

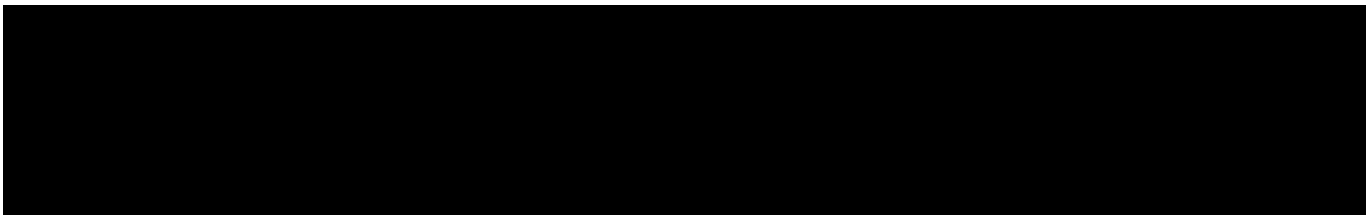
~~TOP SECRET//SI//NOFORN/TISA~~



(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, 2018 – November 30, 2018

March 2021



~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

**(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**

March 2021

(U) TABLE OF CONTENTS

(U) Executive Summary	5
(U) Section 1: Introduction	6
(U) Section 2: Oversight of the Implementation of Section 702	9
(U) I. Joint Oversight of NSA	10
(U) II. Joint Oversight of FBI	13
(U) III. Joint Oversight of CIA	16
(U) IV. Joint Oversight of NCTC	17
(U) V. Interagency/Programmatic Oversight	18
(U) VI. Training	18
(U) Section 3: Trends in Section 702 Targeting and Minimization	21
(U) I. Trends in NSA Targeting and Minimization	21
(U) II. Trends in FBI Targeting	26
(U) III. Trends in CIA Minimization	28
(U) IV. Trends in NCTC Minimization	30
(U) Section 4: Compliance Assessment – Findings	31
(U) I. Compliance Incidents – General	33
(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures	47
(U) III. Review of Compliance Incidents – FBI Targeting and Minimization Procedures	58
(U) IV. Review of Compliance Incidents – CIA Minimization Procedures	64
(U) V. Review of Compliance Incidents – NCTC Minimization Procedures	65
(U) VI. Review of Compliance Incidents – Other	65
(U) VII. Review of Compliance Incidents – Provider Errors	65
(U) Section 5: Conclusion	66
(U) Appendix	A-1

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~*(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)***(U) FACT SHEET****(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA)
Joint Assessments**

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as “Joint Assessments,” and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of March 2021, twenty-one 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.
- (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” and “minimization” procedures and, beginning in October 2018, “querying” procedures. The FISA Amendments Reauthorization Act of 2017 codified new requirements concerning Section 702, including requiring “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. Prior to the FISA Amendments Reauthorization Act of 2017 codification, the minimization procedures contained querying rules. The 2018 certifications (which became effective during this current assessment’s reporting period) were the first certifications to contain the newly required querying procedures.

(U) Highlights from 21st Joint Assessment:

- (U) *Compliance incident rate increased due to a single event.* The compliance incident rate increased significantly during this period, but the vast majority of incidents were caused by a single query event. When that single event is excluded, the compliance incident rate is generally consistent with previous periods.
- (U) *Continued focused efforts to implement Section 702 in a compliant manner.* This Joint Assessment reports that the agencies continued to implement the procedures in a manner that reflects a focused and concerted effort by Intelligence Community (IC) personnel to comply with the requirements of Section 702.

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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

- *(U) What compliance and oversight efforts underlie the Joint Assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, and constitutional requirements. A joint oversight team consisting of experts from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) 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 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. Beginning with the 16th Joint Assessment, this fact sheet has been included. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts, and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews of the targeting and minimization procedures. Section 4 describes compliance trends. The Joint Assessment describes the extensive measures undertaken by the Government to ensure compliance with court-approved targeting and minimization procedures; to accurately identify, record, and correct errors; to take responsive actions to remove any erroneously obtained data; and to minimize the chances that mistakes will re-occur.
- *(U) What are the types of compliance incidents discussed?* Generally, the Joint Assessment groups incidents into six or seven categories. Categories 1-4 (tasking incidents, detasking incidents, notification delays, and documentation errors) discuss non-compliance with targeting procedures. Category 5 discusses incidents of non-compliance with minimization procedures, such as 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.

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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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

March 2021

(U) Reporting Period: June 1, 2018, through November 30, 2018

(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-first joint compliance assessment of the Section 702 program. This assessment covers the period from June 1, 2018, through November 30, 2018 (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 4, 2019; 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 increase in 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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

reporting period – was 33.54%, which represents a significant increase from the prior period (4.36%). 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 14 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 0.22%.

(U) This joint assessment 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 18 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 23.94%.

(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. As required by the Act, 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

Note to Readers: The percentage, 0.22%, cited above is a typographical error. The correct percentage, 0.20%, is provided on page 40

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 raw FISA-acquired information, to include raw Section 702-acquired information.

² (U) See 50 U.S.C. § 1881a(m)(1).

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

herein. This report sets forth NSD and ODNI's 21st joint compliance assessment under Section 702, covering the period June 1, 2018, through November 30, 2018 (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:

An acquisition authorized under subsection (a)—

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

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

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(h) certifications⁴ 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

³ (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702, which was previously submitted on March 4, 2019, as required by Section 707(b)(1) of FISA (hereinafter, the "Section 707 Report"). This 21st Joint Assessment covers the same reporting period as the 21st Section 707 Report.

⁴ (U) Because of certain new requirements added in the 2017 Reauthorization Act, the statutory requirements regarding Section 702 certifications were moved from Section 702(g) to Section 702(h) of FISA following the codification of the 2017 Reauthorization Act. The 2018 certifications became effective in October 2018. Accordingly, this assessment reports on incidents and trends occurring pursuant to certifications approved under the prior law, which were in effect for approximately four and one-half months of this reporting period, and pursuant to certification approved under the new law, which were in effect for the remaining one and one-half months of this reporting period.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

pursuant to the Section 702(h) certifications.⁵ Four agencies are primarily involved in 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, the FBI had a significant number of compliance incidents related to querying of Section 702-acquired information. The FBI amended its 2018 querying procedures 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. 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. The 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 expects that the

5

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

remedial measures undertaken by FBI will allow it to better implement its querying procedures and follow the guidelines in such a manner.

(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 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 NCTC⁶ each handle Section 702-acquired data in accordance with their own minimization procedures.⁷ There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies from using preexisting systems to implement Section 702 authorities. Because of these differences in practice

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

⁷ (U) Each agency's Section 702 targeting, 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 2016 certifications in April 2017 and the 2018 certifications in October 2018. 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.

(U) With the codification of the FISA Amendments Reauthorization Act of 2017 (*see* P.L. 115-118), agencies are required to have querying procedures adopted by the Attorney General and reviewed by the FISC. The 2018 certifications, approved in October 2018, were the first certifications for which separate querying procedures were submitted and approved. Prior to that, the rules governing querying of Section 702-acquired data were contained in each agency's minimization procedures.

(U) In October 2018, the FISC found that CIA, NCTC, and NSA's querying procedures were sufficient, and that FBI's querying procedures were sufficient in certain respect and not sufficient in other respects. FBI began following its querying procedures, insofar as they were determined to be sufficient, in October 2018. After the FISC's decision in October 2018 and the Foreign Intelligence Surveillance Court of Review's (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) The Attorney General-approved querying procedures only for each agency became effective with the FISC-approved 2018 certifications in October 2018. Accordingly, compliance with the query rules contained in each agency's respective 2016 minimization procedures is assessed and discussed within this assessment for approximately four and one-half months of the reporting period, and compliance with each agency's respective 2018 querying procedures is assessed and discussed within this assessment for the remaining portion of the reporting period.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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 office of Mission Performance, Analysis, and Collection (MPAC).⁸ 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 facilities⁹ (also referred to as selectors) once collection begins. NSA must also minimize its collection in accordance with its minimization procedures and 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,¹⁰ 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.

⁸ (U) MPAC was previously called Office of the Deputy Director for Intelligence Integration/Mission Integration Division (ODNI DD/II/MID). Under this current assessment's reporting period, the ODNI reorganized and, as a result of this reorganization, ODNI DD/II/MID was renamed MPAC.

⁹ (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 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.

¹⁰ (U) The NSA targeting procedures require that the onsite reviews occur approximately every two months.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) Figure 1: NSA Reviews****UNCLASSIFIED**

Date of NSA Onsite Review	Targeting, Minimization, and Querying Reviewed
August 24, 2018	June 1, 2018 – July 31, 2018
October 26, 2018	August 1, 2018 – September 30, 2018
December 14, 2018	October 1, 2018 – November 30, 2018

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 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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) NSA's Section 702 minimization procedures in effect prior to October 18, 2018, provided that any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures.¹¹ 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). In both cases, the relevant 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.¹² For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the duration for which the United States person identifier has been authorized to be used as a query term, and any other relevant information. In addition, with respect to queries of Section 702-acquired *metadata* using a United States person identifier, NSA's minimization and querying procedures, as applicable, require that NSA analysts document the basis for each metadata query prior to conducting the query. NSD reviews the documentation for 100% of the metadata queries that NSA provides to NSD.¹³

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting, 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.¹⁴ The purpose of such reporting is to allow the joint oversight team to assess

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

¹² (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. Subsequently, the DNI publicly released the "CY2019 Transparency Report" on April 30, 2020; however, the CY2019 Transparency Report covered information outside this joint assessment's reporting period.

¹³ (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.

¹⁴ (U) If NSA had no prior knowledge of the target's travel to the United States and, upon learning of the target's travel, immediately "detasked" (i.e., stopped collection against) the target's facility, as is required by NSA's targeting

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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]

[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]¹⁵ 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.

(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 bimonthly reviews at FBI headquarters of FBI's compliance with its minimization procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews were conducted at FBI Headquarters on the dates shown in Figure 2.

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.

15 [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) Figure 2: FBI Reviews****UNCLASSIFIED**

Date of FBI Onsite Review	Targeting, Minimization, and Querying Reviewed
July 31 and August 1, 2018	June 2018 targeting decisions
September 11 and 12, 2018	July 2018 targeting decisions
October 10 and 11, 2018	August 2018 targeting decisions; June 1, 2018 – August 31, 2018, minimization and querying decisions
October 31, November 28 and November 29, 2018	September 2018 targeting decisions
January 16 and 17, 2018	October 2018 targeting decisions; September 1, 2018 – November 30, 2018, minimization and querying decisions
January 29 and 31, 2018	November 2018 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.¹⁶ 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) At the FBI reviews, with respect to minimization, the joint oversight team reviews documents related to FBI's application of its Section 702 minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations by the relevant FBI headquarters unit of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States person information.

(U) In addition to conducting minimization reviews at FBI headquarters, during this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention, querying, and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During those field office reviews, NSD reviewed a sample of retention decisions made by FBI personnel in their investigations that acquired Section 702 data and a sample of disseminations containing information acquired under Section 702 that FBI

¹⁶ (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]

The joint oversight team currently reviews all checklists and supporting documentation provided by FBI for approved requests for which information is returned by FBI's database queries.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

identified as potentially containing non-publicly available information concerning unconsenting United States persons. NSD also reviewed a sample of queries by FBI personnel in FBI systems that contain raw (unminimized) FISA-acquired information, including Section 702-acquired information. Those reviews ensure that the queries complied with the requirements in FBI's FISA minimization procedures, including its Section 702 minimization procedures and Section 702 querying procedures, as applicable. In addition, as a result of a Court-ordered reporting requirement in the FISC's *November 6, 2015 Memorandum Opinion and Order*¹⁷ 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 reviews at 14 FBI field offices during this reporting period and reviewed cases involving Section 702-task facilities.¹⁸ ODNI joined NSD at a subset of those reviews; ODNI received written summaries regarding all of the reviews from NSD regardless of whether ODNI was in attendance. Those reviews are further discussed in Section IV below.

(S//NF) Separately, in order to evaluate the FBI's [REDACTED] acquisition [REDACTED] and provision of [REDACTED] 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, annual process reviews occurred in May 2019 and June 2020.

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

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

(U) The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting and minimization procedures, the Attorney General's Acquisition Guidelines, or other

¹⁷ (U) The FISC's November 6, 2015 Opinion and Order approved the 2015 FISA Section 702 Certifications. On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, this *Opinion and Order* on the ODNI public website *IC on the Record*.

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

¹⁸ (S//NF) During those field office reviews, NSD reviewed [REDACTED] cases involving Section 702-task facilities.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

agencies' procedures in which FBI is involved.¹⁹ Those investigations are coordinated with FBI's Office of General Counsel (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.²⁰ 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 20, 2018	June 1, 2018 – July 31, 2018
November 14, 2018	August 1, 2018 – September 30, 2018
January 23, 2019	October 1, 2018 – November 30, 2018

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 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

¹⁹ (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.

²⁰ (U) The Section 702 querying procedures were applicable for only a portion of this joint assessment's reporting period. The query requirements for CIA that were in effect during that portion of this reporting period are contained in CIA's Section 702 querying procedures for the 2018 Certifications, which were posted on *IC on the Record* on October 8, 2019.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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]

[REDACTED] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [REDACTED]

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.²¹ 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) As noted above, NCTC previously played a more limited role in implementing Section 702, as reflected in the "Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended." During this reporting period, NCTC was authorized to receive unminimized Section 702 data and also had access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism. As part of the joint oversight of NCTC to ensure compliance with these procedures, NSD and ODNI conduct 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 2019.

