(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

(U) Reporting Period: June 1, 2019 – November 30, 2019

September 2021

[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

September 2021

(U) TABLE OF CONTENTS

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

(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 September 2021, twenty-three 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. § 1881a(m)(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. This Assessment covers the period from June 1, 2019 through December 31, 2019.

- *(U) Who receives it?* Each Joint Assessment is submitted to the following oversight entities: Foreign Intelligence Surveillance Court (FISC), relevant congressional committees, and the Privacy and Civil Liberties Oversight Board (PCLOB).

- *(U) What is being assessed?* The Attorney General and the DNI jointly assess the Government's compliance with Attorney General Guidelines and with FISC-approved "targeting," "minimization," and "querying" procedures.

- *(U) What are targeting, minimization, and querying 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. Querying procedures set rules for using United States person and non-United States person identifiers to query Section 702-acquired information.

- *(U) What compliance and oversight efforts underlie the Joint Assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, judicial, 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) oversees 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

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

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

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 the Government to provide the FISC, the congressional oversight committees, and the PCLOB 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. 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 improper disseminations of information acquired pursuant to Section 702, and querying procedures, such as non-compliant queries of Section 702-acquired information using United States person identifiers. When appropriate, 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(i) directive, the Joint Assessment includes a review of any compliance incidents by such service providers.

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

(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

September 2021

(U) Reporting Period: June 1, 2019 through November 30, 2019

(U) EXECUTIVE SUMMARY

(U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 *et seq*., as amended, requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702 (hereinafter, "Section 702"), 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, minimization, and querying 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 twenty-third joint compliance assessment of the Section 702 program. This assessment covers the period from June 1, 2019, through November 30, 2019 (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 March 5, 2020; 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.

(U) However, notwithstanding a focused and concerted effort by the Federal Bureau of Investigation (FBI) personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying procedures caused a large number of query errors. In particular misunderstandings at one field office, involving FBI's conduct of "batch queries," led to a significant number of compliance incidents during this reporting period.

(U) During this reporting period, the overall compliance incident rate – calculated as the total number of compliance incidents reported during the relevant reporting period, expressed as a percentage of the average number of facilities subject to acquisition on any given day during the

reporting period – was 20.28%, which represents a significant increase from the prior period (6.91%). As described above, the vast majority of compliance incidents related to a single type of query error, involving FBI's conduct of "batch queries." These incidents, as well as FBI's subsequent remedial measures, are discussed in greater detail later in this assessment. As explained in past assessments and detailed later in this current assessment, the overall compliance incident rate is an imperfect metric, in part because a certain number of the compliance incidents included in the numerator do not bear a meaningful relation to the targeting activities in the denominator. For example, as detailed below, the number of FBI query errors is not related to the average number of facilities subject to acquisition. The imperfections in the metric are particularly evident in this reporting period because the number of compliance incidents in the numerator that do not bear a relation to the denominator (in particular, the FBI query errors) so heavily outweighs the number of compliance incidents that do bear a relation to the denominator (*e.g.*, NSA targeting errors).

(U) This assessment also includes the targeting assessment compliance incident rate for the National Security Agency (NSA) (see Figure 15 below), which represents the number of NSA targeting compliance incidents, expressed as a percentage of the average number of facilities tasked to acquisition, in each case, during the reporting period. During this reporting period, the targeting assessment compliance incident rate for NSA was 0.14%.

(U) This joint assessment, like the 21st and 22nd Joint Assessments, also presents an additional metric that is designed to reflect FBI's rate of compliance with its procedures when conducting queries of unminimized Section 702-acquired information, audited by NSD, given that such errors comprised a substantial number of compliance incidents during this reporting period. NSD and ODNI will determine whether to include this additional metric in future assessments, depending on the types of incidents that were reported in the applicable period. This new metric, which is a query error rate for FBI (see Figure 19 below), represents the total number of FBI query compliance incidents reported to the FISC during the reporting period, expressed as a percentage of the total number of FBI queries audited by NSD in connection with the field office reviews during which NSD identified such FBI query compliance incidents.[1] During this reporting period, the query error rate for FBI was 36.59%.

(U) SECTION 1: INTRODUCTION

(U) FISA Section 702(m)(1)[2] requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to Section 702 and to submit such assessments to the FISC and relevant congressional committees at least once every six months. To fulfill this requirement, a team of oversight personnel from NSD and ODNI (hereinafter, the "joint oversight team") has conducted compliance reviews to assess whether the authorities under Section 702 have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI's 23rd joint compliance assessment under

[1] ~~(S//NF)~~ The number of queries audited and included in this total are queries contained in query logs provided to NSD by FBI that were run in FBI [redacted] NSD has, in prior query audits, found that a small percentage of queries that were included in particular query logs were not run against unminimized FISA-acquired information, to include unminimized Section 702-acquired information.

[2] (U) 50 U.S.C. §1881a(m)(1).

Section 702, covering the period June 1, 2019 through November 30, 2019 (hereinafter, the "reporting period").[3]

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting, minimization, and querying 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:

> (U) 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.

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

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(h) 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. The foreign intelligence information must fall within a specific type (*i.e.*, category) of foreign intelligence information that has been authorized pursuant to the Section 702(h) certifications.[4] Four agencies are primarily involved in

[3] (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702, which was previously submitted on March 5, 2020, as required by Section 707(b)(1) of FISA (hereinafter, the "Section 707 Report"). This 23rd Joint Assessment covers the same reporting period as the 23rd Section 707 Report.

[4] [redacted]

implementing Section 702: NSA, FBI, the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC). An overview of how these agencies implement the authority appears in the Appendix 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. The Appendix, also contained in previous joint assessments, details how each agency implements Section 702 and includes a general description of the oversight at each agency.

(U) As noted above, FBI had a significant number of compliance incidents related to querying of Section 702-acquired information. FBI amended its 2018 querying procedures, which were effective during a portion of this reporting period, in response to concerns raised by the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISC-R) regarding the sufficiency of those procedures. FBI's query-related compliance incidents are detailed below, along with the remedial measures FBI has taken and is taking to address them.

(U) The joint oversight team finds that the agencies have continued to implement their respective 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. However, notwithstanding a focused and concerted effort by FBI personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying procedures caused a large number of query errors. The joint oversight team anticipates that the remedial measures undertaken by FBI should result in significant improvements to FBI's compliance with its querying procedures.

(U) 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

[redacted]

discussed herein and in the Section 707 Report. Each joint assessment provides, as appropriate, 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 the Appendix, NSA and FBI each acquire certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, CIA, and NCTC[5] each handles Section 702-acquired data in accordance with its own minimization procedures.[6] 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 existing agency-specific systems to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

(U) A joint oversight team 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 Mission Integration Directorate Mission Performance, Analysis, and Collection (MPAC) Division. The team members play complementary roles in the review process. The following section 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[7] (also referred to as selectors) once collection begins. NSA

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

[6] (U) Each agency's Section 702 targeting, minimization, and querying procedures are approved by the Attorney General and reviewed by the FISC. The targeting, minimization, and querying procedures that were in effect during this assessment's reporting period were those approved as part of the 2018 certifications in October 2018. In October 2018, the FISC found that CIA, NCTC and NSA's querying procedures were sufficient but that the FBI's querying procedures were not sufficient in certain respects. After the FISC's decision in October 2018 and FISC-R decision in July 2019, the Government amended FBI's querying procedures and submitted those to the FISC in August 2019. The FISC approved the amended FBI querying procedures in September 2019.

(U) On October 8, 2019, the DNI released, in redacted form, each of the 2018 minimization procedures and the 2018 querying procedures for NSA, FBI, CIA, and NCTC, as well the 2018 targeting procedures for NSA and FBI. These 2018 procedures are posted on ODNI's *IC on the Record* website.

[7] (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities (*i.e.*, selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described in this joint assessment, applies to the tasking of every communication facility, regardless of the type of facility. A fuller description of the Section 702 targeting process may

must also minimize its collection in accordance with its minimization procedures and must conduct queries in accordance with its querying procedures. Each of these responsibilities is detailed in the Appendix. 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 the Appendix.

(U) NSD and ODNI's joint oversight of NSA's implementation of Section 702 consists of periodic compliance reviews, which the NSA targeting procedures require,[8] as well as the investigation and reporting of specific compliance incidents. During this reporting period, onsite reviews were conducted at NSA on the dates shown in Figure 1.

(U) Figure 1: NSA Reviews

UNCLASSIFIED

Date of NSA Onsite Review	Targeting, Minimization, and Querying Reviewed
August 23, 2019	June 1, 2019 – July 31, 2019
October 25, 2019	August 1, 2019 – September 30, 2019
December 20, 2019	October 1, 2019 – November 30, 2019

UNCLASSIFIED

(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 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 (*i.e.*, that the target is a non-U.S. person reasonably believed to be located outside the United States, and that the target is reasonably expected to possess, receive, and/or likely communicate foreign intelligence information related to the categories of foreign intelligence information specified in the certifications). For those tasking sheets that, on their face, meet the standards and provide sufficient information, no

be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and is not attempting to make a substantive distinction between the two terms.

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

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 (OCO), 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 querying procedures, which took effect on October 18, 2018, provide that any use of United States person identifiers as terms to identify and select communications must first be approved by NSA's Office of General Counsel (NSA OGC). The procedures 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 United States person identifier, the joint oversight team reviews all approved United States person identifiers to ensure compliance with NSA's minimization procedures.[9] 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 querying 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.[10]

[9] (U) On April 30, 2019, the DNI publicly released ODNI's sixth annual Transparency Report[s]*: Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2018* (hereinafter, the "CY2018 Transparency Report"). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(B)), the 2018 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 2018. The same statistics were reported in the seventh annual transparency report "CY2019 Transparency Report" on April 30, 2020, covering the entire calendar year of 2019. The CY2019 Transparency Report matches part of this assessment's reporting period of January – May 2019.

[10] (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(C)), the CY2018 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 2018. The same statistics were provided in the CY2019 Transparency Report.

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting, minimization, and querying 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.[11] 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 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 FBI

(U) FBI fulfills various roles in the implementation of Section 702, which are set forth in further detail in the Appendix. 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, FBI may receive [redacted][2] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI's Section 702 minimization procedures. As described below, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

---

[11] (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 tasking and detasking complied with its targeting and minimization procedures.

[12] [redacted]

(U) NSD and ODNI's oversight program is designed to ensure FBI's compliance with statutory and procedural requirements for each of those three roles. NSD and ODNI generally conduct monthly reviews at FBI headquarters of FBI's compliance with its targeting procedures and quarterly 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 707(b)(1)(F) of FISA. For this reporting period, onsite reviews were conducted at FBI headquarters on the dates shown in Figure 2.

(U) Figure 2: FBI Reviews

UNCLASSIFIED

Date of FBI Onsite Review	Targeting and Minimization Reviewed
August 20 and 21, 2019	June 2019 targeting decisions
September 18 and 19, 2019	July 2019 targeting decisions; June 1, 2019 – August 31, 2019 minimization decisions
October 29 and 30, 2019	August 2019 targeting decisions
November 13 and 14, 2019	September 2019 targeting decisions
December 17 and 18, 2019	October 2019 targeting decisions; September 1, 2019 – November 30, 2019 minimization decisions
January 15 and 16, 2020	November 2019 targeting decisions

UNCLASSIFIED

(U) Figure 2 is UNCLASSIFIED.

(U) In conducting the targeting review, the joint oversight team reviews the targeting checklists completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.[13] 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 National Security and Cyber Law Branch (NSCLB) are available to answer questions and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

(U) In conducting the FBI headquarters minimization reviews, 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.

[13] ~~(S//NF)~~ If FBI's application of its targeting procedures to [redacted] returns information from the databases discussed in FBI's targeting procedures, then FBI provides a checklist that shows the results of its database queries. If FBI's database queries returned results that FBI identifies as relevant to the target's location or citizenship status, then FBI also provides the joint oversight team with supporting documentation. [redacted] During this reporting period, the joint oversight team reviewed all checklists and supporting documentation provided by FBI for approved requests for which information is returned by FBI's database queries.

(U) In addition to conducting minimization reviews at FBI headquarters during this reporting period, NSD continued to conduct minimization and query reviews at FBI field offices in order to review the retention, querying, and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data.[14] During those field office reviews, NSD reviewed a sample of retention decisions made by FBI personnel in their investigations that acquired Section 702 data and a sample of disseminations containing information acquired pursuant to 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 unminimized FISA-acquired information, including Section 702-acquired information. Those reviews evaluate whether the queries complied with the requirements in FBI's FISA minimization and querying procedures, including its Section 702 querying procedures. In addition, as a result of a Court-ordered reporting requirement in the FISC's *November 6, 2015 Memorandum Opinion and Order*[15] for queries conducted after December 4, 2015, as well as the requirements of the FISA statute, 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 and query reviews at 14 FBI field offices during this reporting period and reviewed cases involving Section 702-tasked facilities.[16] 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 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. While outside this reporting period, the most recent annual process review occurred in June 2020.

~~(S//NF)~~ As further described in detail in the Appendix, FBI nominates potential Section 702 targets to NSA. [redacted]

[14] (U) As noted above, FBI's Querying Procedures were approved, in part, in October 2018. During this current reporting period, FBI's queries were assessed for compliance with FBI's querying procedures, as approved.

