-acquired information. To address the system outage and [redacted] CIA directed users to [redacted]

78 [redacted]

79 [redacted]

[redacted] CIA subsequently corrected these errors. In [redacted], CIA's investigation into the incident described above [redacted] CIA corrected this error and [redacted] As a result of this error, because United States person queries [redacted] any United States person queries conducted in the [redacted] were not available for review by NSD and ODNI. [redacted] involved the inadvertent failure to age off a portion of unminimized data acquired pursuant to Section 702 in the [redacted] CIA has since identified and resolved the [redacted] that led to these compliance incidents and continues to review its FISA [redacted] to ensure [redacted] for age-off and purge requirements.

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

~~(S//NF)~~ During this reporting period, there were no incidents involving non-compliance with FBI's targeting procedures. However, there were [redacted] incidents involving noncompliance with the FBI minimization procedures.[80]

~~(S//NF)~~ Some of FBI's minimization incidents involved improper queries using United States person identifiers, such that the queries were not designed to extract foreign intelligence information or evidence of a crime and thus did not comply with the query standard in the relevant minimization procedures. For example, some of those query incidents involved FBI personnel who conducted queries of FBI personnel names (i.e., for work-related purposes, such as for case load management), but those queries were not designed to extract foreign intelligence information or evidence of a crime. In each of those query incidents, the agents or analysts were reminded of the query restrictions in the FBI minimization procedures.

[redacted]

[80] [redacted]

[redacted]

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

(U) During this reporting period, there were no instances 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 assessed that the historically low number of compliance incidents caused by service providers

81 [redacted]

82

reflected, in part, the service providers' commitment to comply with the law while protecting their customers' interests. However, the low number of those incidents also reflected the continued efforts by the Government and service providers to ensure that lawful intercept systems were effective and compliant with all applicable laws 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 this reporting period, the joint oversight team found that the agencies 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. As in previous reporting periods, the joint oversight team found no 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 the underlying causes of the incidents that did occur. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection activities and continued personnel training. Additionally, as part of its on-going oversight responsibilities, the joint oversight team and the agencies' internal oversight regimes will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.

APPENDIX A

APPENDIX A

(U) IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

(U) I. Overview - NSA

(U) The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).[1] As required by Section 702, those targets must be non-United States persons[2] reasonably believed to be located outside the United States.

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

[redacted]

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

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

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

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

[3] [redacted]

[4] [redacted]

(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to 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) After information is collected from those tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.[6]

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

5 [redacted]

6 [redacted]

(U) A. Pre-Tasking Location

(U) 1. Telephone Numbers

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

(U) 2. Electronic Communications Identifiers

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

[7] [redacted]

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

[9] [redacted]

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

[redacted]

(U) C. Post-Tasking Checks

[redacted]

~~(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] Should traffic not be viewed in at least once every 30 business days, a notice is sent to the tasking team and their management, who then have the responsibility to follow up.

[10] [redacted]

[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]

(U) D. Documentation

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

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

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

Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

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

(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 OCO 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 OCO. For guidance, analysts consult standard operating procedures, supervisors, OCO personnel, and NSA OGC attorneys.

(U) The NSA targeting and minimization procedures also 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. NSA's OCO reviews all Section 702 taskings and conducts spots checks of disseminations based in whole or in part on Section 702-acquired information. The Directorate of Operations Information and Intelligence Analysis organization 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. Compliance officers work with NSA analysts and CIA and FBI points of contact, as necessary, to compile incident reports that are forwarded to both the NSA OGC and OIG. NSA OGC forwards the incidents to NSD and ODNI.

(U) On a more programmatic level, under the guidance and direction of the Compliance Group, NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protections during NSA missions. The Compliance Group complements and reinforces the intelligence oversight program of the 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. The Authorities Integration Group coordinates 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. The Compliance Group has 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. [redacted]

[redacted]

12 [redacted]

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

~~(S//NF)~~ The FISA Program Office was established in December 2010 [redacted] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, 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.