(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 minimization and querying procedures.²² Unlike NSA, FBI, and CIA, NCTC does not directly 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

²¹ (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.

²² (U) NCTC's Section 702 querying procedures (dated September 2018 and effective with the FISC-approved 2018 certifications, in October 2018) were applicable for only a portion of this joint assessment's reporting period.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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 26, 2018	May 1, 2018 – June 30, 2018
September 20, 2018	July 1, 2018 – August 31, 2018
November 29, 2018	September 1, 2018 – October 31, 2018
January 31, 2019	November 1, 2018 – December 31, 2018

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.²³ 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.

²³ (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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) V. Inter-agency / Programmatic Oversight**

(U) Because the implementation and oversight of the Government's Section 702 authorities are a multi-agency effort, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence, and comply with all legal requirements. For those reasons, NSD and ODNI 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 or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review and, where appropriate, seek modifications of their targeting and minimization procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance. In particular, during this reporting period, NSD and ODNI focused on identifying the extent to which non-compliant queries were occurring across the FBI, and on identifying programmatic modifications to address the FBI's non-compliant queries. In subsequent reporting periods, NSD and ODNI worked with FBI to implement changes to its systems, as well.

(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 2016.²⁴ 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 websites²⁵ where personnel can obtain information about specific types of Section 702-related issues and compliance matters.

²⁴ (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, *OVSCI203: FISA Amendments Act Section 702* (Document 17, NSA's Training on FISA Amendments Act Section 702).

²⁵ (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*

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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.²⁶ NSD training at FBI field offices also included training on the reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications. As discussed above, this reporting requirement applies to queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a United States person that was reviewed by FBI personnel.

(U) 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 information. FBI conducted this training between November and December 2019. Current users who did not complete this training by mid-December 2019 would have had their access to unminimized Section 702 information temporarily suspended until they took the training.

(U) During this reporting period, CIA continued to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a required training program for anyone handling raw Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Furthermore, CIA has issued guidance to its personnel about how to properly conduct United States person queries that are reasonably likely to return foreign intelligence information.²⁷

Applications Training (Document 11), *NSA's 702 Training for NSA Adjudicators* (Document 12), and *NSA's 702 Adjudication Checklist* (Document 13).

²⁶ (U) This specific training began before, occurred during, and continued after the current reporting period of June 1, 2018, through November 30, 2018.

²⁷ (U) See *USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data*. As discussed in the previous Joint Assessment, 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."

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) During this reporting period, NCTC provided training on the NCTC Section 702 minimization and querying procedures to all of its personnel who will have access to raw Section 702-acquired information. NCTC uses a training tracking system through which NCTC can verify that its users have received the appropriate Section 702 training before being given access to raw Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed raw Section 702-acquired information in its system to confirm that those personnel who access raw Section 702-acquired information had received training on the NCTC Section 702 minimization 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.

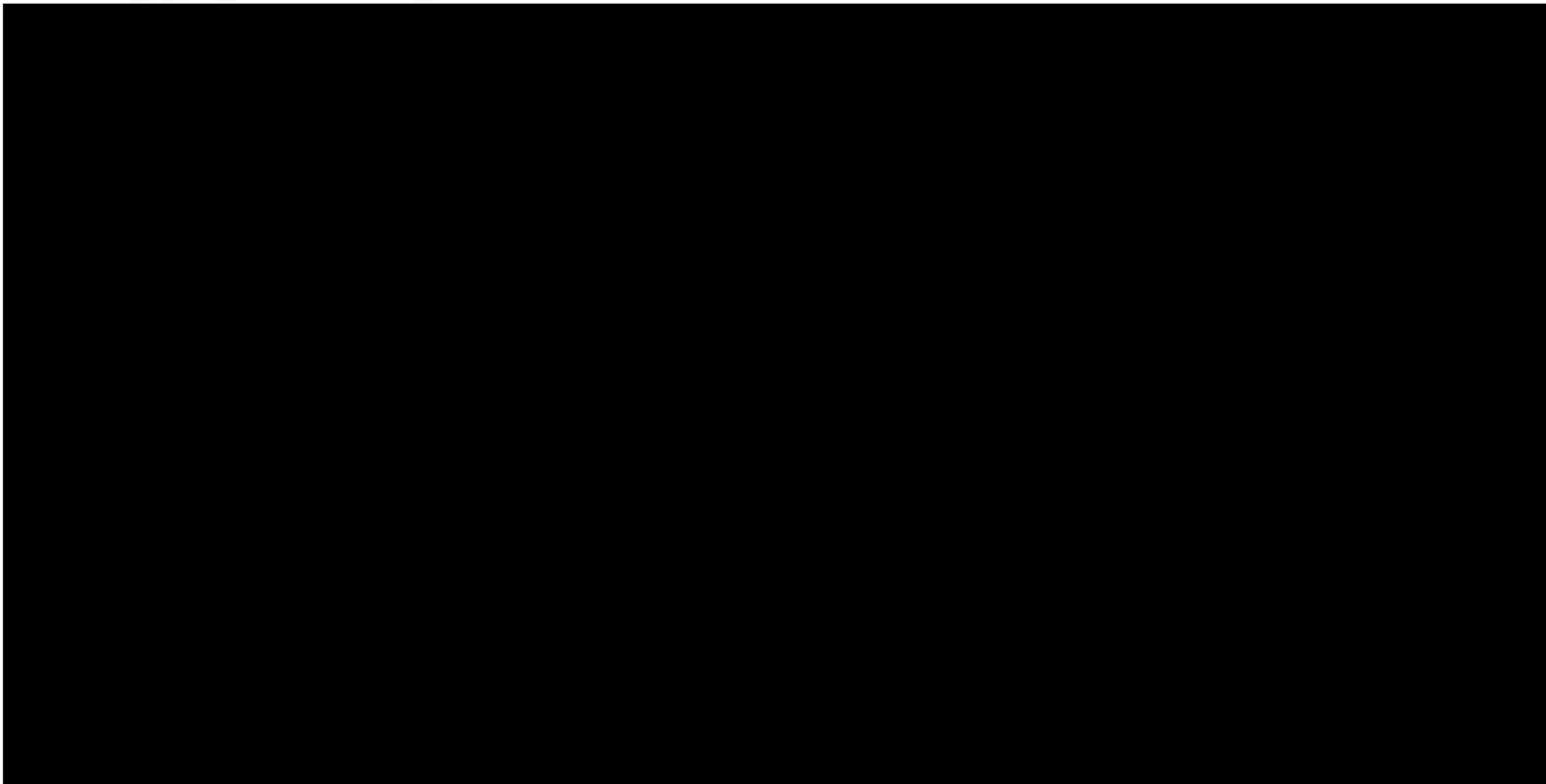
(U) I. Trends in NSA Targeting and Minimization

(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,²⁸ 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.²⁹

²⁸ (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 *CY2018 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*.

²⁹ (U) One of the reporting periods in which the total number of facilities under collection decreased occurred prior to 2010 and is not reflected in Figure 5.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) Figure 5: Average Number of Facilities under Collection**

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

~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [REDACTED] facilities³⁰ were under collection pursuant to the applicable certifications on any given day during the reporting period.³¹ This represents a 24.4% increase from the approximately [REDACTED] facilities under collection on any given day in the last reporting period. [REDACTED]

(U) The above statistics describe the *average* number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the

³⁰ ~~(TS//SI//NF)~~ Beginning in the previous reporting period, 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.

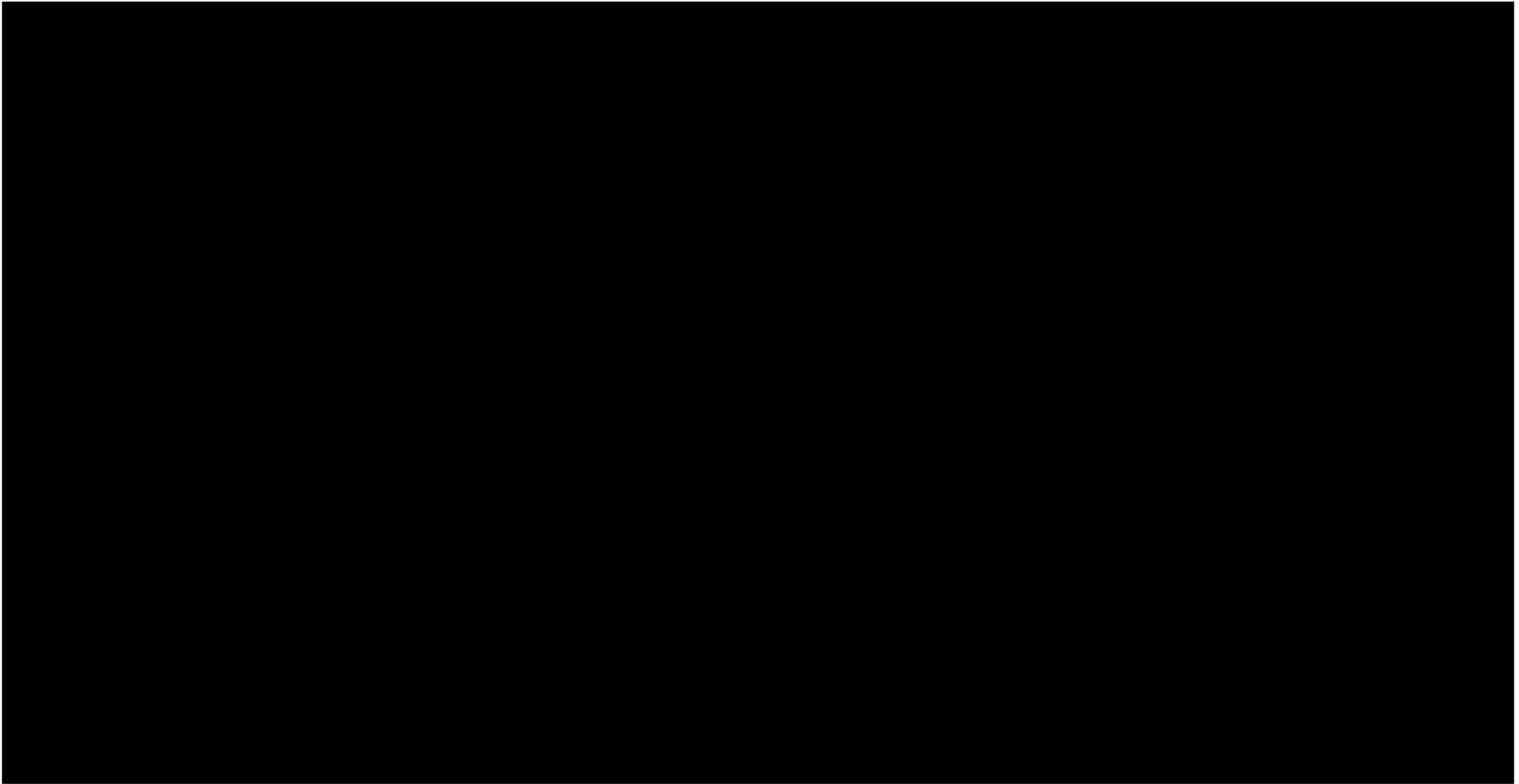
³¹ ~~(S//NF)~~ The applicable certifications for this reporting period were [REDACTED]. In prior reports the Government provided additional statistics, to include the average number of facilities under collection by certification and the average number of facilities delineated by telephony facilities and electronic communications accounts. Due to a technical issue, NSA was unable to determine these numbers for this reporting period.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

reporting period provides another useful metric.³² Classified Figure 6 charts the average monthly numbers of newly tasked facilities from 2013 through 2017 and the total monthly numbers of newly tasked facilities from January 2018 through November 2018.

(U) Figure 6: New Taskings by Month (Yearly Average for 2013 through 2017)



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

~~(S//SI//NF)~~ Specifically, NSA provided documentation of approximately [REDACTED] new taskings during the reporting period. This represents an 8.3% increase in new taskings from the previous reporting period. [REDACTED]

~~(S//SI//NF)~~ From December 2017 through May 2018, NSA tasked an average of approximately [REDACTED] telephony facilities per month. From June 2018 through November 2018, NSA tasked an average of approximately [REDACTED] telephony facilities per month. This represents a [REDACTED] increase in the average number of telephony facilities tasked each month, when compared to the previous six months.

³² (U) The term newly tasked facilities refers to any facility that was added to collection under a certification. This term includes any facility added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked facilities are facilities that had been previously tasked for collection, were detasked, and then retasked.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(S//SI//NF) From December 2017 through May 2018, NSA tasked an average [REDACTED] approximately [REDACTED] electronic communications accounts per month. From June 2018 through November 2018, NSA tasked an average of approximately [REDACTED] electronic communication accounts per month, a [REDACTED] increase from the prior six-month period.

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data and provided NSD and ODNI access to all reports NSA identified as containing United States person information.³³ 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.³⁴ The number of serialized reports NSA has identified as containing United States person information decreased, after increasing for the prior reporting period.