[15] (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*. This Court-ordered reporting requirement was carried forward in subsequent Section 702 FISC opinions.

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

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

[redacted] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in the Appendix.

(U) The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting, minimization, and querying procedures, the Attorney General's Acquisition Guidelines, or other agencies' procedures in which FBI is involved.[17] 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.

(U) III. Joint Oversight of CIA

(U) As further described in detail in the Appendix, 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. 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 and querying procedures.[18] 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. For this reporting period, onsite reviews at CIA were conducted on the dates shown in Figure 3.

(U) Figure 3: CIA Reviews

UNCLASSIFIED

Date of CIA Onsite Review	Minimization and Querying Reviewed
September 25, 2019	June 1, 2019 – July 31, 2019
November 20, 2019	August 1, 2019 – September 30, 2019
January 15, 2020	October 1, 2019 – November 30, 2019

UNCLASSIFIED

(U) Figure 3 is UNCLASSIFIED.

(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

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

[18] (U) The query requirements for CIA that were in effect during this reporting period are contained in CIA's Section 702 Query Procedures for the 2018 Certifications, which were posted on *IC on the Record* on October 8, 2019.

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 querying procedure requirements that such queries are reasonably likely to return foreign intelligence information, as defined by FISA.

~~(S//NF)~~ CIA may receive [redacted] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. Additionally, and as further described in detail in the Appendix, 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 has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in the Appendix.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA's minimization and querying procedures, the Attorney General Acquisition Guidelines, or other agencies' procedures in which CIA is involved.[19] 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) IV. Joint Oversight of NCTC

(U) NCTC is authorized to receive unminimized Section 702 data and also has 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 onsite reviews of NCTC's access, receipt, and processing of minimized Section 702 information received from FBI. NSD conducted a review of minimized Section 702 information received from FBI for this reporting period in July and August 2020.

~~(S//NF)~~ NCTC is authorized to receive unminimized Section 702 information pertaining to counterterrorism. NCTC's processing, retention, and dissemination of such information is subject to its Section 702 minimization procedures. Unlike NSA, FBI, and CIA, NCTC does not directly

[19] (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 non-compliance with the NSA targeting procedures can also involve CIA.

engage in targeting or acquisition, nor does it nominate potential Section 702 targets to NSA. 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 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.

(U) The onsite reviews focus on NCTC's application of its Section 702 minimization and querying procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews at NCTC were conducted on the dates shown in Figure 4.

(U) Figure 4: NCTC Reviews

UNCLASSIFIED

Date of NCTC Onsite Review	Minimization and Querying Reviewed
July 16, 2019	May 1, 2019 – June 30, 2019
September 20, 2019	July 1, 2019 – August 31, 2019
November 15, 2019	September 1, 2019 – October 31, 2019

UNCLASSIFIED

(U) Figure 4 is UNCLASSIFIED.

(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 and querying procedures or other agencies' procedures in which NCTC is involved.[20] Investigations are coordinated through the NCTC Compliance and Transparency Group and NCTC Legal, a forward deployment component of the ODNI OGC, and when necessary, may involve requests for further 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.

[20] (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.

(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 information, and comply with all legal requirements. For those reasons, NSD and ODNI generally lead calls and meetings on relevant compliance topics, including calls or meetings with representatives from all agencies implementing Section 702 authorities, so as to address interagency issues affecting compliance with the statute and applicable procedures. Additionally, during this reporting period, NSD and ODNI conducted weekly telephone calls with NSA to address certain 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 provide a demonstration to the joint oversight team of new or substantially revised systems involved in Section 702 targeting, minimization, or querying 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. During this reporting period, NSA continued to administer the compliance training course dated November 2016.[21] 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[22] where personnel can obtain information about specific types of Section 702-related issues and compliance matters.

[21] (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).

[22] (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).

(U) During this reporting period, FBI 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 also conducted in-person trainings at multiple FBI field offices. For example, during this 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 and the requirements of FBI's querying procedures.[23] 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) As part of its efforts to address certain issues causing the large number of non-compliant queries, in June 2018, and in November 2019, FBI worked with NSD and ODNI to develop updated guidance on the query provisions in FBI's procedures. This enhanced training on the query restrictions in FBI's procedures was designed to address misunderstandings regarding the query standard and how to avoid non-compliant queries. More recently, FBI developed training focused on the query provisions in its Section 702 querying procedures, including system changes designed to address aspects of the 2018 amended querying procedures. This training was mandatory for FBI personnel who are authorized to access unminimized Section 702-acquired information. FBI conducted this training between November and December 2019. Users who did not complete this training by mid-December 2019 had their access to unminimized Section 702-acquired information temporarily suspended until they took the training.

(U) During this reporting period, CIA provided targeted FISA training to attorneys it embeds with CIA operational personnel who regularly address FISA matters, and continued to provide FISA training to any attorney beginning an assignment that may involve the provision of legal advice on FISA matters. Additionally, CIA has a required training program for anyone handling unminimized 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.[24]

(U) NCTC provided training on the NCTC Section 702 minimization and querying procedures to all of its personnel who will have access to unminimized Section 702-acquired

[23] (U) This specific training began before, occurred during, and continued after the current reporting period of June 1, 2018, through November 30, 2018.

[24] (U) *See USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data.* As discussed in previous Joint Assessments, 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."

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 unminimized Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed unminimized Section 702-acquired information in its system to confirm that those personnel who access unminimized Section 702-acquired information had received training on the NCTC Section 702 minimization and querying 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 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,[25] 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.[26]

[25] (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 in its *CY2019 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*.

[26] (U) The reporting periods in which the total number of facilities under collection decreased occurred prior to date ranges depicted in Figure 5.

(U) Figure 5: Average Number of Facilities under Collection

[redacted]

(U) Figure 5 is classified ~~SECRET~~ [redacted]

~~(TS//SI//NF)~~ NSA reports that, on average, approximately [redacted] facilities[27] were under collection pursuant to the applicable certifications on any given day during the reporting period.[28] This represents a 16.5% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period; this increase is consistent with the general trend seen in prior reporting periods.

[redacted]

[27] ~~(TS//SI//NF)~~ Beginning in the Joint Assessment covering the reporting period of December 2017 through May 2018, the Government changed its methodology to count the tasking of [redacted] to ensure consistency with how it counts other tasked facilities. Depending on the number [redacted] in a given reporting period, counting [redacted] could potentially skew the numbers and percentages in such a way that the statistics provided would no longer function as a barometer for the overall health of the Section 702 program.

[28] ~~(S//NF)~~ The applicable certifications for this reporting period were [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.[29] Classified Figure 6 charts the average monthly numbers of newly tasked facilities from 2014 through 2018 and the total monthly numbers of newly tasked facilities from June 2019 through November 2019.

(U) Figure 6: New Taskings by Month (Yearly Average for 2014 through 2018)

(U) Figure 6 is classified ~~SECRET~~ [redacted]

~~(S//SI//NF)~~ NSA provided documentation of approximately [redacted] new taskings during the reporting period. As shown in Figure 6, the increase in the number of newly tasked facilities continued and was largely driven by increases in the number of tasked telephony facilities. From December 2018 through May 2019, NSA tasked an average of approximately [redacted] telephony facilities per month. From June 2019 through November 2019, NSA tasked an average of approximately [redacted] telephony facilities per month – an increase of approximately [redacted] taskings per month. In comparison, over the same time period, electronic communications accounts only increased by an average of approximately [redacted] taskings per month.

(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

[29] (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 were then retasked.

NSD and ODNI access to all reports NSA identified as containing United States person information.[30] Figure 7 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 reviews revealed that the United States person information was at least initially masked in the vast majority of circumstances.[31] The number of serialized reports NSA has identified as containing United States person information increased, after decreasing for the prior two reporting periods.

[30] (U) Previous joint assessments referred to those reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. Given that Section 702 of FISA replaced the PAA in 2008, the Government no longer disseminates minimized information that was previously acquired pursuant to PAA. However, Figure 7 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.

[31] (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.

(U) Figure 7: Total Disseminated NSA Serialized Reports Based Upon Section 702-Acquired Data and Number of Such Reports NSA Identified as Containing USP Information

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

~~(S//NF)~~ For this reporting period NSA identified to NSD and ODNI approximately [redacted] serialized reports based upon minimized Section 702-acquired data. The number of serialized reports identified as containing United States person information increased from [redacted] in the prior reporting period, to the current [redacted][32]

[32] (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.

~~(S//NF)~~ Outside of this reporting period, NSA identified that a technical error caused it to not identify for NSD and ODNI approximately [redacted] serialized reports as containing United States person information. The [redacted] serialized reports are included in the [redacted] figure.

(U) II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities (hereinafter, "Designated Accounts") 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 such Designated Accounts.[33] As detailed below, the number of Designated Accounts has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.[34]

(U) As classified Figure 8 details, FBI approves the vast majority of Designated Accounts and this percentage has been consistently high. The high level of approval can be attributed to the fact that the Designated Accounts have already been evaluated and found to meet the NSA targeting procedures. FBI may not approve NSA's request for acquisition of a Designated Account for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the Designated Accounts 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[35] were rejected on the basis that they were ineligible for Section 702 collection.

(U) The yearly average of Designated Accounts approved by FBI increased yearly from 2014 through 2018. The number of Designated Accounts approved by FBI each month in this reporting period has varied. NSD and ODNI have continued to track the number of Designated Accounts approved by FBI and will incorporate this information into future Joint Assessments.

33 [redacted]

34 [redacted]

35 [redacted]

~~(S//NF)~~ **Figure 8:** [redacted]

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

~~(S//SI//NF)~~ FBI reports that NSA designated approximately [redacted] accounts [redacted] during the reporting period – an average of approximately [redacted] Designated Accounts per month.[36] FBI approved approximately [redacted][37] requests [redacted] These numbers reflect continued increases in the number of accounts designated by NSA and approved by FBI.

[36] [redacted]

(U) [37] ~~(S//NF)~~ As previously noted, beginning with the Joint Assessment covering the reporting period December 2017 through May 2018, the Government changed its counting methodology to ensure statistical accuracy for the number of Designated Accounts approved.

(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 9 compiles the number of such disseminations of reports containing United States person information identified in the reporting periods from December 2014 through May 2015 through the current period of June 2019 through November 2019. While the number of CIA-identified disseminations containing United States person information has fluctuated over the years, those fluctuations have generally been incremental whether upward or downward. The current reporting period's number of CIA-identified disseminations containing United States person information continued that trend, slightly increasing from the last reporting period.

(U) Figure 9: Disseminations Identified by CIA as Containing Minimized Section 702-Acquired United States Person Information (Excluding Certain Disseminations to NCTC)

[redacted]

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

~~(S//NF)~~ During this reporting period, CIA identified approximately [redacted] disseminations of Section 702-acquired data containing minimized United States person information. [redacted] and as reported in prior Joint Assessments, CIA also permits some personnel [redacted]

[redacted]

(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 10 details the total number of files that were either retained or transferred, as well as the number of those retained or transferred files that contain identified United States person information. This current assessment reports the total number of files CIA transferred from June 2019 through November 2019. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.[39] 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.

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

[39] ~~(S//NF)~~ For this reporting period, CIA analysts transferred a total of approximately [redacted] (2.6%) of which were identified by CIA as containing a communication with potential United States person information.

(U) Figure 10: Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred which Contained Potential United States Person Information

(U) Figure 10 is classified ~~SECRET// NOFORN.~~

(U) IV. Trends in NCTC Minimization

(U) Beginning with the reporting period covering June 2017 through November 2017, the Joint Assessment now includes statistics regarding the total number of disseminations identified by NCTC as containing Section 702-acquired information. This number is classified and reported in Figure 11. Starting in the previous reporting period, NCTC identified and provided to NSD and ODNI only disseminations containing minimized United States person information. Because NCTC only began obtaining unminimized Section 702-aquired data after the FISC approval of such in April 2017, there are only five six-month periods to report in this assessment.[40] This current joint

[40] ~~(S//NF)~~ The FISC's April 2017 opinion approved NCTC's 2016 Minimization Procedures allowing NCTC to obtain unminimized Section 702-acquired information. NCTC began receiving unminimized Section 702-acquired information on May [redacted]

assessment reports that the number of disseminations containing minimized United States person information, while low, increased from the previous reporting period.[41]

(U) Figure 11: Disseminations Identified by NCTC as Containing Minimized Section 702-Acquired Information[42]

Figure 11 is classified ~~SECRET//NOFORN.~~

~~(S//NF)~~ During this reporting period, NCTC identified and provided to NSD and ODNI approximately [redacted] disseminations of Section 702-acquired data containing minimized United States person information. This was a 17.6% increase in disseminations containing minimized United States person information when compared to the previous reporting period.

(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement their 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 Section 702 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.

[41] ~~(S//NF)~~ NCTC identified and provided to NSD and ODNI approximately [redacted] disseminations containing minimized United States person Section-702 acquired information.

(U) [42] ~~(S//NF)~~ As noted in previous joint assessments, prior to December 2018, NCTC provided all disseminations to NSD and ODNI for review. Starting with the January 31, 2019 review, which included December 2018 disseminations, NCTC began identifying for NSD and ODNI only disseminations containing United States person information.