[redacted]

(U) **III. Overview NCTC**

~~(S//NF)~~ NCTC does not target or acquire communications pursuant to Section 702. In addition, NCTC does not currently have a process in place to identify or nominate foreign intelligence targets to NSA. However, like CIA and FBI, NCTC may request to be [redacted] on unminimized data (pertaining to counterterrorism) from Section 702 facilities already tasked by NSA. NCTC applies its Section 702 minimization procedures to Section 702 [redacted] data.

~~(S//NF)~~ NCTC, in consultation with NSD, developed an electronic and data storage system, known as [redacted], to retain and process raw FBI-collected FISA-acquired information in accordance with NCTC's Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act. In consultation with NSD, ODNI, NSA, and FBI, NCTC modified [redacted] to (i) provide additional compliance capabilities in support of [redacted] FISA Section 702-acquired counterterrorism data and (ii) monitor compliance with NCTC's Minimization Procedures for Section 702-acquired counterterrorism data (Section 702 minimization procedures). In addition to documenting compliance with the Section 702 minimization procedures requirements, [redacted] also documents the requests for [redacted] of Section 702-acquired information. This documentation includes the [redacted]

~~(S//NF)~~ [redacted] communications from Section 702 tasked facilities are stored within [redacted] where only properly trained and authorized analysts are able to query them. [redacted]

~~(S//NF)~~ NCTC personnel may disseminate Section 702-acquired information of or concerning an unconsenting United States person if that information meets the standard for dissemination pursuant to Section D of NCTC's Section 702 Minimization Procedures.

~~(S//NF)~~ [redacted]. NCTC's Compliance and Transparency Group (hereafter NCTC Compliance) [redacted] conducts periodic reviews of Section 702 [redacted] as well as NCTC Section 702 disseminations in order to verify compliance with NCTC's Section 702 Minimization Procedures and identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.

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

[redacted]

(U) B. Oversight and Compliance

(U) NCTC's FISA compliance program is managed by NCTC Compliance in coordination with NCTC Legal. NCTC provides training to all NCTC personnel who may access raw FISA-acquired information. Access to unminimized Section 702-acquired communications is limited to trained personnel. NCTC compliance personnel and attorneys also respond to inquiries regarding minimization questions. Identified incidents of noncompliance with the NCTC Section 702 Minimization Procedures are reported to NSD and ODNI generally by NCTC Compliance or NCTC Legal personnel.

~~(S//NF)~~ NCTC Compliance was established in the fall of 2014 and is charged with providing strategic direction for the management and oversight of NCTC's access to and use of [redacted] This includes management and oversight of NCTC's FISA 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, FBI, and CIA. In addition, the office leads the day-to-day FISA compliance efforts within NCTC. NCTC Compliance is responsible for providing strategic direction and internal oversight for data handling and management of FISA/Section 702 data, as well as administering and implementing NCTC FISA/Section 702 training, ensuring that all NCTC Section 702 collection is properly [redacted] minimized and disseminated, and that NCTC is complying with all minimization procedures requirements.

(U) IV. Overview - FBI

(U) A. FBI's Role in Targeting – Nomination for Acquiring [redacted] Communications

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition of [redacted] 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 [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 and [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]

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

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

(U) C. Documentation

~~(S//NF)~~ The targeting procedures require that FBI retain the information [redacted] in accordance with its records retention policies [redacted] FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [redacted] extending through [redacted] and culminating in approval or disapproval of the acquisition. In addition, the FBI

standard operating procedures call for [redacted] depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications [redacted] regarding its review of the [redacted] information. Additional checklists have been created to capture information on requests withdrawn [redacted], or not approved by FBI.

(U) D. Implementation, Oversight, and Compliance

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI OGC, particularly the National Security and Cyber Law Branch (NSCLB), as well as FBI's Exploitation Threat Section (XTS), [redacted] and FBI's Inspection Division (INSD). [redacted] XTS has the lead responsibility in FBI for [redacted] requests [redacted]. XTS personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests for [redacted]. XTS also has the lead responsibility for facilitating FBI's nominations to NSA [redacted] communications. XTS, NSCLB, 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) V. Overview - Minimization

(U) After 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, CIA and NCTC. 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) Section 702 minimization procedures do, however, impose additional obligations or restrictions as compared with the 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, NCTC, and FBI have created systems to track the purging of information from their systems. CIA, NCTC, 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.