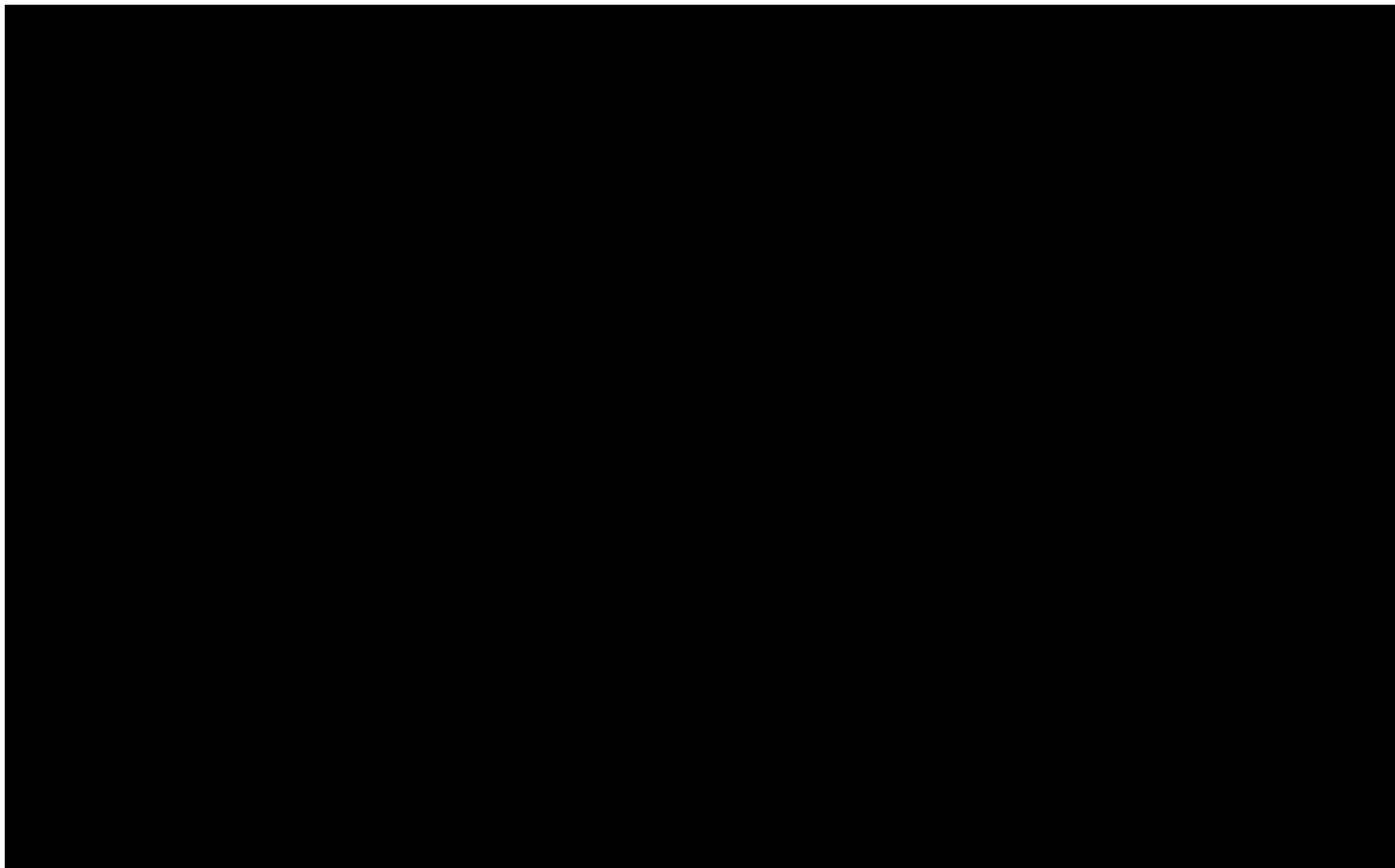
³³ (U) Previous joint assessments referred to those reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. Given that Section 702 of FISA replaced the PAA in 2008, the Government no longer disseminates minimized information that was previously acquired pursuant to 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.

³⁴ (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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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~~) Specifically, in this reporting period NSA identified to NSD and ODNI approximately [REDACTED] serialized reports based upon minimized Section 702-acquired data. This represents a 0.2% decrease from the approximately [REDACTED] serialized reports NSA identified in the prior reporting period. Figure 7 reflects NSA reporting over the last ten reporting periods; the number of reports identified by NSA decreased in only one other reporting period.

(~~S//NF~~) Figure 7 also shows the number of these serialized reports that NSA identified as containing United States person information. During this reporting period, NSA identified approximately [REDACTED] serialized reports as containing United States person information derived from Section 702-acquired data.³⁵ The percentage of reports containing United States person information

³⁵ (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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

was slightly lower this reporting period (7.6%) than the 8.9%, 7.3%, and 8.5% reported in the last three reporting periods.

(U) II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA-designated facilities that FBI approved.³⁶ As detailed below, the number of facilities designated for acquisition has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.³⁷

(U) As classified Figure 8 details, FBI approves the vast majority of NSA's designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA-designated facilities have already been evaluated and found to meet the NSA targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion³⁸ were rejected on the basis that they were ineligible for Section 702 collection.

(U) In 2013, the yearly average of designated facilities approved by FBI increased. The yearly average of designated facilities approved by FBI in 2014 slightly decreased, and then increased again in 2015, 2016, and 2017. The number of designated facilities approved by FBI each month this reporting period has varied. NSD and ODNI have continued to track the number of facilities approved by FBI will incorporate this information into future Joint Assessments.

36

37

38

~~TOP SECRET//SI//NOFORN/TISA~~

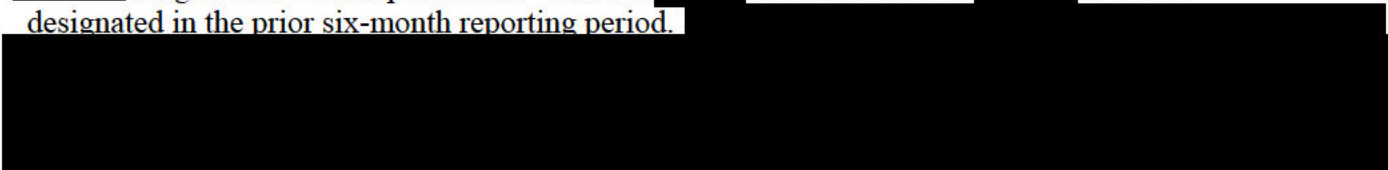
~~TOP SECRET//SI//NOFORN/TISA~~

(S//NF) Figure 8:



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

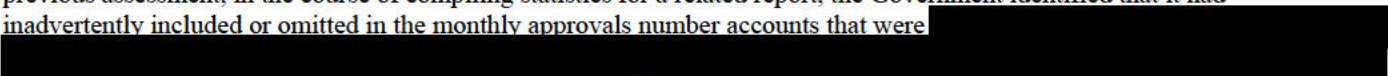
(S//SI//NF) Specifically, FBI reports that NSA designated approximately [REDACTED] accounts [REDACTED] during the reporting period – an average of approximately [REDACTED] designated accounts per month. This is a [REDACTED] increase from the [REDACTED] accounts designated in the prior six-month reporting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



(S//NF) FBI approved [REDACTED]³⁹ requests [REDACTED]



³⁹ (S//NF) Beginning with the previous joint assessment, the Government changed its counting methodology to ensure statistical accuracy for the number of designated accounts approved in a given reporting period. As explained in the previous assessment, in the course of compiling statistics for a related report, the Government identified that it had inadvertently included or omitted in the monthly approvals number accounts that were [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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 2013 – May 2014 through the current period of June 2018 through November 2018. 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, although it decreased 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)**

(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. This is a 22.1% decrease from the approximately [REDACTED] such disseminations CIA made in the prior reporting period. [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

[REDACTED] and as reported in prior Joint Assessments, CIA also permits some personnel [REDACTED]

[REDACTED] NSD reviews all [REDACTED] containing Section 702-acquired information that CIA has identified as potentially containing United States person information to ensure compliance with CIA's minimization procedures. ODNI reviews a sample of such cables.

(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.⁴⁰ 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. Beginning in the middle of the reporting period covered by the 13th Joint Assessment (June 2014 through November 2014), CIA began reporting the number of files CIA transferred to systems with broader access, instead of the number of files retained in systems of limited access, as the number of transferred files provides a more accurate portrayal of CIA's use of Section 702-acquired information. This current assessment reports the total number of files CIA transferred from June 2018 through November 2018. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below. 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.

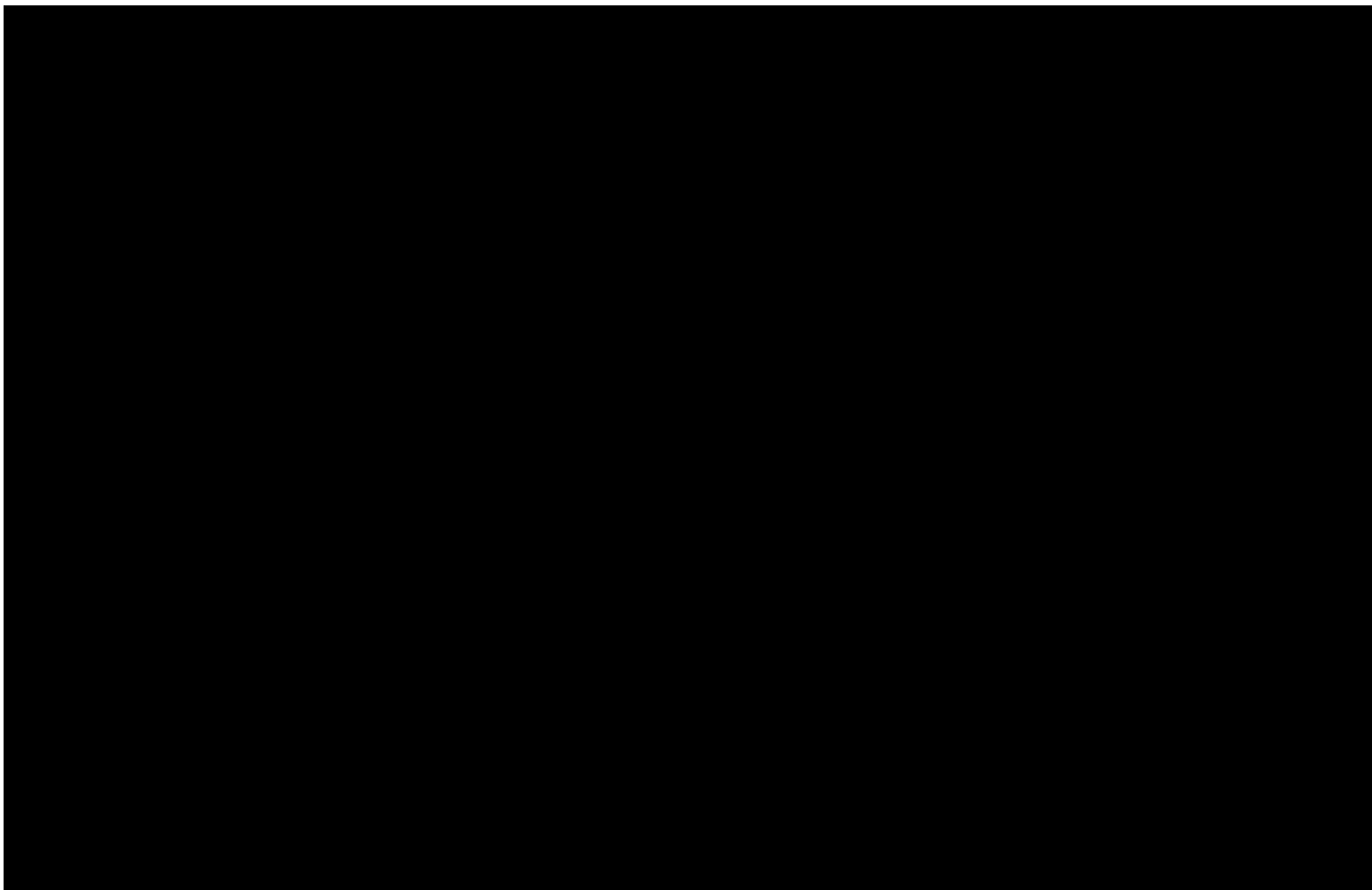
⁴⁰ (S//NF) [REDACTED]

[REDACTED] In making those retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) Figure 10: Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred which Contained Potential United States Person Information⁴¹



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

(~~S//NF~~) For this reporting period, CIA analysts transferred a total of approximately [REDACTED] (2.5%) of which were identified by CIA as containing a communication with potential United States person information. This is a 3.8% decrease in the number of files transferred or retained when compared with the previous reporting period when [REDACTED] (3.3%) of which contained potential United States person information.