(U) However, notwithstanding a focused and concerted effort by FBI personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying requirements caused a large number of query errors. The number of FBI compliance incidents increased substantially compared to the previous reporting period, and this assessment reports a large number of FBI compliance incidents related to querying, and, in particular, FBI's use of "batch queries.[43] The vast majority of these compliance incidents related to a single large query event. As discussed below, non-compliant batch queries were conducted by a limited number of personnel, and some were conducted using a batch query function in an FBI system.[44]

(U) FBI amended its 2018 querying procedures in response to concerns raised by the FISC and the FISC-R regarding the sufficiency of those procedures. The FISC ultimately determined that the FBI's amended querying procedures were adequate, and the joint oversight team has engaged with the FBI to implement those amended procedures and to provide the FISC with periodic reporting regarding that implementation, including with respect to systemic changes and additional training of FBI personnel.[45] These incidents and remedial measures are detailed below and will be updated in future assessments, as appropriate. The joint oversight team anticipates that the remedial measures undertaken by FBI should result in significant compliance improvements.

(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. For example, an "NSA compliance incident" could be caused by typographical errors contained in another agency's nomination to NSA for tasking.

(U) Each of the compliance incidents for this current reporting period is described in detail in the corresponding Section 707 Report. This joint assessment does not reiterate the compliance

[43] ~~(S//NF)~~ The number of FBI minimization or querying errors for the current reporting period was [redacted] compared to the [redacted] minimization errors in the previous reporting period.

[44] ~~(S//NF)~~ The FBI system in which the non-compliant batch queries were conducted was FBI [redacted]

[45] (U) On October 8, 2019, the ODNI posted, on *IC on the Record*, documents related to the 2018 certifications, including the FISC's October 2018 opinion, the FISC-R's July 2019 opinion, the FISC's September 2019 opinion, and FBI amended querying procedures, dated August 2019. Specifically, in its October 2018 opinion, the FISC found that certain parts of FBI's procedures concerning the querying of United States persons were not sufficient. The Government appealed this decision to FISC-R, which affirmed the FISC's decision in part. The Government subsequently submitted amended the FBI's querying procedures to address the issues raised by the FISC and the FISC-R, and the FISC found that the amended procedures were sufficient.

(U) Subsequently, while outside this reporting period, the FISC revisited FBI's non-compliant queries in its December 2019 opinion authorizing the 2019 Section 702 certifications, and its November 2020 opinion authorizing the 2020 Section 702 certifications; these opinions and other documents related to the 2019 and 2020 Section 702 certifications were released on September 4, 2020, and April 26, 2021, respectively, on *IC on the Record*. As it pertained to FBI's querying procedures, the FISC's opinion regarding the 2019 Section 702 certifications found that the FBI was following its schedule for implementing the training and system modifications necessary to comply with its querying procedures. The FISC's opinion regarding the 2020 Section 702 certifications found that FBI's querying procedures were sufficient, but the Court expressed continued concern about FBI's practices involving United States person query terms.

incidents set forth in the Section 707 Report. It does, however, examine those incidents to assess broader implications and to determine whether the agency's corrective measures address those implications.

(U) Specifically, even a small number of incidents can have the potential of carrying broader implications, and a small number of actions can result in numerous incidents also having broad implications, as is the case for the FBI "batch" querying incidents. Thus, the Joint Assessment provides NSD and ODNI's analysis of 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, minimization, or querying procedures and [redacted] compliance incidents involving noncompliance with FBI's targeting, minimization, and querying procedures.[46] In addition, during this reporting period, there were [redacted] incidents of noncompliance with CIA's minimization procedures. There were [redacted] incidents of noncompliance with NCTC's minimization and querying procedures. There was one identified instance of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(i) of FISA.

(U) Figure 12 puts those compliance incidents in the context of the average number of facilities subject to acquisition on any given day[47] during the reporting period.

[46] (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 non-compliant.

[47] [redacted]

(U) Figure 12: Overall Compliance Incident Rate

~~SECRET~~ [redacted]

(U) All compliance incidents during reporting period (June 1, 2019 – November 30, 2019)	[redacted]
(U) Number of facilities on average subject to acquisition during the reporting period	
(U) Overall compliance incident rate: number of incidents divided by average number of facilities subject to acquisition	(U) 20.28%

~~SECRET~~ [redacted]

(U) Figure 12 is classified ~~SECRET~~ [redacted]

(U) The 20.28% overall compliance incident rate represents an increase from the 6.91% overall compliance incident rate in the prior reporting period. As with the previous incident rate, the current reporting period's overall compliance incident rate was predominantly impacted by FBI personnel misunderstanding the query standard in its querying procedures and their use of FBI's batch query tool, where a single improper batch query decision can, and has, resulted in numerous compliance incidents. These incidents – including the remedies – are discussed in detail below. The incident rate was also impacted by a number of non-compliant queries conducted by NSA personnel. As discussed above and detailed below, the manner in which this overall compliance incident rate is calculated results in an imperfect measure of the error rate for the Section 702 program during this reporting period.

(U) As discussed below, notification delays are incidents in which the violation is that the notification requirement contained in the targeting procedures was not satisfied. Substantive compliance incidents are not captured in this metric. If a compliance incident involved both a substantive error (for example, a tasking or detasking error) and the failure to meet the notification requirement, the substantive error was counted separately from the notification delay. For the majority of these notification delays, the only incident of non-compliance was the failure to comply with the notification requirement. Specifically, as part of the oversight team's periodic evaluation of the tools to assess compliance, the joint oversight team, as explained in past Joint Assessments, determined that another valuable measure is to compare the overall compliance incident rate excluding notification delays. If the notification delay incidents are not included in the calculation, the overall compliance incident rate for this reporting period decreases slightly to 20.24%. The comparable incident rates in the two previous reporting periods were 6.9% and 33.52%, respectively. Like the overall compliance rate discussed above in Figure 12, the rate without the notification delay incidents was similarly affected by the FBI querying incidents.

(U) The joint oversight team assesses that, excluding FBI and NSA querying incidents, the compliance incident rate remained low and 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. As it pertains to FBI querying incidents, the joint oversight team has continued to identify a significant number of non-compliant queries in subsequent reporting periods. The joint oversight team continues to work with FBI to reduce these non-compliant queries and improve training and guidance regarding this issue.

(U) As explained in previous assessments, the oversight team periodically evaluates how and what data it collects to provide for more meaningful statistics. For example, the team considers whether there are other means of comparison – whether with the currently tracked actions or by implementing the tracking of certain other data – that could provide a better understanding of overall compliance. The Joint Assessment has traditionally compared the number of compliance incidents (*i.e.*, the "numerator") to targeting activity during the reporting period, which is reflected as the average number of tasked facilities (*i.e.*, the "denominator").

(U) While 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, it remains an imperfect proxy. A flaw with using this particular proxy is that certain types of incidents included in the numerator do not bear a relation to the targeting activity in the denominator. For example, assessing a delayed *detasking* incident (which is an incident resulting from non-compliance with targeting procedures) as contained in the numerator to the average number of *tasked* facilities as contained in the denominator compares closely similar factors – both are directly related to tasking and must meet the requirements of the targeting procedures. However, the factors are not similar when comparing an improper *dissemination* incident or an improper *query* (which are incidents resulting from non-compliance with minimization and querying procedures) to the average number of *tasked* facilities. Minimization and querying incidents implicate the requirements of the minimization and querying procedures, whereas the tasking of a facility implicates the requirements of the targeting procedures. In addition, the number of query and dissemination incidents that can occur in a reporting period are largely independent from the number of facilities tasked during a period, as queries and disseminations can involve facilities that are no longer tasked – or were never tasked – pursuant to Section 702, and multiple queries or disseminations can be made in relation to a single facility. Conceivably, minimization incidents should be compared to the number of total minimization actions, but we are currently unable to count or track minimization actions in that manner. Adding to the dissimilarity is that multiple agencies' (NSA, FBI, CIA, and NCTC) incidents – as well as incidents by service providers – are counted in the overall compliance incident rate, but only two agencies (NSA and FBI) actually conduct targeting activity pursuant to their respective targeting procedures, and only NSA's targeting activities are included in the denominator.

(U) As with prior reporting periods, the number of compliance incidents in the numerator that do not bear a relation to the denominator (in particular, the FBI query errors) heavily outweighs the number of compliance incidents that do bear a relation to the denominator (e.g., NSA targeting errors), making the imperfections in the overall compliance incident rate more evident than in some previous periods. Accordingly, readers should understand that the 20.28% overall compliance incident rate is an imperfect representation of the error rate for the Section 702 program during this reporting period.

(U) As described in prior joint assessments, while assessing that the agencies remain overall compliant, the joint oversight team revisited the value of the overall incident rate proxy and

determined that providing an additional comparison rate would enhance overseers' (the FISC, Congress, and the PCLOB) and the public's understanding of Section 702 compliance. This assessment, accordingly, provides an additional metric (first introduced in the 19th Joint Assessment): the NSA targeting compliance incident rate (see Figures 15 and 16). The joint oversight team has also decided that, because FBI query errors comprised a substantial number of the incidents discovered by NSD during this reporting period, this assessment and, depending on the type of errors that were reported during the applicable period, potentially future assessments will include a query error rate for FBI (see Figure 20), which was first introduced in the 21st Joint Assessment.

(U) Separating the targeting errors from the minimization and query errors allows for another layer of evaluation. We provide these additional metrics (also introduced in the previous assessment) to advance the understanding of the incidents' impact and the causes of those incidents. These metrics are provided after an explanation of the categories of compliance incidents so that the new metrics can better be understood.

(U) Notwithstanding the issues discussed above, the current assessment provides the overall compliance incident rates in Figures 12 above and 13 below so that readers can see the size of the increase from historical periods in order to place the number of FBI query errors discovered during this reporting period in the context of a rate that has been used historically, as these query errors were the driving factor in the rate increase.[48]

(U) B. NSA's Compliance Incidents: Categories and Number of Incidents

(U) As it has been historically, most of the compliance incidents occurring during this reporting period – excluding the FBI querying incidents – involved non-compliance with the NSA's targeting, minimization, or querying procedures. This largely reflects the centrality of NSA's targeting, minimization, and querying efforts in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting, minimization, or querying procedures have generally fallen into the categories below. However, in some instances, an incident may involve more than one category of noncompliance.

(U) Incidents of non-compliance with NSA's Targeting Procedures:

- (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

[48] (U) Note that because of the imperfections described above, and because FBI query errors are only one factor in the overall compliance incident rate, a period-on-period comparison of the rate will still not provide an entirely accurate measure of the increase in FBI query errors.

tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection."

- (U) *Notification Delays*. This category involves incidents in which a notification requirement contained in the targeting procedures was not satisfied.[49]

- (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) Incidents of non-compliance with NSA's Minimization and Querying Procedures:

- (U) *Minimization and Querying Issues.* This category involves incidents relating to NSA's non-compliance with its minimization and querying procedures.

(U) *Other Issues.* This category involves incidents that do not fall into one of the six above categories. In these instances, the joint oversight team will assess each incident to determine if it resulted from non-compliance with NSA's targeting procedures, minimization, and querying procedures and account for those incidents accordingly.

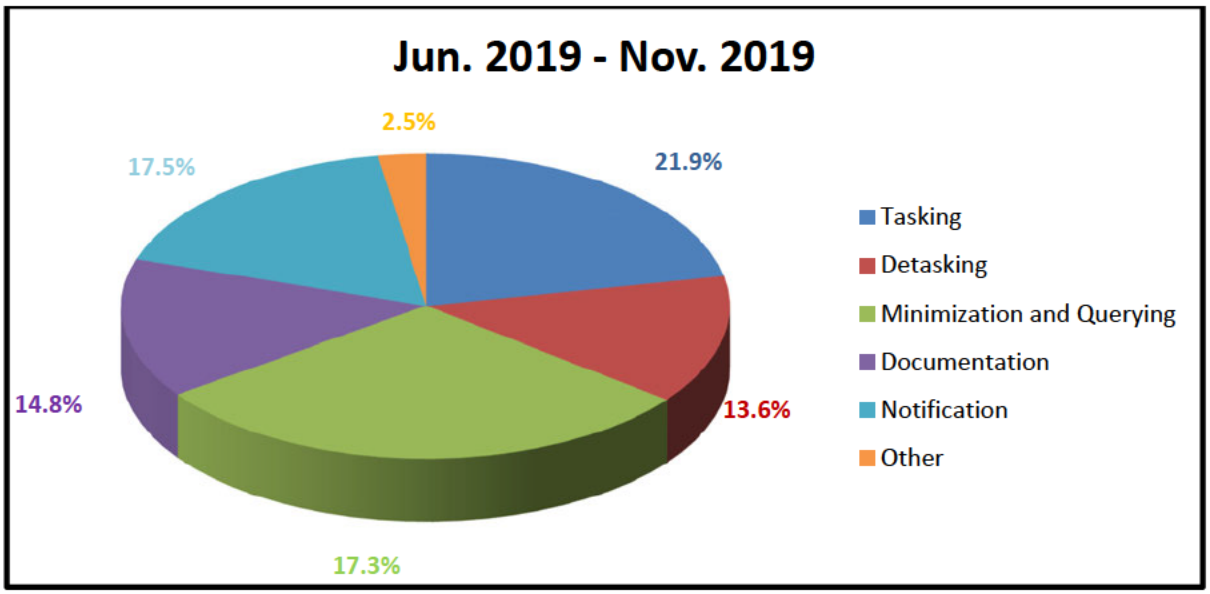
(U) While the above categories specifically pertain to NSA incidents, FBI's targeting incidents categories and all other agencies' minimization and querying incidents categories generally align to those NSA categories. Because only NSA and FBI are permitted to target pursuant to Section 702, only NSA and FBI have targeting procedures (which have been publicly released). All four agencies have minimization and querying procedures (which have been publicly released). Compliance incidents by FBI, CIA, and NCTC are discussed in their respective sections below.

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 13A depicts the percentage of NSA compliance incidents in each category that occurred during this reporting period, whereas Figure 13B provides that actual classified number of NSA incidents.

[49] (U) A compliance incident may involve both a failure to meet the notification requirement and a substantive error (for example, a tasking or detasking error). However, in those instances, the substantive error was counted separate from the notification delay. For the majority of delayed notification incidents, the only incident of non-compliance was the failure to comply with the notification requirement.

(U) Figure 13A: Percentage Breakdown of Compliance Incidents Involving the NSA Targeting, Minimization, and Querying Procedures

UNCLASSIFIED



UNCLASSIFIED

(U) While accurately depicted on the pie chart, the minimization and querying percentage in Figure 13A was mislabeled. It should read 29.7% rather than 17.3%

(U) Figure 13A is UNCLASSIFIED

(U) Figure 13B: Number of Compliance Incidents Involving the NSA Targeting, Minimization, and Querying Procedures

[redacted]

(U) Figure 13B is classified ~~SECRET//NOFORN~~

(U) As Figures 13A and 13B demonstrate, during this reporting period, minimization and querying incidents account for the largest portion of incidents across all categories. Tasking errors and detasking delays account for the second and third largest percentage of incidents, respectively, followed by documentation errors. Tracking the proportion of incidents allows for the joint oversight team to identify trends and to address the non-compliance with appropriate remedies. Being able to do so is important for a variety reasons, especially as it pertains to more substantive tasking and detasking compliance incidents that 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, the joint oversight team also focuses on incidents of noncompliance with minimization procedures 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 increased from [redacted]; minimization and querying incidents decreased from [redacted]; documentation incidents decreased from [redacted]; and "other" category incidents increased from [redacted] The number of notification delays increased from [redacted] There were no overcollection incidents in this period.

(U) As mentioned above, separating the targeting errors from the minimization and querying errors allows for another layer of evaluation as opposed to comparing all of the errors together. By narrowing the focus on errors implicating NSA's targeting procedures, Figure 15 provides the NSA targeting compliance incident rate (a metric introduced in the previous assessment) for this current reporting period. This metric compares similar factors: NSA's number of "targeting incidents" (*i.e.*, the "numerator") to the NSA's targeting activity of the number of average *tasked facilities* (*i.e.*, the "denominator"). The number of NSA's "targeting incidents" includes the following categories of incidents that implicate NSA's targeting procedures: tasking errors, detasking delays, documentation errors, notification delays, overcollection incidents, and other issues. As explained above, incidents that fall under the "other issues" category may be included as well if those constituted errors in following NSA's targeting procedures.

[50] ~~(S//NF)~~ As noted in the previous joint assessment, the number of minimization and querying incidents during the prior reporting period was unusually high as a result of three main factors. First, a system error that inadvertently modified the behavior of certain query terms accounted for approximately 57% of the minimization and querying incidents. Second, [redacted] incidents involving relatively large numbers of improper United States person queries accounted for another 18% of the minimization and querying incidents. Finally, the prior reporting period included an unusually high number of dissemination incidents because one issue – one target office's misapplication of a software tool used to mask United States person identities in disseminations – resulted in [redacted] improper disseminations.

(U) Figure 14: NSA Targeting Compliance Incident Rate

~~SECRET~~ [redacted]

(U) NSA compliance incidents relating to NSA's targeting procedures, during reporting period (June 1, 2019 – November 30, 2019)	[redacted]
(U) Number of facilities on average subject to acquisition during the reporting period	
(U) NSA targeting compliance incident rate: number of targeting incidents divided by average number of facilities tasked to acquisition	(U) 0.14%

~~SECRET~~ [redacted]

(U) Figure 14 is classified ~~SECRET~~ [redacted]

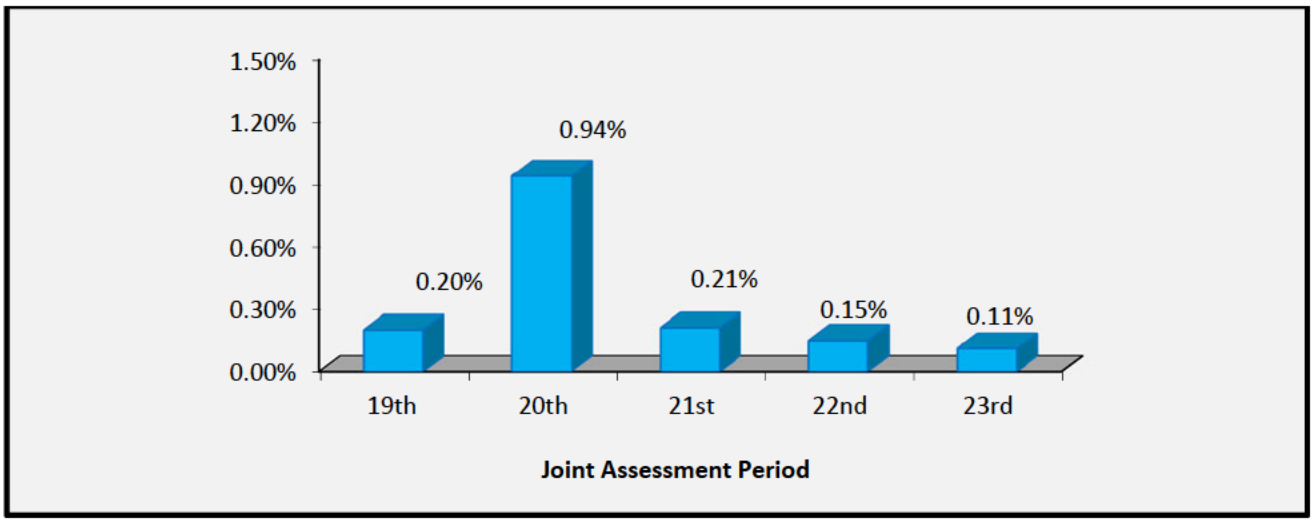
(U) This NSA targeting compliance incident rate percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Also, a single action may result in numerous incidents that have broad implications. Furthermore, other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States persons.

(U) Similar to Figure 12 above and its associated explanation, the joint oversight team determined that excluding NSA's notification delays incidents from the NSA's targeting compliance incident rate provides another measure.[51] Thus, Figure 15 shows that adjusted NSA targeting compliance incident rate of 0.11%, not including notification delay errors (as compared to 0.14% of NSA Targeting Compliance Incident Rate, including notification errors). As described in prior joint assessments, the increase from 0.20% in the 19th reporting period to 0.94% in the 20th reporting period was primarily a result of one NSA office's misunderstanding regarding how a targeting tool functioned, which resulted in an abnormally large number of targeting incidents. As Figure 15 shows, NSA's targeting compliance incident rate (not including notification delays) during this reporting period was at its lowest level since the inclusion of this statistic.

[51] (U) Notification delays are violations of notification requirement contained in the targeting procedures was not satisfied. Substantive compliance incidents are not captured in this metric. If a compliance incident involved both a substantive error (for example, a tasking or detasking error) and the failure to meet the notification requirement, the substantive error was counted separate from the notification delay. For the majority of the notification delays, the only incident of non-compliance was the failure to comply with the notification requirement.

(U) Figure 15: NSA Targeting Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), *not* Including Notification Delays

UNCLASSIFIED



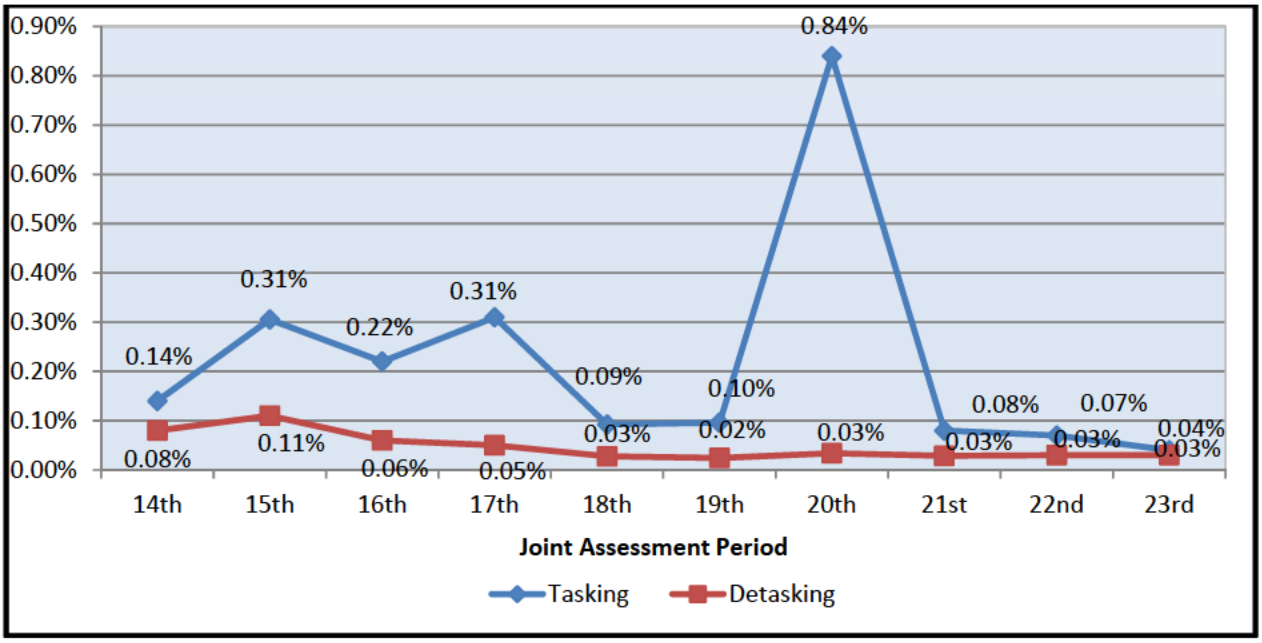
UNCLASSIFIED

(U) Figure 15 is UNCLASSIFIED.

(U) Whereas Figure 15 depicts NSA targeting incidents by combining all targeting incidents, except for notification delays, Figure 16 depicts NSA's compliance incident rates individually for tasking and detasking incidents. Figure 16 separates those types of incidents for more granularity and understanding of the trends for each. As previously calculated and reported, the tasking and detasking incident rate is compared to the average facilities on collection for the given reporting period. 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).

(U) Figure 16: Tasking and Detasking Incident Compliance Rates

UNCLASSIFIED



UNCLASSIFIED

(U) Figure 16 is UNCLASSIFIED.

(U) It is important to note that while Figure 16 provides a visual into trends of non-compliance, the non-compliance rate is less than 1%. The tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection.[52] The tasking incident rate decreased to 0.04% during this reporting period, which is historically low. As previously noted, the increase in the tasking incident rate reported in the 20th Joint Assessment was primarily to a single NSA targeting office misunderstanding how to use a targeting tool. The tasking compliance incident rate involving facilities used by United States persons remained almost zero. 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. The percentage of compliance incidents involving detasking incidents has remained consistently low. The detasking compliance incident rate involving facilities used by United States persons was also close to zero.

[52] (U) Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have reasonably known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. Detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.

[redacted]

(U) C. FBI: Number of Compliance Incidents

(U) The total number of compliance incidents identified relating to FBI's targeting procedures slightly decreased as compared to the last period. The number of errors relating to FBI's minimization and querying procedures substantially increased this reporting period. The high number of incidents can almost entirely be attributed to one event relating to improper queries.[53] These non-compliant queries were conducted by a limited number of personnel, and were conducted as part of a batch query function in a FBI system.[54]

(U) Classified Figure 17 shows the classified number of incidents for the last ten reporting periods (*i.e.*, from the 14th through the 23rd reporting periods). With the exception of the 19th through the 23rd reporting periods, the number of FBI's identified targeting, minimization, and querying errors remained consistently low. The joint oversight team assesses that the increase in identified FBI errors beginning in the 20th reporting period is attributable to various factors. In particular, NSD increased its focus on reviewing FBI querying practices; this focus resulted in NSD's increased experience in evaluating those types of FBI queries and NSD's increased knowledge of the FBI systems storing Section 702-acquired information. When these two factors were combined with a particular sample population of FBI users in the reviews NSD conducted, it resulted in NSD identifying a larger number of non-compliant queries.

(U) Notwithstanding the large number of querying incidents in this reporting period, 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. As it pertains to the querying incidents, the joint oversight team has worked closely with FBI on developing additional training for FBI personnel on the query requirements, and, subsequent to the reporting period, FBI has undertaken efforts to update its internal systems in ways that should help facilitate a decrease in the number of querying incidents in future reporting periods. More information about these errors, including the causes and remedies, are provided in the Section III below reviewing FBI's compliance incidents. The FBI has been working to address and resolve identified compliance issues. The remedial and mitigation steps taken by the FBI to address these issues are discussed in Section III below.