(U) IV. Trends in NCTC Minimization

(U) Beginning with the reporting period covering June 2017 through November 2017, the Joint Assessment includes statistics regarding the total number of disseminations identified by NCTC as containing Section 702-acquired information. This number is classified and reported in

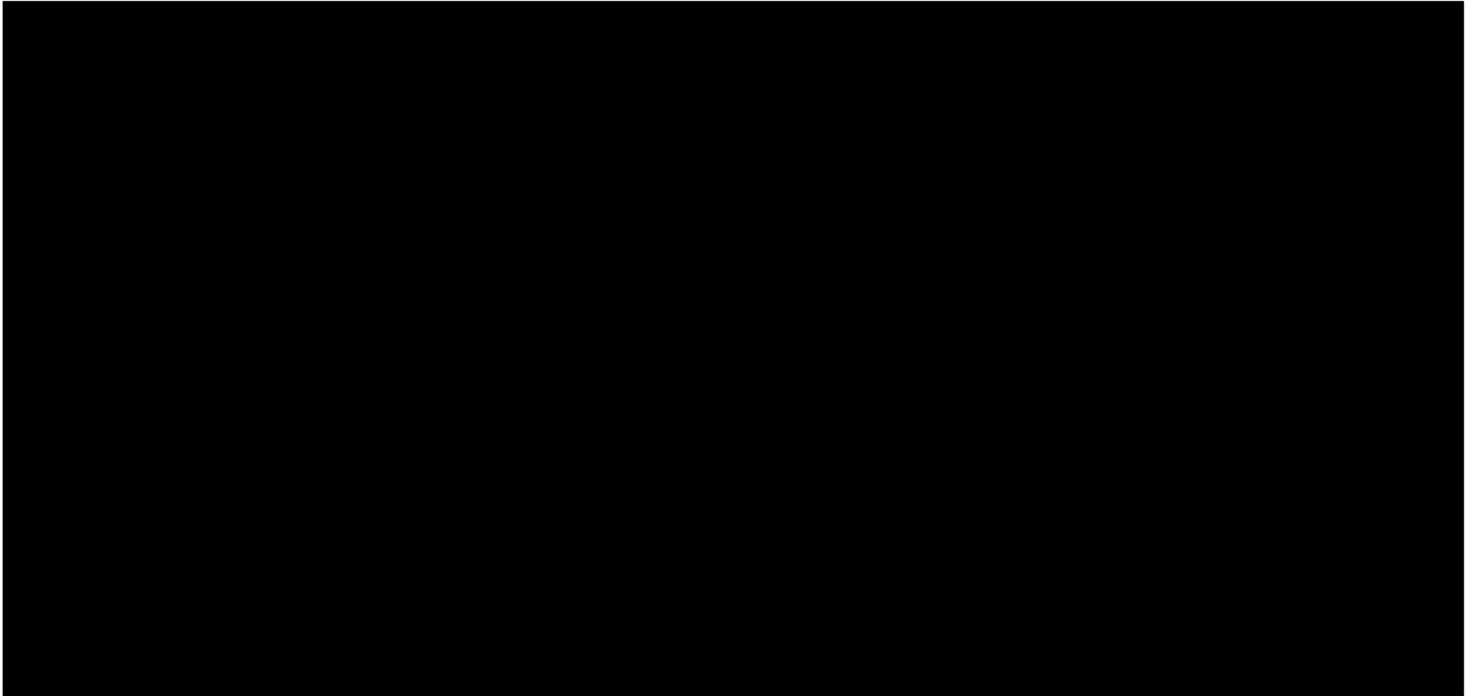
⁴¹ (U) CIA reviewed the numbers presented in this chart for previous joint assessments and identified that some of the numbers reported in previous joint assessments were incorrect. Those numbers have been updated accordingly.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

Figure 11. Because NCTC only began obtaining raw Section 702-acquired data after the FISC approval of such in April 2017, there are only three six-month periods to report in this assessment.⁴² The number of disseminations identified by NCTC increased substantially this reporting period, likely due to NCTC's overall increased use of the authority.

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



(U) Figure 11 is classified ~~SECRET//NOFORN~~.

(~~S//NF~~) During this reporting period, NCTC identified to NSD and ODNI approximately [REDACTED] disseminations containing Section 702-acquired data, regardless of whether they contained U.S. person information. This is an 817% increase over the approximately [REDACTED] disseminations made by NCTC in the prior reporting period. Of the [REDACTED] disseminations, NCTC provided [REDACTED] of these to NSD and ODNI for review. Starting with the January 31, 2019 review, which included November 2018 disseminations, NCTC began identifying for NSD and ODNI only disseminations containing United States person information. There were no such disseminations for the month of November.

⁴² (~~S//NF~~) The FISC's April 2017 opinion approved NCTC's 2016 minimization procedures allowing NCTC to obtain raw Section 702-acquired information. NCTC began receiving unminimized Section 702-acquired information on [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS**

(U) This assessment reports a large number of FBI compliance incidents related to querying, and, in particular, FBI's use of "batch queries," which significantly increased the number of incidents during the current reporting period.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) The 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 overall compliance incident rate increased significantly during this reporting period, in large part due to the high number of the FBI querying incidents.

(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.

(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

⁴³ (S//NF) The number of FBI minimization 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's [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 FBI 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; this opinion and other documents related to the 2019 Section 702 certifications were released on September 4, 2020, 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 comply with its querying procedures.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

querying requirements 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 increase in compliance incidents during this reporting period. The joint oversight team expects that the remedial measures undertaken by FBI will allow it to better implement its querying procedures and follow the guidelines in such a manner.

(U) Although the overall compliance incident rate during this reporting period, expressed as a percentage of overall collection activity, increased significantly, when the FBI's single largest querying incident is excluded, the overall compliance incident rate is generally consistent with the rates reported in previous periods.

(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 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) 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 and minimization procedures, for a total of [REDACTED] incidents involving NSA or FBI procedures.⁴⁶ In addition, during this reporting period, there were [REDACTED]

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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

incidents of noncompliance with CIA's minimization procedures. There were [REDACTED] incidents of noncompliance with NCTC's minimization and querying procedures. Furthermore, there was one incident in which another federal agency (U.S. Customs and Border Protection) issued and disseminated certain reports that contained minimized information acquired pursuant to Section 702 but did not include the accompanying caveat required by Section 106(b) of FISA. In addition, there were [REDACTED] identified instances 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 day⁴⁷ during the reporting period.

(U) Figure 12: Overall Compliance Incident Rate

SECRET [REDACTED]	
(U) All compliance incidents during reporting period (June 1, 2018 – November 30, 2018)	[REDACTED]
(U) Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
(U) Overall compliance incident rate: number of incidents divided by average number of facilities subject to acquisition	(U) 33.54%
SECRET [REDACTED]	

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

(U) The 33.54% overall compliance incident rate represents an increase from the 4.39% overall compliance incident rate in the prior reporting period. As with the previous overall compliance incident rate,⁴⁸ the current reporting period's overall compliance incident rate was predominantly driven by FBI personnel misunderstanding the query standard in its minimization procedures. The misunderstanding by FBI personnel caused over a hundred thousand non-

⁴⁷ [REDACTED]

⁴⁸ (U) As explained in the previous joint assessment, the 4.39% compliance incident rate was primarily driven by: (1) one NSA office misunderstanding how one of NSA's tasking tools worked and thus not appropriately reviewing multiple facilities prior to tasking, which resulted in numerous facilities being incorrectly tasked; and (2) FBI personnel misunderstanding the query standard in its minimization procedures, which resulted in thousands of non-compliant queries.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

compliant queries – almost all of which pertained to a single event. These incidents – including the remedies – are discussed in detail below. The joint oversight team conducted an analysis of the overall compliance incident rate and determined that nearly all of the increase in the rate was driven by the significant rise in the number of FBI query errors; other types of compliance incidents included in the overall compliance incident rate were generally in line with the historical low rates and did not drive the increase in the rate to the extent that FBI query errors did. 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) The number of notification delays substantially decreased during this reporting period. 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 33.52%. The comparable incident rate in the previous reporting period was 4.32%; in all preceding reporting periods the comparable incident rate was less than 1%. 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) When excluding FBI querying incidents, the overall compliance incident rate – with and without the notification delay incidents – remained low, which the joint oversight team assesses 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. The joint oversight team has continued to identify a significant number (though substantially lower than in this reporting period) of non-compliant FBI queries in subsequent reporting periods. The joint oversight team continues to work with FBI to reduce the number of these non-compliant queries and improve training and guidance regarding the conduct of queries in FISA-acquired data.

(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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

in the numerator do not have 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 number of average *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 number of average *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) The imperfections in the overall compliance incident rate 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). Accordingly, readers should understand that the 33.54% 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 14 and 15). The joint assessment team has also decided that, because FBI query errors comprise 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 19).

(U) Separating the targeting errors from the minimization 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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) B. NSA's Compliance Incidents: Categories and Number of Incidents**

(U) As has been true historically, most of the compliance incidents occurring during this reporting period – excluding the FBI querying incidents – involved non-compliance with the NSA's targeting or minimization procedures. This largely reflects the centrality of NSA's targeting and minimization efforts in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting or minimization procedures have generally fallen into the 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 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 or with NSA's minimization procedures and account for those incidents accordingly.

(U) While the above categories specifically pertain to NSA incidents, the FBI's targeting incidents categories and all agencies' minimization incidents categories generally align to those

⁴⁹ (U) As explained above, 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.

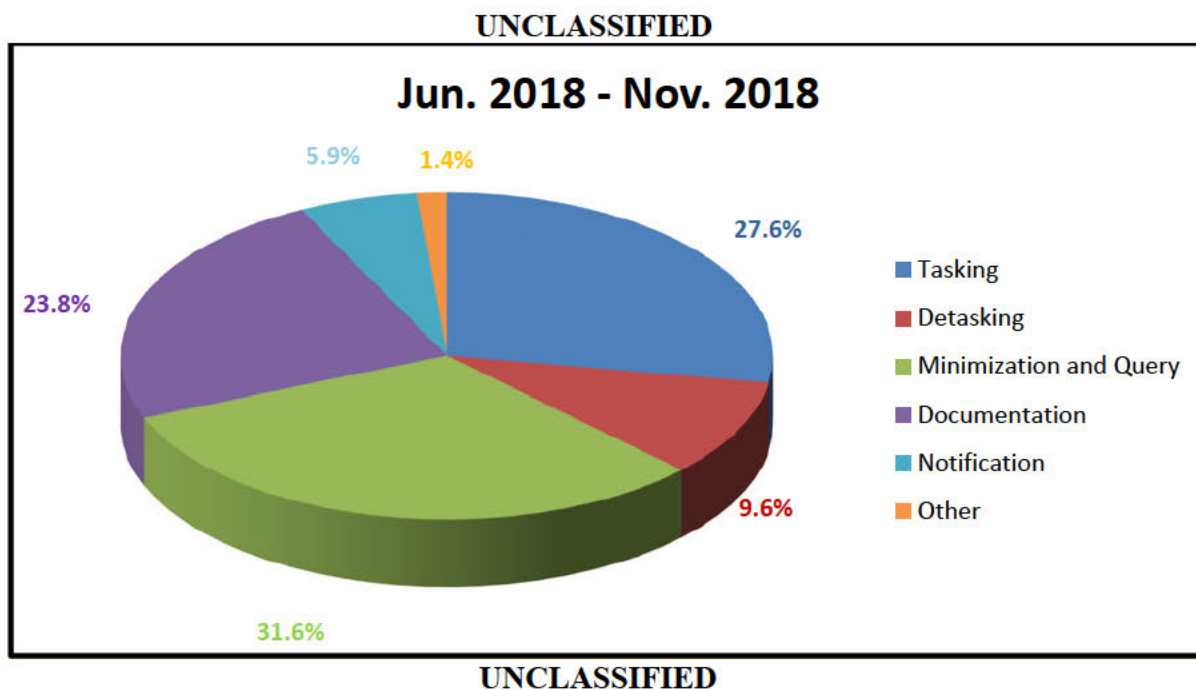
~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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.

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

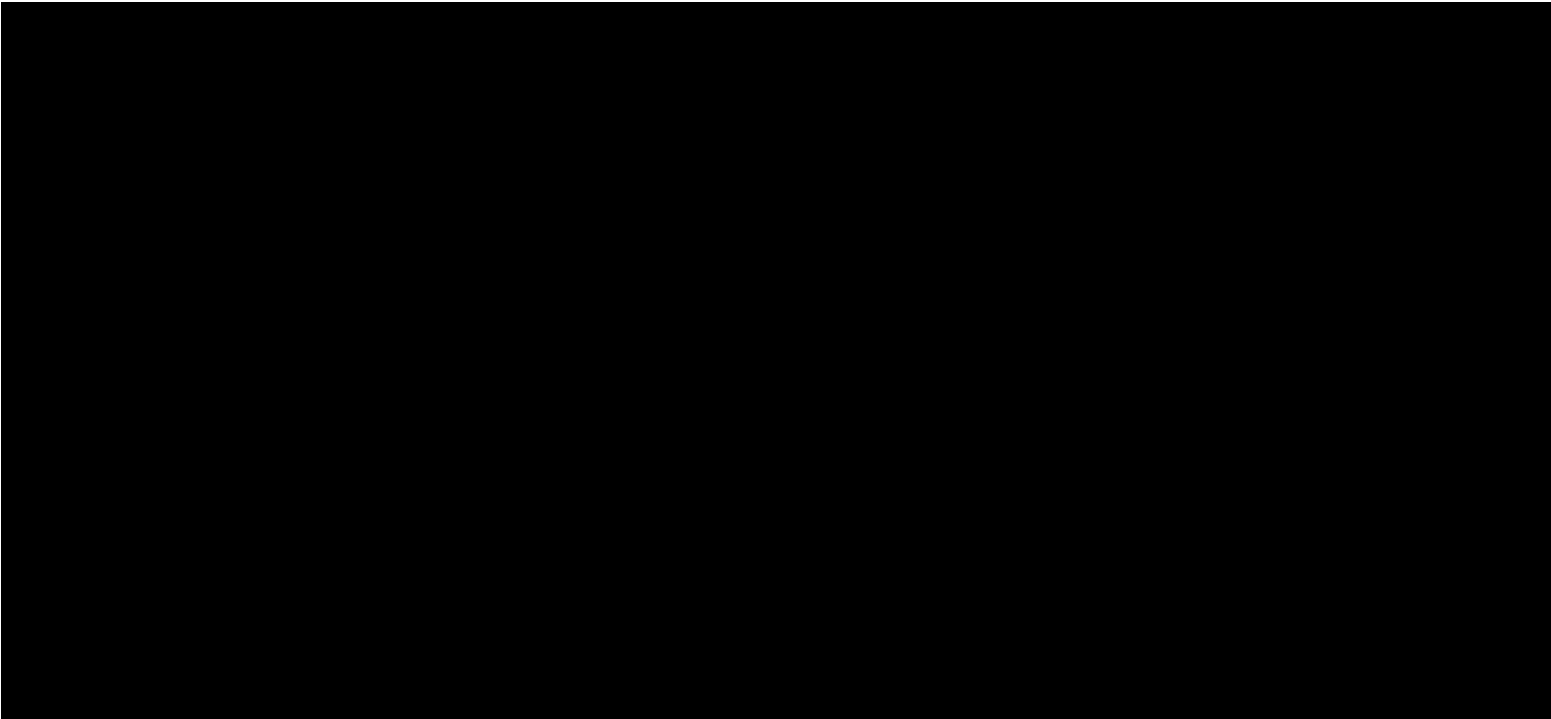


(U) Figure 13A is UNCLASSIFIED

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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



(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 then documentation errors account for the second and third largest percentage of incidents, respectively, followed by detasking delays. 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] [REDACTED] detasking incidents increased from [REDACTED] minimization and querying incidents increased from [REDACTED] documentation incidents increased from [REDACTED] [REDACTED] and “other” category incidents increased from [REDACTED] The number of notification delays decreased 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 14 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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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.

(U) **Figure 14: NSA Targeting Compliance Incident Rate**

SECRET	
(U) NSA compliance incidents relating to NSA’s targeting procedures, during reporting period (June 1, 2018 – November 30, 2018)	
(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) 0.20%

~~SECRET~~

(U) Figure 14 is classified ~~SECRET~~

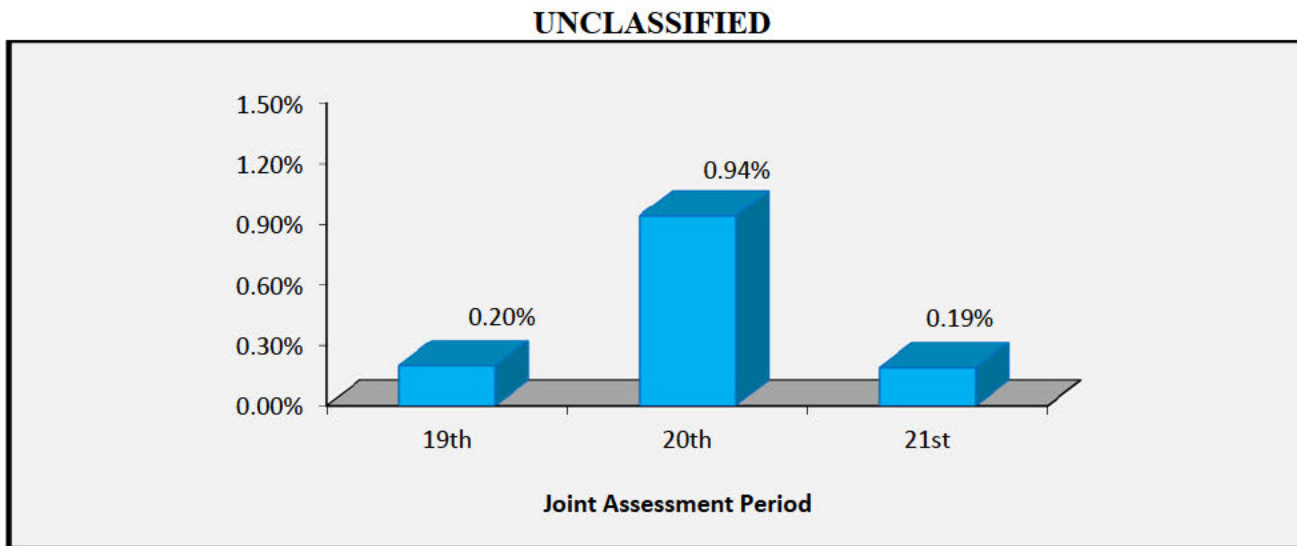
(U) This NSA targeting compliance incident rate percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Also, a single action may result in numerous incidents that have 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 and the subsequent explanation above concerning notification delay incidents, the joint oversight team determined that excluding NSA’s notification delays incidents from the NSA’s targeting compliance incident rate provides another measure. Thus, Figure 15 shows that adjusted NSA targeting compliance incident rate of 0.19%, not including notification delay errors (as compared to 0.20% of NSA targeting compliance incident rate, including notification errors). As described in the previous Joint Assessment, the increase from 0.20% in the 19th reporting period to 0.94% in the prior 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 generally consistent with the rate during the 19th Joint Assessment period.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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**

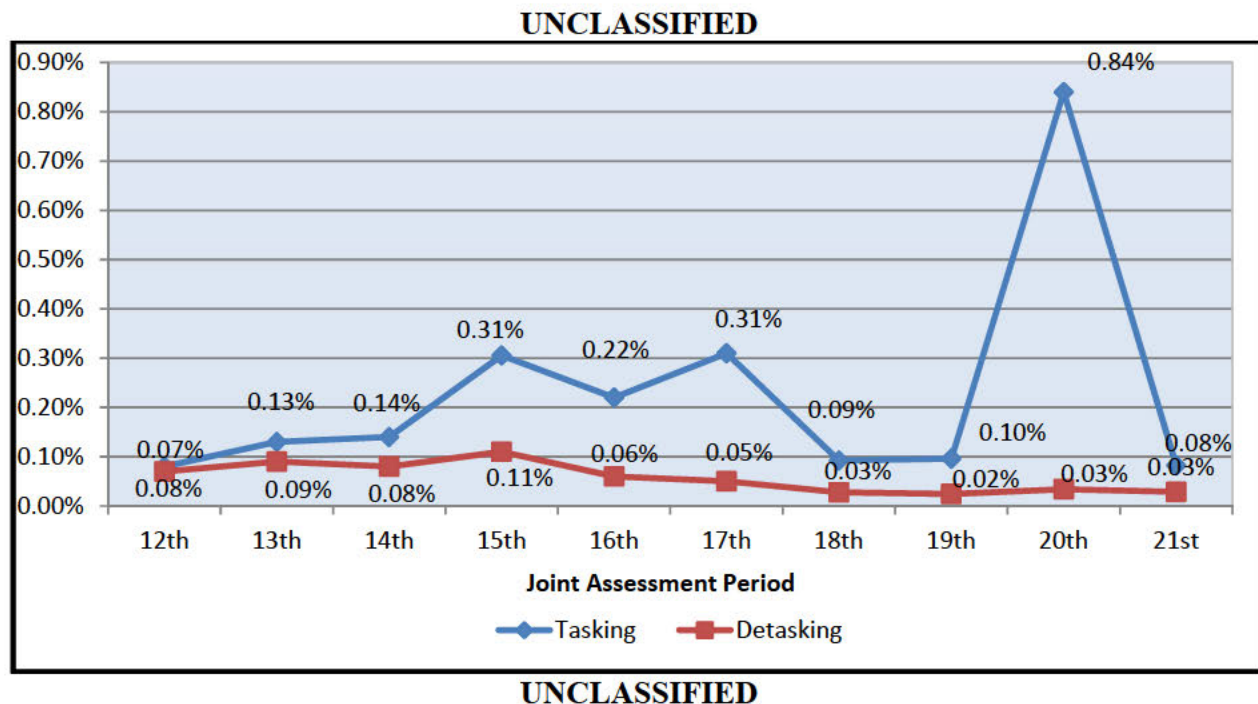


UNCLASSIFIED

(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).

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) Figure 16: Tasking and Detasking Incident Compliance Rates**

(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.⁵⁰ The tasking incident rate noticeably decreased to 0.08% during this reporting period from 0.84% in the previous period. As previously noted, the increase in the tasking incident rate during the prior period was primarily due 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.

⁵⁰ (U) Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. Detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) C. FBI: Number of Compliance Incidents**

(U) The total number of compliance incidents identified relating to FBI's targeting procedures decreased as compared to the last period. However, the number of errors relating to FBI's minimization procedures increased significantly to over 100,000 – almost entirely due to a single event relating to improper queries.⁵¹ These non-compliant queries were conducted by a limited number of personnel, and the vast majority were conducted as part of a batch query function in a FBI system.⁵²

(U) Classified Figure 17 shows the classified number of incidents for the last ten reporting periods (*i.e.*, from the 12th through the 21st reporting periods). With the exception of the 19th through the 21st reporting periods, the number of FBI's identified targeting and minimization errors remained consistently low. The joint assessment team assesses that the increase in FBI errors beginning in the 20th reporting period is attributable to NSD's increased focus on reviewing FBI querying practices, including as a result of NSD's increased experience in the evaluation of FBI queries and its increased knowledge of the FBI systems storing Section 702-acquired information. When combined with the particular sample population of FBI users in the reviews NSD conducted, these factors 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 that substantially increased during this reporting period, the joint oversight team 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.

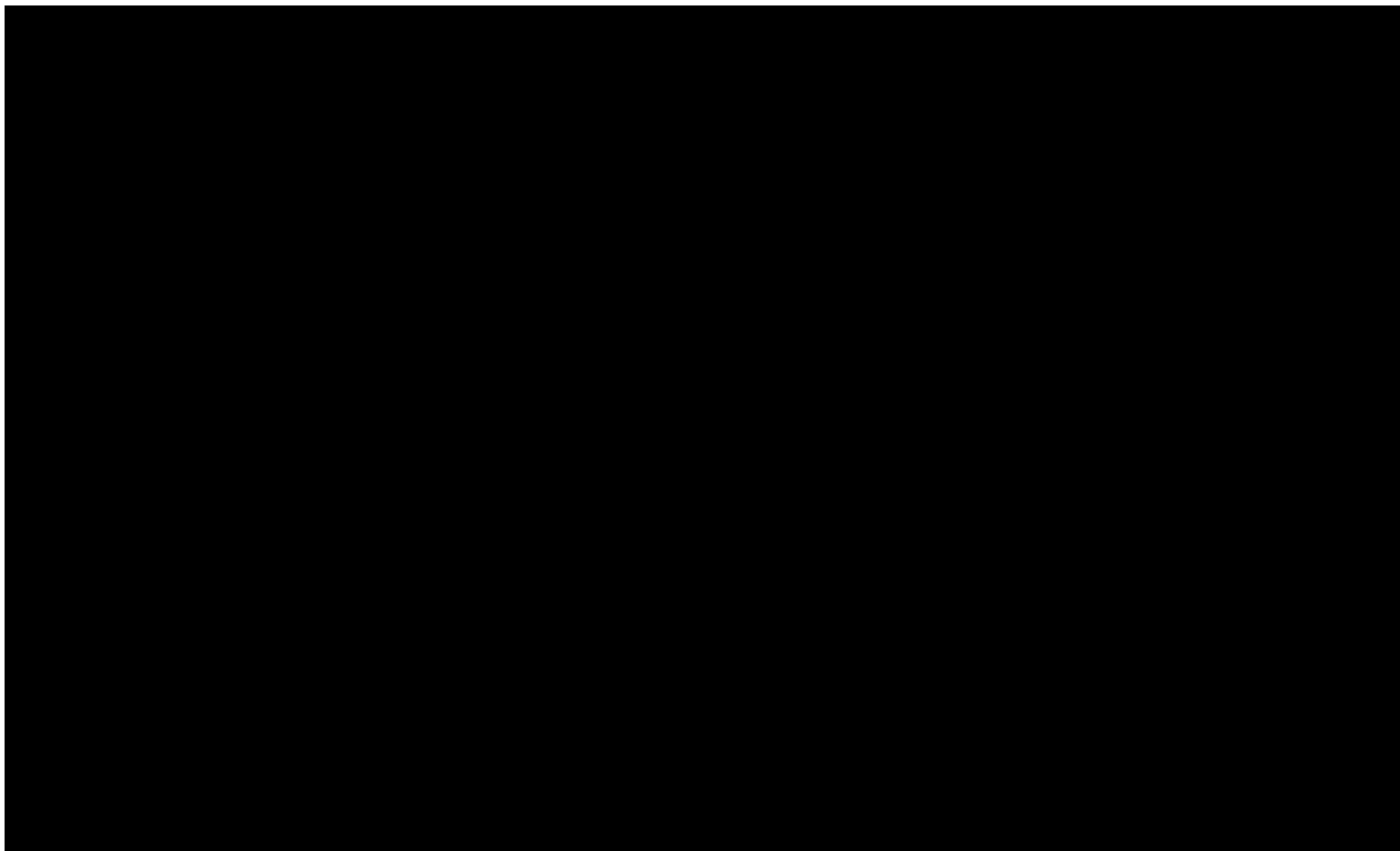
⁵¹ (S//NF) Specifically, in the 21st reporting period, [REDACTED] incidents of non-compliance with the FBI targeting or minimization procedures were identified. The vast majority of these incidents pertain to non-compliant queries, and in particular, two non-compliant query incidents comprise nearly the entire [REDACTED] incidents.

⁵² (S//NF) The FBI system, in which the non-compliant batch queries were conducted, was FBI's [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) Figure 17: Number of Compliance Incidents Involving the FBI Targeting, Querying, 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. During this reporting period, the FBI targeting compliance incident rate was 0.003%. 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 assessment 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

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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.⁵³

(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, 2018 – November 30, 2018)	
(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 ⁵⁴	
(U) FBI query compliance incident rate: number of query incidents reported, divided by number of queries audited	(U) 23.94%

~~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 raw (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. In addition, the accuracy of this metric is dependent on FBI providing NSD with accurate logs regarding the queries conducted during the relevant sample period. 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

⁵³ (U) Note that combining the NSA targeting incident rate and the FBI query error rate will not average out to the overall compliance incident rate because, among other things, each rate is calculated using different denominators.