[53] ~~(S//NF)~~ Specifically, in the 23rd reporting period [redacted] incidents of non-compliance with the FBI targeting or minimization procedures were identified. The vast majority of these incidents pertains to non-compliant queries, and in particular, two compliance errors comprise nearly the entire [redacted] incidents.

[54] ~~(S//NF)~~ The FBI system, in which the non-compliant batch queries were conducted, was FBI [redacted]

(U) Figure 17: Number of Compliance Incidents Involving the FBI Targeting and Minimization Procedures

(U) Figure 17 is classified ~~SECRET//NOFORN.~~

(U) In light of the joint oversight team's decision to provide the NSA targeting compliance incident rate above, the joint oversight team determined that it would also increase transparency to include a metric representing the FBI targeting compliance incident rate. This rate was provided in previous Joint Assessments, but it was discontinued in the 17th Joint Assessment as the joint oversight team believed, at the time, that the overall compliance incident rate and total number of FBI incidents provided in Figure 17 were more useful. The FBI targeting compliance incident rate was reintroduced in the 21st Joint Assessment. During this reporting period, the FBI targeting compliance incident rate was 0.005%, a slight decrease from the previous period (0.007%). Historically, this rate has remained well below one percent. The joint oversight team assesses that FBI's compliance with respect to targeting is a result of its training, systems, and processes.

(U) As discussed above, the joint oversight team has decided to provide a metric depicting FBI's query error rate. Figure 18 provides the FBI query compliance incident rate, which is calculated as the total number of FBI query compliance incidents reported by NSD to the FISC during the reporting period, expressed as a percentage of the total number of FBI queries audited by NSD in connection with the field office reviews during which NSD identified the FBI query compliance incidents reported to the FISC during the reporting period.

(U) Figure 18: FBI Query Compliance Incident Rate

~~SECRET//NOFORN~~

(U) FBI query compliance incidents reported to the FISC during the reporting period (June 1, 2019 – November 30, 2019)	[redacted]
(U) Number of FBI queries audited by NSD in connection with field office reviews during which NSD identified the FBI query compliance incidents reported to the FISC during the reporting period[55]	
(U) FBI query compliance incident rate: number of query incidents reported, divided by number of queries audited	(U) 36.59%

~~SECRET//NOFORN~~

(U) Figure 18 is classified ~~SECRET//NOFORN~~.

(U) In connection with its reviews at FBI field offices, NSD reviews a sample of queries conducted by FBI personnel in FBI systems that contain unminimized FISA-acquired information, including Section 702-acquired information. FBI provides NSD with logs of all the queries conducted in its systems during a given three-month period preceding the relevant field office review. NSD reviews the query logs and then consults with FBI personnel to obtain additional facts regarding the queries that were conducted. It is possible that some of the queries in the logs provided by FBI were not run against Section 702-acquired data, as NSD's query audits are designed to review compliance with FBI's query requirements in all of its applicable FISA procedures.[56] The FBI query error rate may also include identical queries that were conducted multiple times. For example, if NSD discovered that the same improper query was conducted on two separate occasions, that would be counted as two compliance incidents.

(U) Neither the number of incidents reported in Classified Figure 17, nor the FBI query compliance incident rate in Classified Figure 18, is based on the number of compliance incidents that *occurred* during a given reporting period. Rather, each is based on the number of incidents that were *reported* to the FISC as compliance incidents during the reporting period. There may be delays in resolving and reporting compliance incidents after they are first identified, in part, because of delays in the Government's investigation while FBI gathers the relevant facts, or while FBI and NSD discuss whether the facts of a matter constitute a compliance incident. Incidents that occur

[55] (U) This number also includes the number of FBI queries audited by NSD in connection with any field office reviews completed by NSD during this reporting period for which no FBI query compliance incidents were discovered.

[56] (U) FBI personnel may elect to run queries against FISA Titles I, III, and V but not against Section 702-acquired information. The query logs reviewed by NSD for its query audits include queries of information acquired pursuant to all FISA authorities, and the joint assessment team has not attempted to identify and exclude any queries that were included in the query logs but not run against Section 702-acquired information.

during a given reporting period, accordingly, may be reported over multiple assessments, and the number of incidents reported in a given assessment may include incidents that occurred during multiple periods. The number of query compliance incidents reported in Classified Figure 18, and the FBI query compliance incident rate in Classified Figure 18, may, therefore, include queries audited by NSD during the reporting period for a prior Joint Assessment.

(U) In addition, because of the delays in resolving and reporting certain compliance incidents, incidents discovered at a single field office review may be reported during different reporting periods. When that occurs, the total number of FBI queries audited by NSD in connection with the relevant field office review is included in the denominator of the FBI query compliance incident rate for both reporting periods, even though the total number of FBI query compliance incidents discovered as a result of auditing those queries is split between reporting periods. There were two field office reviews for which some, but not all, of the FBI query compliance incidents were reported during this reporting period.

(U) Although each of the metrics in Classified Figure 17 and Classified Figure 18 has limitations, the joint oversight team believes that they nevertheless provide informative measures of FBI's compliance with its querying procedures.

(U) D. CIA and NCTC: Number of Compliance Incidents

~~(S//NF)~~ There were [redacted] incidents during this reporting period that involved CIA's minimization and querying procedures,[57] which is the same number of incidents reported in the previous reporting period. 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 and querying procedures and the work of its internal oversight team.

~~(S//NF)~~ There were [redacted] incidents during this reporting period that involved NCTC's minimization and querying procedures, which is a decrease from the previous reporting period.[58] The joint oversight team assesses that NCTC's overall compliance is a result of its training, systems, and process that were implemented when NCTC was authorized to receive certain unminimized Section 702-acquired information.

(U) Classified Figure 19 provides the classified number of minimization and querying errors that involved CIA for the last ten reporting periods and NCTC for reporting periods beginning with the 19th assessment period. These numbers have remained consistently low for CIA and for NCTC. The joint oversight team assesses that CIA's and NCTC's compliance is a result of its training, systems, and processes that were implemented by each agency.

[57] (U) Recall that CIA does not have targeting procedures and may not target. Because CIA only has minimization procedures and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

[58] (U) Recall that NCTC does not have targeting procedures and may not target. Because NCTC only has minimization procedures and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

(U) Figure 19: Number of Compliance Incidents Involving the CIA or NCTC Minimization and Querying Procedures

(U) Figure 19 is classified ~~SECRET//NOFORN~~.

(U) E. Service Providers: Number of Compliance Incidents

(U) ~~(S//NF)~~ Finally, there was one incident of non-compliance caused by an error made by communications service providers in this reporting period, which represents an increase from the zero incidents reported in the prior reporting period. The joint oversight team assesses that the historically 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, Minimization, and Querying 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 Section 707 Report provides further details regarding each individual incident and information on applicable remedial and mitigating actions. For each individual incident in the Section 707 Report, details are provided as to how any erroneously acquired, disseminated, or queried information was handled through various purge, recall, and deletion processes. Information is also provided about personnel remediation and, when applicable, wider training efforts to address incidents. In certain instances, processes or technical tools are adjusted, as appropriate, to remedy the incidents, to mitigate impact, and to reduce the potential for future incidents.

(U) 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, minimization, and querying 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, minimization, and querying procedures.

(U) The NSA compliance incident rate for this reporting period, excluding FBI, CIA, and NCTC compliance incidents, is 0.20% and represents a decrease from the NSA compliance incident rate of 0.48% in the previous reporting period.

(U) 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 improper queries which were not reasonably likely to return foreign intelligence information due to their design. Regardless of United States person status, robust oversight is conducted to ensure compliance with all aspects of the targeting and minimization procedures; all identified incidents are reported to the FISC and to the Congress, and all incidents are required to be appropriately remedied. As with all incidents, the joint oversight team works closely with NSA to identify causes of incidents in an effort to prevent future incidents, regardless of United States person status.

(U) In the subsections that follow,[59] this Joint Assessment examines some of the underlying causes of incidents of non-compliance. This Joint Assessment first begins by examining and explaining incidents impacting United States persons' privacy interests, even though those incidents represent a minority of the overall incidents, followed by a discussion of other types of human errors and communication issues. The joint oversight team believes that analyzing the trends of these incidents, especially with regard to their causes, helps 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 non-compliance with the targeting, minimization, and querying procedures, including any necessary purges resulting from these incidents. Both the tasking compliance incident rate and detasking compliance incident rate involving facilities used by United States persons were low during this reporting period. 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 erroneously acquired, disseminated, or queried

[59] (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.

United States person information was remediated through various purge, recall, and deletion processes.

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

(U) ~~(S//NF)~~ During this reporting period, 3.7% of the tasking errors involved instances where facilities used by United States persons were tasked pursuant to Section 702. This represents a slight increase from the prior reporting period.[60] 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. These incidents represent isolated instances of insufficient due diligence, or other oversights, and did not involve an intentional effort to target a United States person. The majority of these tasking errors involved situations where an analyst made an erroneous assessment, overlooked information, and/or conducted insufficient research prior to tasking a facility and, as a result, inadvertently tasked a facility used by a United States person. In all of the incidents, personnel were reminded of the Section 702 tasking requirements, use of any applicable collection was restricted in NSA's systems, and the collection was purged as required by NSA's targeting and minimization procedures.

~~(TS//SI//NF)~~ For example, a few incidents were caused due to analysts misunderstanding the tasking requirements as they pertained to United States persons [redacted]

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

(U) During this reporting period, 5% of the detasking delays involved facilities used by a United States person. This represents a slight decrease from the last reporting period.[62] The detasking delay incidents impacting United States persons in this reporting period were caused by unintentional human errors, such as misunderstandings of the detasking requirements and analysts' faulty analysis of information that erroneously led them to continue to assess that the target was a

60 [redacted]

61

62

non-United States person located outside the United States or instances of poor interagency communication. In all of the incidents, personnel were reminded of the Section 702 detasking requirements, any applicable collection was purged, and no reporting was identified based on the collection. If any of the applicable collection was subsequently identified as having not been deleted or recalled as required, that failure would be reported as a compliance incident.

~~(TS//SI//NF)~~ In one example of a delayed detasking, while processing [redacted]

(U) B. Effect of Human Error

(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. Each of the agencies has established processes to both reduce human errors and to identify such errors when they occur. Some human errors, such as those resulting from misunderstanding the rules and procedures, can be mitigated with additional training and guidance. These processes and trainings have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated.

(U) (1) Tasking & Destasking Errors

(U) This section discusses some of the common types and causes of tasking errors and detasking delays from this reporting period, along with the corresponding compliance trends.[64] The majority of the detasking delays during this reporting period involved (i) non-United States persons who either traveled to the United States or appeared to have traveled to the United States, or (ii) unexplained indications that a Section 702-tasked account appeared to have been accessed from within the United States.

- (U) "Foreignness determination" errors – Certain tasking errors result from NSA not properly establishing a sufficient basis to assess that a target was located outside the

63 [redacted]

64 [redacted]

United States (otherwise referred to as the "foreignness determination") or not sufficiently addressing conflicting information that calls into question whether a target was located outside the United States. During this reporting period, approximately 12.0% (a decrease from the previous reporting period, which reported approximately 16.4% of these tasking errors) of tasking errors were the result of insufficient foreignness determinations.[65] Certain of these incidents involved the failure to conduct a necessary foreignness check prior to tasking, or involved too long of a delay between the necessary foreignness checks and the tasking of the facility. In many of these incidents, NSA advised that it acquired no data from the erroneous tasking. However, in the instance data was acquired, it was purged as necessary.

- (U) "Foreign intelligence information purpose" errors – Certain tasking errors result from NSA's failure to establish a valid "foreign intelligence information purpose" for the tasking (*i.e.*, that the targeted user is reasonably expected to possess, receive, and/or is likely communicate foreign intelligence information as defined in 50 U.S.C. § 1801(e)) in relation to the categories of foreign intelligence information specified in the Section 702 certifications. During this reporting period, approximately 11% of tasking errors (a decrease from the previous reporting period, which reported 23% of these tasking errors),[66] were the result of NSA not having a sufficient foreign intelligence purpose for the tasking. In all of the instances, at the time of tasking, NSA had sufficiently established that the users were non-United States persons located outside the United States. Any erroneously collected information was purged, and no reporting was identified.

~~(U//FOUO)~~

- ~~(U)~~ Typographical errors – Certain tasking errors result from typographical or similar errors. During this reporting period, approximately 39% of tasking errors (a slight increase from the previous reporting period) involved such typographical or similar errors. The majority of these errors were caused by CIA. An additional approximately 3.7% of tasking errors were caused by NSA analysts inadvertently [redacted] of a certain type of facility. In each case, NSA advised that there was no indication that the relevant facilities were used by a United States person or by someone in the United States. NSA and CIA further advised that each had completed any required purges and had identified no reporting based on this collection.[67]

~~(U//FOUO)~~

- ~~(U)~~ Incorrect providers – Certain tasking errors result from NSA inadvertently tasking a facility to an incorrect provider. During this reporting period, 4% of tasking errors (a substantial decrease from the previous reporting period) involved tasking a facility to an incorrect provider. As noted in the previous Joint

65 [redacted]

66 [redacted]

67 [redacted]

Assessment, NSA took steps to address these errors, including reminding Section 702 adjudicators who review proposed taskings to look specifically for this type of error. In addition, in May 2019, NSA implemented a technical solution [redacted] NSA, CIA, and FBI advised that they each completed any required purges, and that each has identified no reporting based on this collection.