⁵⁴ (U) This number also includes the number of FBI queries audited by NSD in connection with field office reviews completed by NSD during this reporting period and for which no FBI query compliance incidents were discovered.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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 during a given reporting period may, accordingly, 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 17, 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) Although each of the metrics in Classified Figure 17 and Classified Figure 18 has limitations, the joint assessment 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 procedures,⁵⁵ which is a slight increase from the zero 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.⁵⁶ The joint oversight team assesses that NCTC's 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 errors that involved CIA for the last ten reporting periods and NCTC for reporting periods beginning with the 19th assessment period. These numbers have generally remained 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.

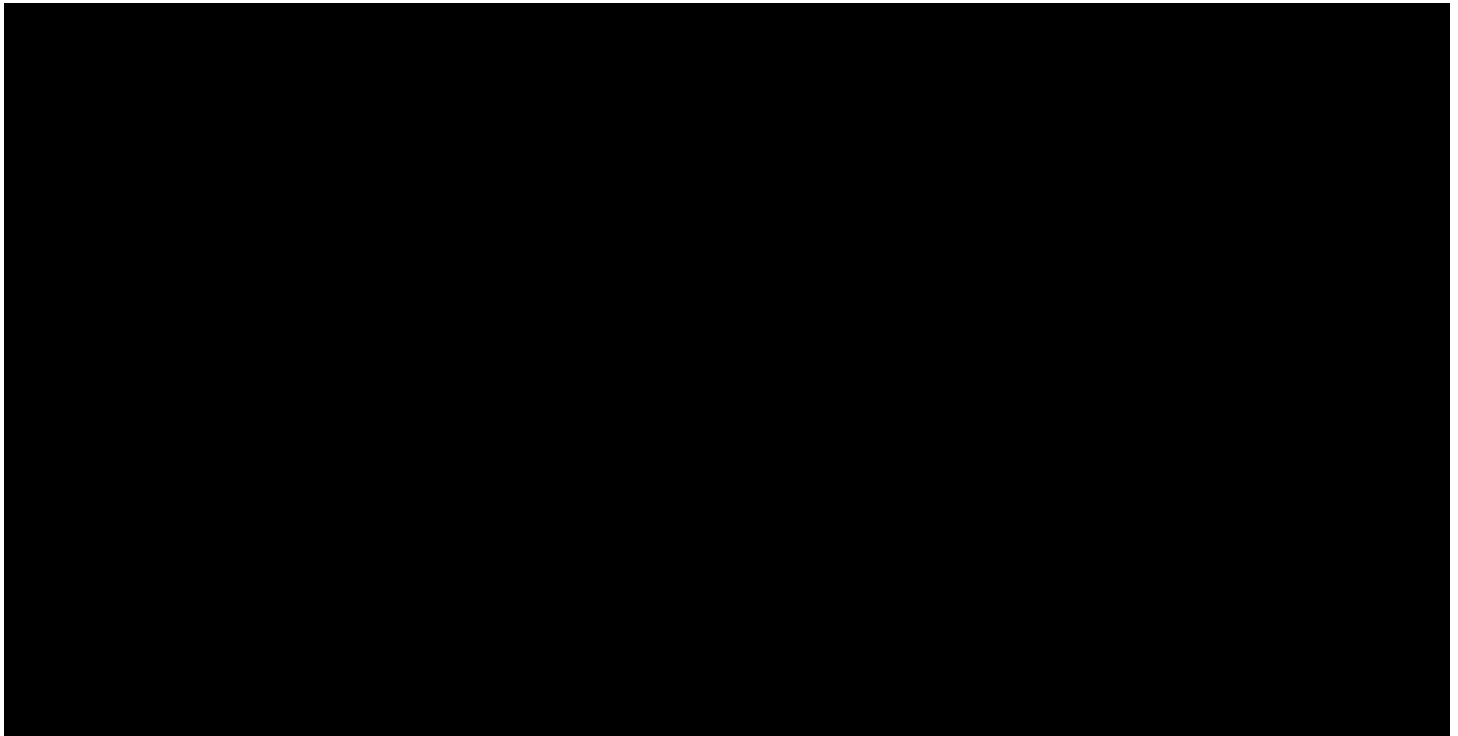
⁵⁵ (U) Recall that CIA does not have targeting procedures and may not target. Because CIA only has minimization procedures (and, after October 2018, querying procedures), errors can only occur as it pertains to its minimization and querying procedures.

⁵⁶ (U) Recall that NCTC does not have targeting procedures and may not target. Because NCTC only has minimization procedures (and, after October 2018, querying procedures), errors can only occur as it pertains to its minimization and querying procedures.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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

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

(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 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. Most of those incidents did not involve United States persons, and instead involved matters such as typographical

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. A small number of incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-compliance with NSA's minimization procedures and querying procedures involving the unintentional improper dissemination, retention, or querying of Section 702-acquired information.

(U) 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 FISC and to Congress; and all incidents are required to be appropriately remedied. For example, the joint oversight team identified compliance incidents where the non-United States person target was not reasonably expected to possess, receive, or likely communicate foreign intelligence information concerning a foreign power or foreign territory as defined in 50 U.S.C. § 1801(e). The accounts used by those users were detasked, and the relevant personnel were reminded of the Section 702 tasking requirements. 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) The Section 707 Report provides further details regarding each individual incident and information on applicable remedial and mitigating actions. 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 NSA compliance incident rate for this reporting period, excluding FBI, CIA, and NCTC compliance incidents, is 0.30%⁵⁷ and represents a decrease from the compliance incident rate of 1.06% in the previous reporting period.

(U) In the subsections that follow,⁵⁸ 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 communication issues and human errors. The joint oversight team believes that analyzing the trends of these incidents, especially in regards to their causes, help the agencies focus resources, avoid future incidents, and improve overall compliance.

⁵⁷ (U) The overall compliance incident rate (accounting for all four agencies) for this reporting period is 33.54%.

⁵⁸ (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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) A. The Impact of Compliance Incidents on United States Persons**

(U) A primary concern of the joint assessment team is the impact of certain compliance incidents on United States persons. The Section 707 Report discusses every incident of noncompliance with the targeting and minimization procedures, including any necessary purges resulting from these incidents. Most of these incidents did not involve United States persons, and instead involved matters such as typographical errors in tasking that resulted in no collection, detasking delays with respect to facilities used by non-United States persons who had entered the United States, or the unintentional improper dissemination, retention, or querying of Section 702-acquired information.

(U) Some incidents, however, did involve United States persons during the recent reporting period. As noted above, both the tasking compliance incident rate and detasking compliance incident rate involving facilities used by United States persons was close to zero during this reporting period. For tasking and detasking incidents, United States persons were primarily impacted by (1) tasking errors that led to the tasking of facilities used by United States persons, and (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person. United States persons were also impacted by minimization and querying 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 United States person information was handled through various purge, recall, and deletion processes.

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

(U) Only approximately 2% of the total number of NSA tasking errors identified during this reporting period involved instances where facilities used by United States persons were tasked pursuant to Section 702. These incidents represent isolated instances of insufficient due diligence and did not involve an intentional effort to target a United States person.

(U) All of the tasking errors in this reporting period impacting United States persons involved the tasking of facilities where the Government knew or should have known that at least one user of the facility was a United States person.⁵⁹ These tasking errors involved various errors by targeting analysts, including typographical or similar errors, and erroneously determining that a tasked account was used by the intended target.⁶⁰ In these incidents, personnel were reminded of the Section 702 tasking requirement, any applicable collection was purged, and no reporting was identified based on the collection.

59


60

~~TOP SECRET//SI//NOFORN/TISA~~

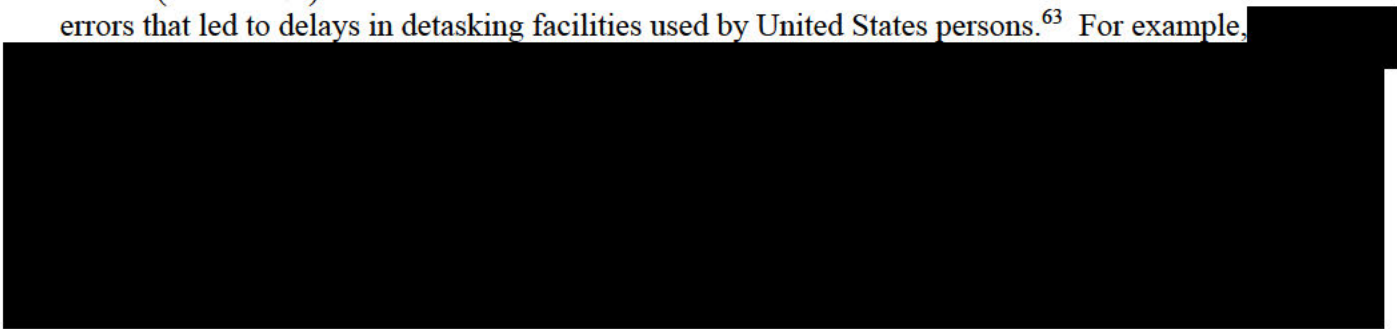
~~TOP SECRET//SI//NOFORN/TISA~~*(U) (2) Delays in Detasking Impacting United States Persons*

(U) The majority of the detasking incidents involved (i) non-United States persons who either traveled to the United States or appeared to have traveled to the United States or (ii) an unexplained indication of an account that appeared to have been accessed from within the United States. Only 9.7% of the total number of detasking delays involved facilities used by a United States person. As discussed in further detail below, the detasking delay incidents impacting United States persons in this reporting period were caused by human errors (e.g., misunderstandings of the detasking requirements or analysts' overlooking information that should have led them detask accounts used by United States persons). In these incidents, the relevant personnel were reminded of the Section 702 detasking requirements.

(TS//SI//NF) Of the detasking delays involving facilities used by United States persons,⁶¹ incidents involved a misunderstanding of the detasking requirements. For example,



(TS//SI//NF) Other incidents were the result of overlooked information or other similar errors that led to delays in detasking facilities used by United States persons.⁶³ For example,

**(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. As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established processes

61

62

63

64

65

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated, such as typographical errors discussed below. Other human errors, such as those resulting from misunderstanding the rules and procedures, can be mitigated with additional training and guidance.

(U) (1) Tasking and Detasking Errors

(U) Training and guidance can mitigate the risk of certain tasking and detasking errors resulting from personnel misunderstanding the rules and procedures. During this reporting period, multiple incidents resulted from personnel not fully understanding certain aspects of the targeting procedures governing the tasking and detasking of facilities.

(U) First, there were tasking incidents in which NSA did not properly establish a sufficient basis to assess that the target was located outside the United States – otherwise referred to as the “foreignness determination.” In some cases, comprising approximately 3%⁶⁶ of the tasking errors during this reporting period, these incidents occurred because the analyst did not conduct a necessary foreignness check or because there was too long of a delay between the necessary foreignness checks and the actual tasking of the facility. This is in line with the previous assessment, which reported that such tasking errors accounted for 2% of all tasking errors. In all of these incidents, there is no indication that the facilities were used by a United States person or by someone in the United States.

(U) In addition, approximately 15% of the tasking errors during this reporting period were the result of insufficient foreignness determinations that were not the result of an analyst failing to conduct a necessary foreignness check.⁶⁷ In some of these incidents, NSA did not sufficiently address conflicting information that called into question whether a target was located outside the United States. For example, in one instance, NSA tasked a target’s facility while it was still investigating information indicating that the target might be in the United States.⁶⁸ Additionally, a small number of these tasking errors occurred because NSA personnel did not understand the targeting procedures and approved inappropriate taskings.⁶⁹

66

67

68

69

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) Second, there were tasking errors related to NSA's failure to establish a valid "foreign intelligence information purpose" (*i.e.*, that the targeted user is reasonably expected to possess, receive, and/or 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 certifications.⁷⁰ In approximately 15% of tasking errors (an increase from the previous reporting period, which reported 4% of these tasking errors, but in line with the 19th Joint Assessment, which also reported 15% of these tasking errors),⁷¹ NSA did not have a sufficient basis to assess that the user of the tasked facility would be reasonably expected to possess, receive, or likely communicate foreign intelligence information related to a specific group listed in Exhibit F of a particular certification.⁷² In those instances, at the time of tasking, NSA had sufficiently established that the users were non-United States persons located outside the United States. Although NSA intended to acquire foreign intelligence information related to a specific Exhibit F group, NSD and ODNI determined that there was not a reasonable basis to assess that tasking the facility would result in the acquisition of foreign intelligence information related to a specific group listed in Exhibit F.

(U) Approximately 15% of tasking errors during this reporting period were the result of an incorrect application of NSA's administrative processes for tasking facilities that resulted in a previously facility being retasked without fully applying NSA's Section 702 targeting procedures.⁷³ The majority of these tasking errors were discovered when NSA conducted an internal review. NSA determined that its adjudicators mistakenly believed that they were making administrative updates to the tasking records for each facility instead of approving new taskings, and, accordingly, they did not properly apply the targeting procedures. Additionally, NSA's investigation revealed that the adjudicators were incorrectly using one of NSA's tools to verify foreignness.

⁷⁰ (U) As detailed in the Appendix, NSA analysts must provide a written explanation for each tasking request establishing a link between the targeted user and the foreign intelligence purpose covered by the certification under which the targeted user's facility is being tasked. Errors resulting from incorrect documentation are discussed later in this assessment.