- (U) Incomplete detaskings – Certain detasking delays result from NSA detasking (or another agency requesting that NSA detask) some, but not all, of a target's facilities. During this reporting period, 15% of detasking delays (a slight decrease from the previous reporting period) involved such incidents where certain of a target's facilities were not timely detasked. Again, any data acquired as a result of such detasking errors is required to be purged.

(U) As noted above, some of the above tasking and detasking errors were caused by personnel misunderstanding or misapplying the rules or procedures related to tasking or detasking, while others were caused by inadvertent human errors. In each case, the relevant agency had advised that it reminded its personnel about the Section 702 tasking and detasking requirements, or to exercise care when completing tasking and detasking processes, as applicable.

(U) (2) Minimization and Querying Errors

(U) NSA's minimization procedures have various requirements, including rules regarding under what circumstances Section 702-acquired information may be *disseminated*, and rules regarding how long unminimized Section 702-acquired information may be *retained*. NSA's querying procedures also have various requirements, including rules regarding *querying* unminimized Section 702-acquired information. Particular issues of non-compliance with minimization procedures are detailed below.

(U) Querying Rules: During this reporting period, NSA's querying procedures included two types of restrictions on querying unminimized Section 702 collection.

1) (U) NSA's Section 702 querying procedures in effect during this reporting period required that queries of unminimized Section 702 collection *must be designed in a manner "reasonably likely to return foreign intelligence information."* For example, if a query does not meet this standard due to a 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) (U) Although NSA's Section 702 querying procedures in effect during this reporting period permitted queries of unminimized Section 702 collection using United States person identifiers, such queries *must be approved by NSA OGC*. If an NSA analyst used a United States person identifier that had not been approved by NSA OGC to query Section 702-acquired data, it constituted a compliance incident.

[68] (U) For example, this type of query error occurs when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially receives overly broad results as a result of the query.

(U) During this reporting period, NSA minimization and querying incidents accounted for 29% of all NSA incidents of noncompliance, as compared to 66% in the previous reporting period, including a notable decrease in the number of minimization incidents.[69]

(U) As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization and querying procedures. In the previous reporting period, approximately 94% of NSA's minimization and querying incidents involved improper queries. During this reporting period, out of all of NSA's total minimization and querying errors, approximately 88% involved improper queries, of which:

- (U) Approximately 50.1% of the minimization and querying errors involved queries that were not reasonably likely to return foreign intelligence information. The total number of such non-compliant queries decreased substantially from the previous reporting period. The substantial decrease was mainly due to one compliance error reported in the prior period that caused several hundred non-compliant queries. During this reporting period, some of the non-compliant queries were caused by NSA analysts not including sufficient limiting criteria in the query term, or incorrectly formatting the query such that it was not appropriately limited; other errors were caused by typographical errors; and still other errors were caused by analysts querying identifiers that did not have a sufficient foreign intelligence connection.[70] NSA advised that, in each case, the relevant personnel had been reminded of the query requirements and that all query results had been deleted or aged-off.

- (U) Approximately 38.6% of the minimization and querying errors involved NSA analysts conducting queries using a United States person identifier without approval. The total number of such United States person queries also substantially decreased

[69] ~~(S//NF)~~ Minimization and querying incidents decreased to [redacted] incidents in the previous reporting period. As noted above, the number of minimization and querying incidents during the previous reporting period was unusually high because a small number of individual errors caused a large number of minimization and querying incidents.

[70] ~~(TS//SI//NF)~~ There were [redacted] such non-compliant queries during this reporting period, compared to [redacted] in the previous reporting period. In one example, an NSA analyst queried a generic term and did not include sufficient limiting criteria. In a second example, there were [redacted] queries during the reporting period that involved queries of Section 702-acquired metadata using terms associated in some manner with [redacted] The query terms included United States person identifiers associated with [redacted] NSA analysts indicated that they ran the queries because [redacted] Although the NSA analysts who ran the queries were searching for [redacted] the metadata queries were not reasonably likely to retrieve foreign intelligence information and did not meet the requirements of the NSA querying procedures. [redacted]

from the previous reporting period.[71] The substantial decrease was mainly due to a small number of compliance errors reported in the prior period that each involved large numbers of improper queries. During this reporting period, in one incident, FBI provided an NSA analyst with a list of identifiers associated with foreign-located members of a terrorist group. The NSA analyst mistakenly assumed that the list of identifiers did not need to be checked to determine if any of the identifiers were used by United States persons prior to conducting the queries. The list did include United States person identifiers, and as a result, the analyst inadvertently queried the United States person identifiers without the necessary approvals. Subsequently, an NSA auditor discovered the error, and the query results were confirmed deleted. NSA advised that the relevant analyst would receive additional training and had been reminded to exercise care when performing this task.

(U) The joint oversight team assesses that NSA's overall training and guidance to its personnel has contributed to its overall compliance with its querying procedures, although individuals continue to make mistakes. The joint oversight team has reviewed the human errors that caused the minimization and querying errors during this reporting period and has not identified any discernible patterns in the types or causes of these errors.

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

(U) Dissemination Rules: NSA's minimization procedures set forth requirements for the dissemination of United States person information. In the current reporting period, incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in NSA's minimization procedures represented approximately 9% of the total number of minimization and querying incidents. The overall number of dissemination incidents decreased substantially from the prior reporting period.[72] The substantial decrease was mainly due to the large number of improper disseminations during the prior reporting period that were caused by one NSA target office's misunderstanding of how to use a software tool to redact United States person identities. Improper disseminations of United States person information are usually the result of a human error oversight, generally because United States person information that is not necessary to understand foreign intelligence information is included in the dissemination. For example, in one instance, an NSA analyst discovered that NSA had issued a report that included the name of a United States person whose identity was not necessary to understand foreign intelligence information. The error occurred because the analyst did not conduct sufficient due diligence prior to disseminating the information. NSA recalled the report and reissued it without the United States person information. NSA advised that the relevant personnel have been reminded

[71] ~~(S//NF)~~ There were [redacted] United States person query incidents involving NSA during this reporting period, compared to [redacted] in the previous reporting period. All [redacted] incidents involved NSA analysts using United States person identifiers that had not been approved to query Section 702-acquired data.

[72] ~~(S//NF)~~ There were [redacted] incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in the NSA minimization procedures, compared to [redacted] in the previous reporting period. As reported in the previous Joint Assessment, [redacted] of the dissemination incidents from the prior reporting period were caused by a systemic error in one target office.

of the Section 702 dissemination requirements.[73] In another instance, the error occurred because disseminations of United States person information were distributed to a broader group of recipients than is permitted by NSA's Section 702 minimization procedures. The joint oversight team has reviewed the human errors that caused the dissemination errors during this reporting period and has not identified any discernible patterns in the types or causes of these errors.

(U) As was the case with NSA querying incidents, there were no identified NSA incidents of an analyst intentionally violating the dissemination rules.

~~(S//NF)~~ Retention Rules: There were [redacted] incidents where NSA inadvertently retained information acquired pursuant to Section 702 that should have been purged.[74] These incidents primarily involved NSA system errors, including human error in system coding. In one incident, [redacted] records derived from FISA-acquired data, including Section 702-acquired data, was retained longer in NSA systems than would be permitted by NSA's Section 702 minimization procedures. Based on the types of NSA systems where the data was over-retained, NSA assesses it is unlikely that any of the over-retained records would have been used in any disseminations, FISA applications, or taskings pursuant to Section 702 of FISA. NSA has deleted the over-retained records from its systems.

(U) (3) Other Errors

(U) Documentation Errors: The NSA targeting procedures require that for each tasked facility NSA document the source of the "foreignness determination" and identify the foreign power or foreign territory about which NSA expects to obtain foreign intelligence information. The targeting procedures also require a written explanation of the basis for its assessment, at the time of targeting, that the target is expected to possess, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked ("foreign intelligence purpose"). The number of documentation errors increased to approximately 14.7% of the total number of compliance incidents in this period from 9% in the prior reporting period.[75] In all of these incidents, while the actual tasking of each facility was appropriate, the analyst failed to sufficiently document the "foreignness determination" or the "foreign intelligence purpose" on the tasking sheet, or the Section 702(h) certification to which the facility was tasked was not appropriate based on the documented foreign intelligence purpose. NSA advised that it subsequently issued reminders to the analysts to review tasking sheets thoroughly prior to

[73] [redacted]

[74] ~~(TS//SI//NF)~~ For example, there were [redacted] incidents involving the retention of unminimized Section 702-acquired data beyond the period permitted by NSA's Section 702 minimization procedures, as well as [redacted] incidents involving NSA's failure to purge Section 702-acquired information that was required to be purged pursuant to NSA's Section 702 targeting procedures.

[75] ~~(S//NF)~~ [redacted] incidents resulted from documentation errors, representing a decrease from the last reporting period, [redacted] However, the number of documentation errors resulting from the tasking of a facility to a different DNI/AG Section 702(h) certification than intended remained high, increasing [redacted] in the prior reporting period.

submission and to select the proper certification based on the information they want to receive from the user.

(U) Notification Delays: Finally, there were a number of reported incidents where NSA failed to timely provide the required notice to NSD and ODNI after NSA has discovered that a tasked selector was used from within the United States or by a United States person. Notification errors increased significantly to 18% in this reporting period from 1.12% in the last reporting period.[76] NSA advised that the increase in these types of errors during this reporting period was due to a staffing shortage combined with an increase in reported incidents. NSA further advised that it subsequently hired an additional staffer and implemented a weekly auditing process to ensure the required notice to NSD and ODNI is provided in a timely manner.

(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 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 this reporting period, approximately 15% of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.[77] This is only a slight decrease from last reporting period's 19.4% and, thus, the joint oversight team assesses that there is still room to improve agency communication. The detasking delays caused by miscommunication typically involved travel or possible travel of non-United States persons to the United States. Further, none of the tasking errors involved situations in which intra-agency miscommunications resulted in the erroneous tasking of a facility.

(U) The joint oversight team assesses that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its ongoing oversight efforts, the joint oversight team will also continue to monitor NSA, CIA, FBI, and NCTC's Section 702

[76] ~~(TS//SI//NF)~~ There were [redacted] reporting delays in this reporting period, and in [redacted] of the incidents the only violation was a failure to provide the required notice to NSD. These reporting delays rang from one to 56 business days, with an average delay of approximately four business days and a median delay of approximately one business day. [redacted]

[77] ~~(S//NF)~~ There were [redacted] such incidents in this reporting period, a slight reduction from the [redacted] reported in the previous period. [redacted]

activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

(U) III. Review of Compliance Incidents – FBI Targeting, Minimization, and Querying Procedures

(U) There was a significant increase in the number of incidents involving noncompliance with the FBI targeting, minimization, and querying procedures, with a large majority of those incidents involving querying errors.[78] Most of the querying incidents were caused by personnel misunderstanding the application of the query standard in the context of batch queries.

(U) A. Targeting Incidents

~~(S//NF)~~ During this reporting period, there were [redacted] incidents involving non-compliance with FBI's targeting procedures, which represents a slight decrease from [redacted] incidents during the previous reporting period.[79] In all [redacted] cases, FBI personnel approved a request to [redacted] from a Designated Account prior to completing all searches of FBI systems required by the FBI targeting procedures. In one of the incidents, the request involved a United States person's communication and, therefore, the account was detasked. In the other incidents, FBI conducted additional searches after the review and advised that it had no information indicating that the Designated Accounts were used by a United States person or by someone located in the United States, thus, the accounts remained tasked. In all of the incidents, FBI personnel were reminded of the Section 702 requirements for tasking, including completing all the required searches in FBI systems.

(U) B. Minimization and Querying Incidents

(U) With respect to FBI's minimization and querying procedures, the total number of compliance incidents increased substantially from the previous reporting period. The vast majority of these errors involve FBI's use of a "batch query" tool. As discussed below, these non-compliant batch queries were conducted by a limited number of personnel, and some were conducted using a batch query function in a FBI system.[80] In addition to discussing the batch querying incidents, this assessment discusses retention errors and other query errors involving noncompliance with the FBI minimization and querying procedures. Details about remedial actions are provided below. In general, personnel involved in these compliance incidents were reminded of the requirements under FBI's minimization and querying procedures.

[78] ~~(S//NF)~~ As noted above, [redacted] compliance incidents involved violations of FBI's targeting, minimization, or querying procedures. While this represents a substantial increase over the [redacted] FBI compliance incidents reported in the previous reporting period, it is a decrease from the 21st Joint Assessment, which reported [redacted] FBI compliance incidents. Out of the total FBI compliance incidents for this reporting period, only [redacted] were targeting errors and the remaining [redacted] were minimization or querying errors.

[79] [redacted]

[80] ~~(S//NF)~~ The FBI system in which the non-compliant batch queries were conducted was FBI [redacted]

(U) (1) Batch Query Errors Caused by Misunderstanding or Lack of Awareness

(U) During this reporting period, FBI personnel conducted batch queries of large numbers of identifiers, including U.S. person identifiers, without having a reasonable expectation that such queries were likely to return foreign intelligence information or evidence of a crime. Because certain FBI systems permit users to conduct multiple queries as part of a single batch query, a single action can result in thousands of improper queries. For example, if a user wanted to conduct a query based on 100 e-mail accounts that had been in contact with a FISA target, the user could use the batch query tool, which would result in 100 queries being conducted using each e-mail account as a query term. In these incidents, although the FBI analysts conducted the queries for work-related purposes, such as attempts to investigate threats, the analysts misunderstood the application of the query requirements. Thus, as the FISC explained in its October 2018 opinion, "a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons."[81] Because of the impact of these batch queries, remedial and mitigation action was significant and is detailed below.

~~(S//NF)~~ ~~(U)~~ During this reporting period, the largest batch query incident was caused by FBI personnel misunderstanding or misapplying the query standard. A vast majority of the improper queries resulted from one employee's batch query; while that employee conducted the queries for work-related purposes, the query terms were not reasonably likely to retrieve foreign intelligence information or evidence of a crime and, thus, constituted compliance incidents.[82] To address these types of batch query compliance incidents where a single improper decision or assessment by FBI personnel results in noncompliant queries corresponding to a large number of individuals, the FBI recently imposed a requirement that individual queries conducted using the batch query tool in

[81] (U) *FISC's October 18, 2018 Opinion*, at 68.

[82] ~~(S//NF)~~ The largest single FBI compliance incident involved [redacted] improper batch queries of unminimized FISA-acquired information in [redacted] Specifically, an FBI staff operations specialist (SOS) conducted a batch query in [redacted] using the names and other identifiers (such as social security numbers and dates of birth) of individuals, including United States persons [redacted] The query involved the identifiers of approximately 16,000 individuals. The FBI believed that the batch query was compliant because, at the time of the query [redacted] However, NSD assessed that FBI had reason to believe that a particular query would be reasonably likely to return foreign intelligence information or evidence of a crime only [redacted] Given that NSD identified at two field offices this specific issue involving queries of identifiers associated with [redacted] NSD asked FBI to determine whether any similar queries have been conducted by other field offices.

~~(S//NF)~~ The FBI reports that the results of the batch query were not reviewed [redacted] To the extent such queries are discovered, NSD will report those instances to the FISC. NSD reminded the SOS about the query requirements in the FBI Section 702 query procedures and FBI's FISA minimization procedures. In its December 2019 Section 702 Opinion, the FISC found that, "the FBI's position that the queries for all 16,000 persons were reasonably likely to retrieve foreign intelligence information or evidence of a crime is unsupportable." *FISC's October 18, 2018 Opinion* at 67.

(U) This report erroneously cites the relevant FISC opinion. The reference should be to the *FISC's December 6, 2019 Opinion* at page 67.

[redacted] of 100 or more identifiers require FBI attorney approval prior to the queries being conducted. This change became effective in [redacted] as of June 29, 2021.

(U) (2) Query Errors Caused by Misunderstanding or Lack of Awareness

(U) During this reporting period, after batch queries are removed, most of the improper query incidents resulted from FBI personnel misunderstanding the querying rules even though the queries were conducted for work-management purposes or work-related purposes. These queries were not, however, reasonably likely to retrieve foreign intelligence information or evidence of a crime and, thus, constituted incidents. In most of the instances, FBI personnel did not fully understand the application of the query rules; however, it appears that in limited instances, FBI personnel explained that they did not recall why they ran the query.

(U) For example, some of the improper queries involved FBI personnel conducting queries, including using United States person identifiers, to research current or prospective state or local employees without a reasonable basis to believe the queries would be likely to return foreign intelligence information or evidence of a crime.[83] In another incident, NSD determined that FBI personnel conducted queries using United States person identifiers to look for evidence of public corruption without having a reasonable basis to believe the queries would be likely to return evidence of a crime.[84] FBI personnel also conducted queries that, while reasonably likely to return foreign intelligence information, were overly broad as constructed.[85] In all of these incidents, FBI personnel misunderstood the application of the query rules, and they were subsequently reminded of how to correctly apply the query rules.

~~(S//NF)~~ In other incidents, FBI personnel advised that they did not appreciate that queries would be running against unminimized FISA-acquired information and, thus, would be subject to

[83] ~~(S//NF)~~ In one incident, an FBI Task Force Officer (TFO) [redacted] conducted approximately [redacted] queries in [redacted] using the names and dates of birth of individuals who were [redacted] officer candidates [redacted] and were nearing graduation. [redacted] Insofar as the results of these non-compliant queries included raw FISA-acquired information, FBI advised that it did not disseminate or otherwise use any such information. ~~(S//NF)~~ In another incident, an SOS and a TFO conducting approximately [redacted] queries in [redacted] using the names and dates of birth of individuals who had [redacted] FBI advised that these queries did not return any Section 702-acquired information. [redacted]

[84] ~~(S//NF)~~ An SOS conducted approximately [redacted] queries in [redacted] using the names, and in some cases the dates of birth, of individuals and companies, including United States persons, who either held public office [redacted] area of responsibility or who had contributed money to the campaign of someone who had run for public office in that area. [redacted] Although the SOS advised that he/she conducted these queries in order to find evidence of a crime – specifically, to find evidence of public corruption – at the time of the query the SOS had no reason to suspect that any of the queries would retrieve evidence of a crime. During the review, the SOS advised that, to the best of his/her recollection, none of these queries returned any raw FISA-acquired information.

[85] ~~(S//NF)~~ An FBI linguist conducted [redacted] queries in [redacted] but failed to limit the search to results [redacted] Although these queries returned raw FISA-acquired information [redacted] advised that he/she did not disseminate or otherwise use any such information. [redacted]

the query standard. This is particularly the case with respect to query incidents that have been identified with queries run in a specific FBI database that contains non-FISA acquired and unminimized FISA-acquired information. As a result, for these queries, FBI personnel did not think to apply the query standard to their proposed queries before conducting queries in that particular FBI database, or failed to opt out of conducting queries against unminimized FISA-acquired information. A change that FBI has recently implemented to make [redacted] a default opt-out for searches of FISA-acquired information is designed to prevent this type of incident. At the time these queries were conducted, [redacted] was configured to automatically include FISA datasets – including data acquired pursuant to Titles I, III, and V as well as Section 702 of FISA – and any other datasets the user was authorized to access unless personnel intentionally excluded such data. Pursuant to a recent change the FBI has implemented, a user will now have to intentionally decide to opt-in to raw FISA datasets if the user wants to query those datasets. This change to [redacted] became effective on June 29, 2021.

(U) In addition to the minimization reviews conducted by NSD, described *supr*a in Section II, NSD also conducted National Security Reviews (NSRs) at FBI field offices during this reporting period. During an NSR, team members review, *inter alia*, a sampling of each office's national security assessments to verify that they were opened for an authorized purpose – that the basis for the assessment was not arbitrary or groundless speculation, nor based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin, or religion of the subject. *See generally* Attorney General Guidelines for Domestic Operations (AGG-DOM) at 10, 13, 16-19, Section II. While FBI personnel may query FBI systems containing unminimized Section 702 data as part of an assessment, any queries involving assessments that lacked an authorized purpose would be *ipso facto* improper, as such queries would not be reasonably likely to return foreign intelligence or evidence of a crime. Additionally, queries of the complainant (the person who provided the tip upon which the assessment was based) to assess the complainant's credibility would be improper absent a reasonable basis for believing that the query would return foreign intelligence information or evidence of a crime. During this review period, NSD identified through three of its NSRs six queries involving assessments that NSD determined had an authorized purpose, but where the complainant was improperly queried.[86] In all of these incidents, FBI personnel misunderstood the application of the query rules, and they were subsequently reminded of how to correctly apply the query rules.

~~(S//NF)~~ ~~(U)~~ There were also [redacted] incidents involving violations of the FBI's Section 702 querying requirements[87] that require the Government to promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that FBI identifies as concerning a United States person in response to a query that is not designed to find

[86] [redacted]

[87] (U) This requirement is not contained in the FBI's querying procedures. Rather, it is contained in the FISC's opinion approving the relevant annual certifications.

and extract foreign intelligence information.[88] Further, Section 702(f)(2)(A) provides that FBI may not access the contents of communications acquired pursuant to Section 702 that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information unless the FBI applies for an order from the FISC, based on probable cause, and the FISC enters an order approving the application. In these instances, NSD determined that these queries had been conducted solely to find and extract evidence of a crime as part of predicated criminal investigations. The [redacted] incidents were discovered by NSD while conducting oversight reviews at six FBI field offices. Subsequent investigation by the FBI into these queries revealed that they returned Section 702-acquired information, and NSD presumed that such information was reviewed by FBI personnel absent specific information to the contrary.[89] The system that was involved with these particular incidents was configured, at the time of the incidents, to preview content of responsive information for users when they executed a query. The FBI has since reconfigured the system at issue so that it no longer presents a preview of the content of unminimized Section 702-acquired information in response to a query. The users who executed these queries were unaware of the particular requirements of Section 702(f)(2), and of an option provided by the system to indicate that their queries were being run solely to extract evidence of a crime in support of a predicated criminal investigation. Because the queries were run using United States person query terms, to find and extract evidence of a crime, in support of predicated criminal investigations, and NSD had to presume that FBI personnel reviewed the Section 702-acquired information because of this system design issue, without first obtaining an order from the FISC, NSD reported these incidents to the FISC as potential violations of Section 702(f)(2)(A) of FISA.[90]

---

[88] [redacted]

[89] ~~(S//NF)~~ For queries in [redacted] during the period of time for this assessment, although FBI was able to confirm whether or not a user reviewed the contents of Section 702-acquired information returned by a query (*i.e.*, by opening the product(s) containing the Section 702-acquired information), the manner in which [redacted] was configured did not allow FBI to confirm whether a user was exposed to content that is previewed for the user on their computer screen in response to a query. With limited exceptions [redacted] query results returned to a [redacted] user would have generally included a 100 character context (or summary) field for each search result, which could include information from FISA-acquired products. When presented, this summary field consists of the 100 characters surrounding the individual search "hit" (*e.g.*, the query term) within the individual product. As a result, a [redacted] user could be exposed to FISA-acquired information in response to a query without actually clicking on the actual FISA-acquired product. Further, individual [redacted] users have the ability to customize the number of search results that appear on each screen page that the query returns (*e.g.*, 25, 50, 100 results per page) and have the ability to change those preferences at any time. During the period of time covered by this assessment, [redacted] was not designed to log how far down a user scrolls through search results on an individual screen, or to automatically report how many, or which, pages of search results an individual user clicks through. Accordingly, without any additional information (*e.g.*, the user remembers not reviewing the query results or the user set up his/her user preferences to not have the summary field displayed when the query results are returned), NSD presumed that the users would have viewed the content of the 702-acquired information in the summary field.

[90] ~~(S//NF)~~ For example, on March 12, 2019, an Operational Support Technician (OST) [redacted] ran a query in [redacted] using an identified United States person [redacted] in connection with a predicated criminal investigation [redacted] Subsequent investigation by the FBI into this query revealed that it returned two Section 702-acquired products which were displayed on a search results page that the OST clicked through. The FBI reports that none of these results were used for any further analytic, investigative, or evidentiary purpose. In addition, on April 3, 2019, the same OST ran [redacted] queries in [redacted] using an individual's name as the query term, as well as a query of the individual's name in combination with the individual's date of birth, and queries of e-mail accounts, a phone number used by this United States person, all in connection with a predicated

(U) In these incidents, NSD reminded the personnel about the query requirements in the FBI Section 702 query procedures and FBI's FISA minimization procedures, and discussed these requirements with other personnel during NSD's training conducted for the field offices. In addition to the reconfiguration of the system at issue as noted above, if the user seeks to access Section 702-acquired content returned from a query, the system will force the user to complete the query in another FBI system. That other FBI system requires the user to answer a question in a pop-up box that asks whether the query is being done only to retrieve evidence of a crime. An information icon also is provided, providing the user with information relating to the requirements of Section 702(f)(2) of FISA. FBI designed the radio buttons, however, to automatically default the answer to this question in the system to "No." If a user proceeds from that default "No," they are able to select from a series of pre-populated justifications for their query, or select "other" and provide their own, written justification. Once the system receives that justification from the user, it allows the user to access the contents of the Section 702-acquired information. If, however, the user answers "Yes" to the question as to whether it is a query being done to retrieve evidence of a crime, the user is provided with three drop-down justifications for their query: "Court Order"; "Exigent Circumstances" or "Neither". If a user selects "Court Order" or "Exigent Circumstances", she is allowed to proceed to access the contents of the Section 702-acquired information. At that same time, an alert is sent to FBI's NSCLB, which then conducts additional research into the nature of the query, and coordinates as necessary with NSD. If the user selects "Neither", they are prevented from accessing the contents of the Section 702-acquired information, and are provided with an alert that instructs her that she either needs to obtain an order from the FISC or have exigent circumstances to be able to review the contents of the Section 702-acquired information. This alert also directs the user to contact NSCLB or their field office Chief Division Counsel with any questions.

(U) (3) Other Errors Caused by Misunderstanding or Lack of Awareness

(U) During this reporting period, there were some incidents that involved non-compliance with the provisions of the FBI minimization procedures concerning establishment of a review team for a target charged with a crime pursuant to the United States Code.[91] As soon as the FBI knows that a target is charged with such a crime, FBI's minimization procedures require that the FBI follow certain steps, including establishing a review team of one or more monitors. The members

---

criminal investigation [redacted] Subsequent investigation by the FBI into these queries revealed that they returned four Section 702-acquired products which were displayed on a search results page that the OST clicked through. These queries were conducted using United States person query terms, to find and extract evidence of a crime, in support of predicated criminal investigations unrelated to national security. The FBI reports that none of these results were used for any further analytic, investigative, or evidentiary purpose. NSD reported these queries as violations of Section 702(f)(2)(A) of FISA and section IV.A.2 of the FBI Section 702 query procedures.