⁷¹ ~~(TS//SI//NF)~~ [REDACTED] he majority of these incidents were discovered through NSD and ODNI's bi-monthly reviews of all newly tasked Section 702 selectors [REDACTED] involved taskings in which the analysts had indicated that the user of the facility possessed, was expected to receive, and/or was likely to communicate foreign intelligence information based on the fact that [REDACTED]

⁷² [REDACTED]

⁷³ [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(S//NF) Additionally, approximately 3% of tasking errors occurred because NSA established the foreignness of a facility based on the fact that [REDACTED]

[REDACTED] ⁷⁴ However a [REDACTED] and [REDACTED] not conclusively demonstrate that [REDACTED] in these instances, NSA did not have additional information to establish that [REDACTED] [REDACTED] used by individuals who may be properly targeted for collection pursuant to Section 702.

(U) Finally, there were detasking delays that occurred because personnel at NSA, FBI, and CIA did not understand certain rules and procedures regarding when facilities need to be detasked. Specifically, approximately 23% of detasking delays occurred as a result of misunderstandings.⁷⁵ As with other compliance incidents, any data acquired as a result of such tasking and detasking errors is required to be purged.

(U//FOUO) Typographical and Similar Inadvertent Errors: Despite multiple pre-tasking checks, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors and similar accounted for approximately 34% of the tasking errors made in this reporting period, which is an increase from the previous reporting period, in which typographical and similar errors accounted for 3% of the tasking errors.⁷⁶ The majority of these typographical or similar errors were caused by a specific type of error.⁷⁷ Subsequent to the reporting period, and after discussing these incidents with NSD, 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 approximately April 2019 and in September 2019, NSA implemented technical solutions [REDACTED]

(U) Additionally, approximately 19% of the detasking delays from this reporting period were the result of others inadvertent errors, such as an NSA analyst inadvertently detasking some, but not all, of a target's facilities that required detasking.⁷⁸ Some of these detasking delays were the result of personnel attempting to detask a target's remaining facilities but failing to complete the

74

75

76

77

78

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

process. Approximately 9% of detasking delaying from this reporting period involved indications of upcoming travel to the United States by non-United States persons, where the relevant personnel inadvertently failed to detask the target's facilities prior to arrival.⁷⁹ As with other compliance incidents, any data acquired as a result of such tasking and detasking errors is required to be purged.

(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 raw Section 702-acquired information may be *retained*. NSA's querying procedures (and NSA's minimization procedures in effect during a portion of this period) also have various requirements, including rules regarding *querying* raw Section 702-acquired information. Whenever possible, all erroneous query results were deleted, disseminated reports were recalled, and collection purged. Relevant personnel were reminded of the Section 702 query, dissemination, and retention requirements, as appropriate. Particular issues of non-compliance with minimization procedures are detailed below.

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

- 1) NSA's Section 702 querying procedures require that queries of raw Section 702 collection *must be designed in a manner "reasonably likely to return foreign intelligence information."* For instance, if a query does not meet this standard due to a typographical or comparable error in the construction of the query term,⁸⁰ it constituted a compliance incident, regardless of whether the query term used a non-United States person identifier or a United States person identifier. The same requirement was included in NSA's Section 702 minimization procedures that were in effect at the beginning of the reporting period.
- 2) Although NSA's Section 702 querying procedures permit queries of raw 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. NSA's Section 702 minimization procedures that were in effect at the beginning of the reporting period similarly required such queries to be approved in accordance with NSA's internal procedures.⁸¹

79

⁸⁰ (U) For example, this type of query error can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overly broad results as a result of the query. As another example, a non-compliant query can be caused when an analyst makes a typographical error in a query term, thereby querying an account identifier that does not exist and thus is unlikely to return foreign intelligence information.

⁸¹ (U) Prior to April 2017, joint assessments discussed a third restriction pertaining to upstream collection. In April 2017, NSA ceased collecting "abouts" communications in Section 702 "upstream" internet surveillance. Instead, NSA limited such collection to internet communications that are sent directly to or from a foreign target. See NSA's public

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) Compared with the previous reporting period, the overall NSA minimization and querying incident rate significantly increased from 5% during the previous reporting period to 31.6% during this reporting period.⁸² The significant increase in minimization and querying incidents over the previous reporting period was almost entirely accounted for by the increase in improper queries, and was almost entirely due to one event involving multiple queries.

(U) As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization procedures. During this reporting period, out of all of NSA's total minimization and querying errors, approximately 88.9% involved improper queries,⁸³ of which:

- Approximately 64% of the minimization and querying errors involved NSA analysts conducting queries using a United States person identifier without approval as required by NSA's internal procedures; and⁸⁴
- Approximately 25% of the minimization and querying errors involved queries that were unlikely to return foreign intelligence information.⁸⁵

When an NSA analyst conducts an improper United States person query or an otherwise non-compliant query, NSA reminds the relevant personnel of the query requirements. As in previous reporting periods, there were no NSA incidents of an analyst intentionally running improper queries.

(U) One example of a query that was unlikely to return foreign intelligence information involved an analyst omitting a parenthesis from the query term. Another example of a query incident involved an analyst who conducted a United States person query in Section 702 collection, but, due to a misunderstanding, failed to obtain pre-approval for the query. When an NSA analyst conducts an improper query, NSA reminds the relevant personnel of the query requirements.

(U) Dissemination rules: NSA's minimization procedures also set forth requirements for the dissemination of United States person information. In the current reporting period, incidents involving NSA's disseminations of United States person information that did not meet the dissemination standard in NSA's minimization procedures represented approximately 4.6% of the total number of minimization incidents (as compared to 6.4% of minimization incidents during the

statement, dated April 28, 2017, "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702" at <https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activities.shtml>

⁸² (S//NF) Minimization incidents increased [REDACTED] incidents in the previous reporting period [REDACTED] in this reporting period.

⁸³ (U) In the previous reporting period, approximately 92.4% of NSA's minimization procedures errors involved improper queries.

⁸⁴ (S//NF) There were [REDACTED] United States person query incidents involving NSA during this reporting period, compared [REDACTED] the previous reporting period. [REDACTED]

⁸⁵ (S//NF) There were [REDACTED] non-compliant query incidents during this reporting period, compared [REDACTED] the previous reporting period. [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

previous reporting period).⁸⁶ As was the case with NSA querying incidents, there were no identified incidents of an NSA analyst intentionally violating the dissemination rules.

(U) In one example, NSA issued a report that included the names of United States persons whose identities were not necessary to understand foreign intelligence information.⁸⁷ NSA recalled the report and reissued it with a masked reference to the United States person. In another example, NSA discovered that an NSA analyst had issued a report that contained information from which United States persons' identities could be ascertained and whose identities were not necessary to understand foreign intelligence information.⁸⁸ The error occurred because the person responsible for releasing the report did not realize that the report contained sufficient contextual information from which the United States person's identity could be ascertained. NSA recalled the report and reissued it with a masked reference to the United States person. In all of the incidents involving improper disseminations, NSA reminded the relevant personnel of the dissemination requirements.

(U) In addition, NSA's minimization procedures require NSA personnel to consult with NSA OGC prior to disseminating information that may be protected by the attorney-client privilege. During the reporting period, there were multiple incidents in which NSA issued reports that referenced possible attorney-client communications without first consulting with NSA OGC.⁸⁹

(U) Retention rules: Furthermore, there were multiple incidents involving the improper retention of information acquired pursuant to Section 702.⁹⁰ In one such instance, NSA retained Section 702-acquired data for longer than permitted under the Section 702 minimization procedures because the relevant records were not properly indexed when they were ingested by the applicable NSA system.⁹¹

(U) (3) Other Errors

(U) Documentation Errors: In addition to the types of errors discussed above, human error also resulted in documentation errors, which comprised approximately 24% of the NSA compliance incidents in this reporting period.⁹² The NSA targeting procedures require that for each tasked

86

87

88

89

90

91

⁹² (TS//SI//NF) [REDACTED] incidents resulted from documentation errors, representing a substantial increase from the last reporting period, [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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 explanation⁹³ of the basis for NSA’s assessment at the time of targeting that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked (“foreign intelligence purpose”). 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. As in the past, NSD discussed these errors with NSA compliance personnel and has sought information from NSA on the cause of the increase and measures NSA can take to reduce such errors.

(U) Notification Delays: Finally, there were a number of reported incidents where NSA failed to timely provide the required notice to NSD and ODNI when a tasked selector was used from within the United States or by a United States person. These notification errors increased to approximately 7% of the NSA compliance incidents in this reporting period from the 1.6% in the last reporting period.⁹⁴ Many of these notification errors resulted from a training issue that occurred during a transition period in the office at NSA that handles incident reporting.⁹⁵

(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.

⁹³ (U) NSA’s documentation requirement is explained further in the Appendix.

⁹⁴

⁹⁵

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) In this reporting period, approximately 24% of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.⁹⁶ This is an increase from last reporting period's 18% and, thus, the joint oversight team assesses the need for improvement in communicating. The detasking delays caused by miscommunication typically involved travel or possible travel of non-United States persons to the United States. However, only approximately 1% of all tasking errors involved situations in which intra-agency miscommunications resulted in the erroneous tasking of a facility.⁹⁷ In all of these incidents, the erroneous collection was deleted and any identified reporting was recalled.

(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 on-going oversight efforts, the joint oversight team will also continue to monitor NSA, CIA, and FBI's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

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

(U) There was a significant increase in the number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period, with the overwhelming majority of those incidents involving minimization errors (specifically, querying errors).⁹⁸ Most of the minimization and querying incidents were caused by some personnel misunderstanding the application of the query standard in the context of batch queries. In particular, a single misunderstanding resulted in over one hundred thousand queries, comprising 97.9% of the FBI's targeting and minimization errors during this reporting period.⁹⁹

(U) A. Targeting Incidents

(S//NF) During this reporting period, there [REDACTED] incidents involving non-compliance with FBI's targeting procedures,¹⁰⁰ which represents a slight decrease from the already low number of incidents [REDACTED] during the previous reporting period. In both cases, FBI personnel approved a

96

97

98

99

10

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

[REDACTED] from a Designated Account prior to completing all searches of FBI systems required by the FBI targeting procedures. FBI personnel were reminded of the requirements of the FBI targeting procedures.

(U) B. Minimization and Querying Incidents

(U) With respect to FBI's minimization procedures, the total number of compliance incidents increased significantly to over one hundred thousand during the current reporting period from a number in the thousands in the previous reporting period.¹⁰¹ As discussed below, these non-compliant batch queries were conducted by a limited number of personnel, and a majority of these errors were conducted using a "batch query" tool in an FBI system.¹⁰² Details about remedial actions are provided below. Additionally, there were a small number of other instances of non-compliance with FBI's minimization procedures, which are also discussed below. In general, personnel were reminded of the requirements under FBI's minimization procedures.

(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. Certain FBI systems permit users to conduct multiple queries as part of a single batch query. 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 personnel conducted the queries for work-related purposes, such as attempts to investigate threats, the personnel misunderstood the application of the query requirements. Thus, as the Court 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."¹⁰³ Because of the impact of these batch queries, remedial and mitigation action was significant and is detailed below.

(U) Most of these batch query incidents were caused by FBI personnel not appreciating that their queries would be subject to the query standard because they were running against raw FISA-acquired information, as well as FBI personnel misunderstanding or not being familiar with that 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 raw FISA-acquired information.¹⁰⁴ As a result, for some of the queries at issue that were run in this system, FBI personnel either misapplied the query standard or did not think to apply the query standard to their

¹⁰¹ (S//NF) The number of minimization errors for the current reporting period was [REDACTED] compared to the [REDACTED] minimization errors in the previous reporting period.

¹⁰² (S//NF) The FBI system in which the non-compliant batch queries were conducted was FBI [REDACTED]

¹⁰³ (U) FISC's October 18, 2018 Memorandum Opinion and Order, at 68.

¹⁰⁴ (S//NF) [REDACTED] the database referenced.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

proposed queries before conducting queries in that particular FBI database, or failed to opt out¹⁰⁵ of conducting queries against raw FISA-acquired information.

(S//NF) The largest single FBI compliance incident involved 105,613 improper batch queries of raw FISA-acquired information in [REDACTED].¹⁰⁶ Between July 27 and August 10, 2018, an FBI intelligence analyst ran batch queries in [REDACTED] using the identifiers of all individuals [REDACTED]

[REDACTED] The analyst advised that the queries were run to determine if any of the individuals were either current or former subjects of FBI predicated international terrorism investigations, and advised that he/she did not intend to run the queries against raw FISA-acquired information. The analyst failed to opt out of the raw FISA datasets in [REDACTED] when these queries were conducted, and, thus, they ran in datasets in [REDACTED] that included FISA-acquired information. The analyst advised that the queries did not return any raw FISA-acquired information.

(S//NF) In another instance, an intelligence analyst conducted approximately 1,946 queries in [REDACTED] using the names and dates of birth of individuals, including United States persons, who were registered competitors [REDACTED].¹⁰⁷ The analyst advised that he/she conducted these queries in order to determine whether any of the individuals posed a national security or terrorism threat. The analyst further advised that, prior to conducting these queries, there were no known threats associated with [REDACTED] and he/she had no reason to suspect that any of the queries would return foreign intelligence information or evidence of a crime; rather, he/she conducted the queries as part of routine event safety checks. In addition, the analyst advised that he/she does not remember the queries returning raw FISA-acquired information and confirmed that he/she did not retain or use any results of the queries.

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

(U) During this reporting period, most of the separate 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

¹⁰⁵ (S//NF) [REDACTED] is currently designed to have user queries run against raw FISA-acquired information if the user is allowed access to such information and has not affirmatively opted out of such information. This has been an underlying cause of multiple incidents. As background, [REDACTED] was originally designed in this manner to further data aggregation and integration. "[REDACTED] allows FBI personnel to run a single query across [REDACTED] datasets and view the corresponding results from the various datasets in an aggregated manner. This capability assists FBI personnel in identifying connections in different sources of information, such as confidential human source reporting, FISA collection, information shared by foreign partners, and documentation held by other U.S. Government entities..." See *Declaration of the Director of the FBI*, filed with the FISC September 14, 2018.