[91] ~~(S//NF)~~ [redacted] The joint oversight team assesses that one incident was the result of a misunderstanding of the review team requirement in the FBI Section 702 minimization procedures, while the other incident was the result of a miscommunication between FBI divisions. In these incidents, the relevant personnel have been reminded about the requirements in the FBI Section 702 minimization procedures regarding attorney-client communications, including the review team requirements. Of note, there were [redacted] such incidents in the previous reporting period. The joint oversight team assesses that NSD's oversight reviews, NSD's and FBI's training at FBI field offices on the attorney-client privileged communication provisions of the minimization procedures, and the modified automated tool FBI uses to request [redacted] will continue to help facilitate both the identification of review team compliance incidents and assist in the prevention of any future incidents.

of the review team must be individuals who have no role in the prosecution, and they initially assess and review the Section 702-acquired information to determine whether the communications are attorney-client privileged. Failure to timely establish such a review team constitutes a compliance incident.

(U) ~~(S//NF)~~ Additionally, there was one incident where FBI personnel improperly disseminated United States person information acquired pursuant to Section 702.[92] The dissemination did not comply with section III.C.1.c, section IV.A, or section IV.B of FBI's Section 702 minimization procedures, in that the United States person information did not reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime.

(U) C. Remedial Steps Taken to Address Query Errors

(U) The joint oversight team has worked with FBI to re-focus existing training for field office personnel on the query requirements. Such focused training emphasizes the query standard, provides examples of compliant and non-compliant queries, and details how to opt out of querying unminimized FISA-acquired information. Additionally, in June 2018, FBI, in consultation with the joint oversight team, issued guidance to all components where personnel had access to unminimized FISA-acquired information. This guidance explained the query standard and how to apply it. The guidance also discussed compliance issues involving the application of the query standard, including issues relating to queries run using the "batch" search function. Additional emphasis was provided concerning issues involving queries run against unminimized 702-acquired information to find and extract only evidence of a crime (and not foreign intelligence information). Each FBI field office was instructed to train their personnel on the June 2018 guidance.

(U) Further, while outside the reporting period for this current joint assessment, in January 2019, FBI and NSD conducted joint training for all FBI NSCLB personnel and all field office legal personnel, on FBI's querying procedures. FBI field office legal personnel were instructed to provide this training to all personnel with access to unminimized FISA-acquired information. In fall 2019, FBI, in consultation with NSD, developed and deployed mandatory training for FBI personnel on the query standard and on the system changes FBI made to address the query issues. FBI is also currently developing revised standard training for personnel who have access to unminimized FISA-acquired information, which will involve an increased focus on the query standard.

(U) NSD has also undertaken additional query training at FBI field offices. At each FBI field office where NSD conducts a minimization review, NSD generally conducts training for the field office on minimization-related topics. NSD has addressed the query standard during these trainings since 2016, and since then, has significantly increased the amount of time spent during these training sessions on the query standard and query incidents. This training includes multiple hypothetical examples derived from actual query incidents, and demonstrates, through screen captures, both how personnel can avoid query incidents in situations where they do not need to run their queries against unminimized FISA-acquired information and how personnel can select the

[92] ~~(S//NF)~~ The relevant personnel were reminded about the requirements in the FBI Section 702 minimization procedures. [redacted]

appropriate option to allow the FBI to better track and comply with requirements involving queries run against unminimized 702-acquired information to find and extract only evidence of a crime (and not foreign intelligence information).

(U) As part of the FBI Section 702 amended querying procedures[93] that were adopted by the Attorney General in 2019 and submitted to the FISC as part of the certification reauthorization process, the Government clarified the query standard in FBI's procedures to help facilitate a better understanding of the query standard, to the extent the prior language caused confusion. The amended procedures also instituted recordkeeping and documentation requirements for United States person queries and, in response the FISC ordered the Government to periodically update it on FBI's implementation of the new requirements.[94] Between September and November 2019, the FBI implemented changes to FBI systems storing unminimized FISA-acquired information that were necessary to comply with the amended procedures. Among other things, these changes require FBI personnel to provide a justification, explaining how their query meets the query standard when running queries of United States person query terms and when they seek to access Section 702-acquired contents returned by such queries. All query terms and justifications are logged for oversight purposes. In addition, FBI, in consultation with NSD, developed and deployed new training, as detailed above, for FBI personnel on the query standard and on the system changes. All personnel with access to unminimized FISA-acquired information were required to complete the training by mid-December 2019, and all personnel who subsequently require such access must first complete this training prior to being granted access. The joint oversight team believes that the above continuing efforts will help facilitate a better understanding of the query requirements.

(U) Finally, as detailed above, the FBI recently took additional steps to address the batch query compliance incidents and instances where users do not intend to query raw FISA-acquired information but fail to opt-out of such datasets through system and other changes. The joint oversight team anticipates that these changes should result in significant compliance improvements.

[93] (U) In August 2019, the Attorney General adopted amended FBI Section 702 querying procedures, which were subsequently approved by the FISC in September 2019, as part of the 2018 certifications.

(U) FBI's querying procedures for the 2019 Section 702 certification contained similar provisions and were approved by the FISC in December 2019, as a part of the FISC's *December 6, 2019 Memorandum Opinion and Order*. That opinion, along with other documents related to the 2019 Section 702 certification, was released in redacted form on September 4, 2020, on *IC on the Record*.

[94] ~~(S//NF)~~ During the latter part of this reporting period, the FBI implemented changes to [redacted] relating, among other things, to how those systems record United States person query terms and provide justifications for queries of United States person query terms. [redacted] "45-Day Report Regarding the Federal Bureau of Investigation's (FBI) Implementation of the FBI's Section 702 query procedures" (Sept. 26, 2019). Pursuant to these system changes, users will be prompted to provide certain information when conducting queries of United States person query terms. [redacted]

(U) IV. Review of Compliance Incidents – CIA Minimization and Querying Procedures

(U) ~~(S//NF)~~ During this reporting period, there were a small number of incidents involving noncompliance with the CIA minimization and querying procedures.[95] Those incidents involved instances of CIA improperly retaining Section 702-acquired information and unauthorized access to Section 702-acquired information by CIA personnel.

~~(TS//NF)~~ For example, in [redacted] ncidents, CIA retained certain United States person information that did not meet the relevant retention standard in CIA's databases; CIA subsequently minimized the improperly retained information and deleted any improper disseminations of the information. [redacted]

(U) V. Review of Compliance Incidents – NCTC Minimization and Querying Procedures

(U) During the reporting period, there were a small number of incidents involving violations of NCTC's minimization and querying procedures in effect at the time of the incidents.[96] Most of the incidents relating to NCTC's procedures during this reporting period involved improper queries of Section 702-acquired data. In these queries, NCTC personnel inadvertently omitted limiting syntax that would have otherwise narrowed the scope of the query. None of the queries were conducted using United States person identifiers.

~~(S//NF)~~ The remaining incident involved NCTC's improper disclosure of Section 702-acquired information in a manner that was not consistent with NCTC's Section 702 minimization procedures. Specifically, NCTC [redacted]

[95] ~~(S//NF)~~ CIA receives unminimized communications from selectors that it nominates to NSA for targeting [redacted]

[96] ~~(S//NF)~~ There were [redacted] total incidents during this reporting period. [redacted]

[redacted]

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

~~(S//NF)~~ During the reporting period, there was one reported instances of non-compliance by a "specified person" (*i.e.,* a provider) to whom the Attorney General and DNI have issued directives pursuant to Section 702(i) of FISA.[97] [redacted]

(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. Nevertheless, a continued focus is needed to address the underlying causes of the incidents that did occur, especially those incidents relating to improper queries. 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 ongoing 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.

97 [redacted]

APPENDIX

APPENDIX

(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]

(U) As affirmed in affidavits filed with the 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), FBI, and the National Counterterrorism Center (NCTC) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA, FBI, and NCTC, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA, FBI, and NCTC 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.

[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~~ [redacted]) NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA's review of [redacted] 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 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]

(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 [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, minimization, and querying 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 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 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 conducts the Mission Compliance Risk Assessment (MCRA) that assesses the risk of non-compliance with the rules designed to protect privacy and to safeguard information. Risks are assessed annually by authority and/or function for SIGINT and Cybersecurity Missions. The results are used to inform management decisions, priorities, and resource allocations regarding the NSA/CSS Comprehensive Mission Compliance Program (CMCP).

(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. Based on its foreign intelligence analysis, CIA may "nominate" a facility to NSA for potential acquisition under one of the Section 702(h) certifications. The nomination provides NSA with the basis for CIA's assessment [redacted]

[redacted]

11 [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] 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, minimization, and querying questions. Identified incidents of noncompliance with the CIA minimization and querying procedures are generally reported to NSD and ODNI by CIA OGC.

[redacted]

(U) III. Overview – NCTC

A. (U) NCTC's Handling of Section 702 data

~~(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 and querying 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 unminimized 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 FISA. 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 and querying procedures for Section 702-acquired counterterrorism data (Section 702 minimization procedures). In addition to documenting compliance with the Section 702 minimization and querying procedures requirements, [redacted] also documents the requests for [redacted] of Section 702-acquired information. This documentation includes the foreign intelligence justification (pertaining to counterterrorism) for [redacted] the facility and supervisory concurrence with an analyst's request.

~~(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. As a supplement to the requirements of NCTC's Section 702 minimization and querying procedures, NCTC's internal business process requires that NCTC analysts provide a written justification for each query, as well as a written justification for each minimization action to mark a product as meeting the retention standard in order to document how the query or minimization was compliant with the standards in NCTC's Section 702 minimization or querying procedures, as applicable. By internal policy, all [redacted] requests and minimization actions must be reviewed and approved [redacted] by the analyst's supervisor.

(U) ~~(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 (hereinafter, "NCTC Compliance") within the Office of Data Strategy and Compliance (ODSC) conducts periodic reviews of Section 702 query logs and minimization logs, as well as NCTC Section 702 disseminations in order to verify compliance with NCTC's minimization procedures and identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.

[redacted]

[redacted]

~~(S//NF)~~ [redacted] Pursuant to Section A.6 of NCTC's Section 702 minimization procedures, [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 unminimized 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 minimization and querying 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 all datasets pursuant to executive order, statute, interagency agreement, applicable IC policy, and internal policy. 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 Section 702 data, as well as administering and implementing NCTC Section 702 training, ensuring that all NCTC Section 702 collection is properly [redacted] minimized and disseminated, and that NCTC is complying with all minimization and querying procedures requirements.

(U) IV. Overview – FBI

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

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition communications. including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to

~~(S//NF)~~ The FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate for FBI must then apply its own, additional procedures, which require FBI to review NSA's conclusion of foreignness

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

[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 [redacted] information. Additional checklists have been created to capture information on requests withdrawn by [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 Technology and Data Innovation Section (TDI) (formerly named the Exploitation Threat Section (XTS)), FBI's [redacted] and FBI's Inspection Division (INSD). [redacted] TDI has the lead responsibility in FBI for [redacted] requests [redacted] TDI personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests [redacted] TDI also has the lead responsibility for facilitating FBI's nominations to NSA [redacted] TDI, 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 [redacted] In addition, NSD conducts training on the Section 702 minimization procedures at multiple FBI field offices each year.

(U) ~~(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. TDI and NSCLB 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 and Querying

(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; if the Government queries that collection, it must follow specific query rules. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. The FISC-approved querying procedures set rules for using United States person and non-United States person identifiers to query unminimized Section 702-acquired information. Prior to the FISA Amendments Reauthorization Act of 2017 codification, the minimization procedures contained querying rules. The 2018 certifications were the first certifications to contain the newly required querying procedures.

(U) 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.

(U) With passage of the FISA Amendments Reauthorization Act of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f)(1) requires that the querying procedures be consistent with the Fourth Amendment and that they include a technical procedure whereby a record is kept of each United States person term used for a query. Congress added other requirements in Section 702(f), which pertain to accessing certain results of queries conducted by FBI. Specifically, under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can review the contents of a query using a United States person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security.

(U) Queries may be conducted in two types of unminimized Section 702-acquired information: (i) Section 702-acquired *content* and (ii) Section 702-acquired *metadata*. Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to FISC-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to retrieve foreign intelligence information or, in the case of the FBI, evidence of a crime. This standard applies to all Section 702 queries, regardless of whether the term concerns a United States person or non-United States person.

(U) The agencies have similar querying procedures. For example, the agencies' procedures require a written statement of facts justifying that the use of any such identifier as a query selection term of Section 702-acquired content is reasonably likely to retrieve foreign intelligence information or, in the instance of FBI, evidence of a crime. Some querying rules are unique to individual agencies. For example, NSA's Section 702 querying procedures also require that any United States person query term used to identify and select unminimized section 702-acquired content must first be approved by NSA's Office of General Counsel and that such an approval include a statement of facts establishing that the use of any such identifier as a selection term is

reasonably likely to retrieve foreign intelligence information. In addition, with respect to queries of Section 702-acquired metadata using a United States person identifier, NSA's querying procedures require that NSA analysts document the basis for each metadata query prior to conducting the query.