¹⁰⁶ [REDACTED]

¹⁰⁷ [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

that they did not recall why they ran the query. In other incidents, FBI personnel were generally unaware of, or were not thinking of, the fact that their queries would be running against raw FISA-acquired information and did not intend to return such information. In each of the incidents below, FBI personnel were reminded of the rules regarding queries.

(U) Specifically, some of the improper queries involved FBI personnel conducting queries of United States person identifiers, including using their own or other FBI personnel names for work-related purposes, such as for case load management.¹⁰⁸ Other incidents involved FBI personnel running queries using terms, such as FBI report numbers or national security letter numbers, to find work-related information or documents unrelated to raw FISA-acquired information.¹⁰⁹ In these incidents, FBI personnel misunderstood the application of the query rules and, in some instances, personnel did not appreciate that running queries in a database that contains raw FISA would mean that those queries would be subject to the querying rules. FBI personnel were subsequently reminded of how to correctly apply the query rules.

(U) Other incidents involved queries of individuals, including United States persons, who were being considered as potential sources of information. While those queries were conducted for work-related purposes, they were conducted without having a reasonable basis to believe that such queries were likely to return foreign intelligence information or evidence of a crime. For example, in one instance, FBI personnel conducted approximately multiple queries using identifiers associated with individuals whom FBI had identified as potential sources.¹¹⁰ In other incidents, the queries were non-compliant because the queries were overbroad and/or not reasonably designed to find and extract foreign intelligence information or evidence of a crime.¹¹¹ In 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)~~ Some of the improper queries involved queries that were not justified because the FBI personnel conducting the queries did not have reason to believe that the query would return foreign intelligence information or evidence of a crime.¹¹²

108

109

110

111

¹¹² ~~(S//NF)~~ In one instance, FBI personnel conducted multiple queries of an individual who had the same last name as the FBI personnel. The TFO initially told NSD he could not recall why he ran these queries. NSD asked the chief division counsel at the field office to speak to the personnel again after the review. During that discussion, the personnel admitted that he ran the queries because of a tip from his mother about a threatening phone call regarding the individual's father having an extra-marital affair.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) Finally, other incidents involved improper queries conducted not in furtherance of an operational need designed to find and extract foreign intelligence information or evidence of a crime, but rather as part of an administrative training exercise.¹¹³ At the time of the queries, the FBI Section 702 minimization procedures did not permit queries to be conducted against raw-FISA acquired information for this purpose. As part of the FISC-approved 2018 certifications, the Government amended the FBI's querying procedures to allow, under certain circumstances, such training queries.¹¹⁴

(U) (3) Other Minimization Errors Caused by Misunderstanding or Miscommunication

(U) During this reporting period, there were also 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. 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 of the review team must be individuals who have no role in the prosecution, and they initially review the Section-702 acquired information to determine whether the communications are privileged. Failure to timely establish such a review team constitutes a compliance incident.

(S//NF) During this reporting period, two errors involved the failure to timely establish such a review team because of a misunderstanding or miscommunication.¹¹⁵ The joint oversight team assesses that these types of incidents typically are the result of individual failures or confusion. For example, in one such incident, the FBI agent assigned to the case concerning a federally indicted Section 702 target failed to notify the FBI agent responsible for reviewing the Section 702-task facilities that the target had been charged until several months after the sealed complaint had been filed. 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 [REDACTED]

[REDACTED] will help facilitate both the identification of review team compliance incidents and assist in the prevention of any future incidents. The joint oversight team assesses that continued oversight and training, as well as FBI's modified tool, will continue to help facilitate both the identification of review team compliance incidents and assist in the prevention of any future incidents.

113 [REDACTED]

¹¹⁴ (U) These procedures, along with other documents related to the 2018 Section 702 certification, were publicly released on October 8, 2019, on *IC on the Record*.

115 [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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

(U) Since 2018, 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 raw 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 raw 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 raw 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 its 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 raw FISA-acquired information. FBI is also currently developing revised standard training for personnel who have access to raw 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 raw FISA-acquired information and how personnel can select the appropriate option to allow the FBI to better track and comply with requirements involving queries run against raw 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 procedures¹¹⁶ 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 the

¹¹⁶ (U) In August 2019, the Attorney General adopted amended FBI’s 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*.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

Court on FBI's implementation of the new requirements.¹¹⁷ Between September and November 2019, the FBI implemented changes to FBI systems storing raw 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. These changes also made it easier for FBI personnel to "opt-out" of running their queries against FISA-acquired information. 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 raw 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) IV. Review of Compliance Incidents – CIA Minimization and Querying Procedures

(U) During this reporting period, there were a small number of incidents involving noncompliance with the CIA minimization and querying procedures. Those incidents involved inadvertent instances of CIA either improperly retaining Section 702-acquire information or not completely removing Section 702-acquired information that should have been deleted from CIA systems.

(S//NF) CIA receives unminimized communications from selectors that it nominates to NSA for targeting [REDACTED]. Communications from those selectors are routed into access-controlled CIA data repositories specifically designated to receive information obtained pursuant to Section 702, which are physically or logically separated from other CIA data repositories. As previously reported to the Court, CIA separates all Section 702-acquired metadata from Section 702-acquired communications and separately retains that metadata in metadata-only repositories.

(S//NF) Specifically, one incident involved the improper retention of United States person identifying information that was not necessary to understand foreign intelligence information in a widely accessible CIA system.¹¹⁸ The error was due to a misunderstanding of the capabilities of [REDACTED] software [REDACTED]. CIA has sanitized the United States person identifying information in its system and counseled the responsible personnel. A second incident involved CIA's failure to notify NCTC of the obligation to purge certain Section 702-

¹¹⁷ (S//NF) Subsequent to the reporting period, the FBI has implemented changes [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. *See, e.g.,* [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. *See id.* at 10, 13-14.

¹¹⁸ [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

acquired data from NCTC's repositories.¹¹⁹ NCTC data repositories ingest certain [REDACTED] from CIA systems; NCTC personnel, accordingly, rely on CIA personnel to notify them when [REDACTED] are subject to purge for various reasons, including because they contain non-compliant Section 702-acquired information. However, from November 2016 through July 2018, CIA failed to notify NCTC when CIA ordered the purge [REDACTED] Section 702-acquired information that had been directed to NCTC repositories. CIA has added NCTC personnel to its purge notification distribution list, and NCTC has purged the relevant [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 a violation of NCTC's minimization and querying procedures in effect at the time of the incidents.¹²⁰ All of the incidents relating to NCTC's procedures during this reporting period involved improper queries of Section 702-acquired data.¹²¹ In these queries, NCTC personnel misunderstood the rules and were reminded about how to apply the rules. None of the queries involved queries conducted using United States person identifiers.

(U) VI. Review of Compliance Incidents – Other

(U) During the reporting period, there was one incident involving a violation of the FISA statute by a federal agency other than NSA, CIA, FBI, and NCTC. Specifically, U.S. Customs and Border Protection (CBP) disseminated reports containing minimized, FISA-acquired information, which appeared to be based on NSA reporting, for law enforcement purposes and intelligence purposes without including an accompanying caveat, as required by 50 U.S.C. § 1806(b).¹²² The Government believes that the NSA reporting contained the proper caveats. CBP advised that it recalled each of the reports and reissued them with the required caveat; CBP further advised that it advised the relevant personnel of the FISA caveat requirement.

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

(S//NF) During this reporting period, there were [REDACTED] instances of noncompliance (compared to one incident during the last reporting period) by an electronic communication service provider with a Section 702(i) directive, only one of which affected numerous facilities. [REDACTED]

[REDACTED]¹²³

¹¹⁹ [REDACTED]

¹²⁰ (S//NF) There were [REDACTED] incidents during this reporting period as opposed to [REDACTED] incidents during the previous reporting period.

¹²¹ [REDACTED]

¹²² (U) Section 1806(b) requires any disclosure of FISA-acquired information or information derived from FISA for law enforcement purposes to include a caveat indicating that the information "may only be used in a criminal proceeding with the advance authorization of the Attorney General." Failure to include such a caveat constitutes a compliance incident.

¹²³ [REDACTED]

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(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.

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

APPENDIX

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~


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 persons² reasonably believed to be located outside the United States.

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



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

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

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

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

3



4

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to receive or communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General's Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

(U) Under NSA's FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a "selector") is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.⁵ In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA "tasks" that facility in the relevant tasking system. The facilities are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

(U) After information is collected from those tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (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

5



6



A-3

~~TOP SECRET//SI//NOFORN/TISA~~

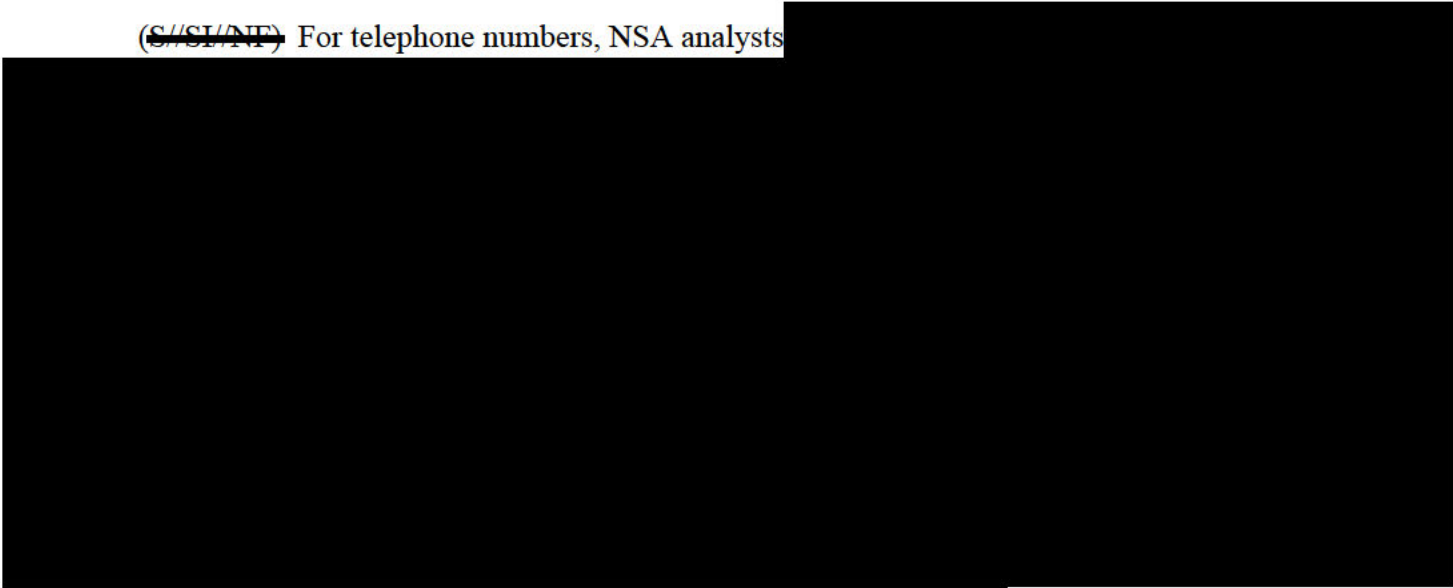
~~TOP SECRET//SI//NOFORN/TISA~~

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

(U) A. Pre-Tasking Location

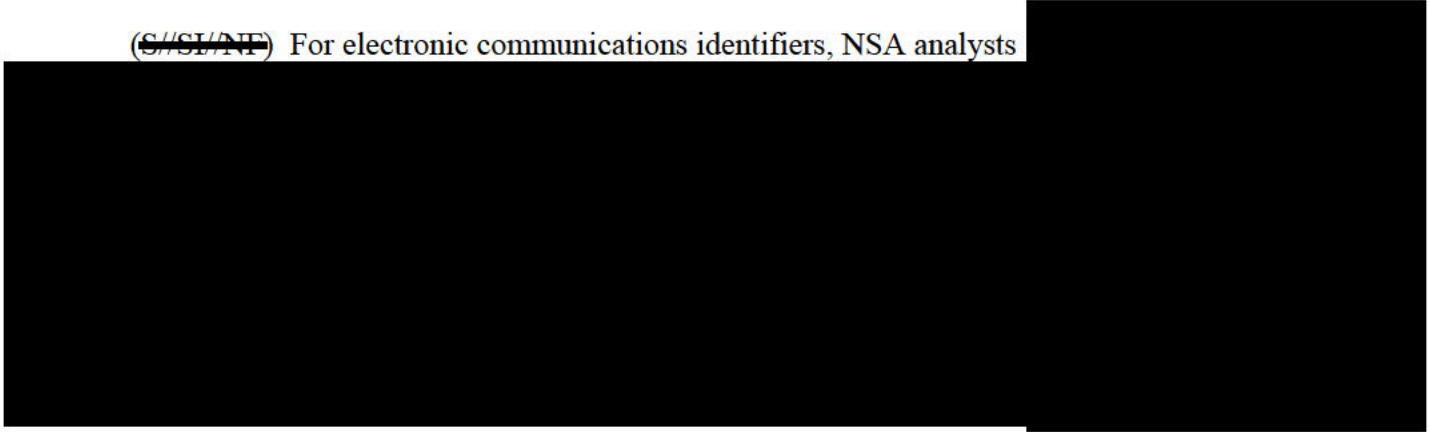
(U) 1. Telephone Numbers

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



(U) 2. Electronic Communications Identifiers

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



7



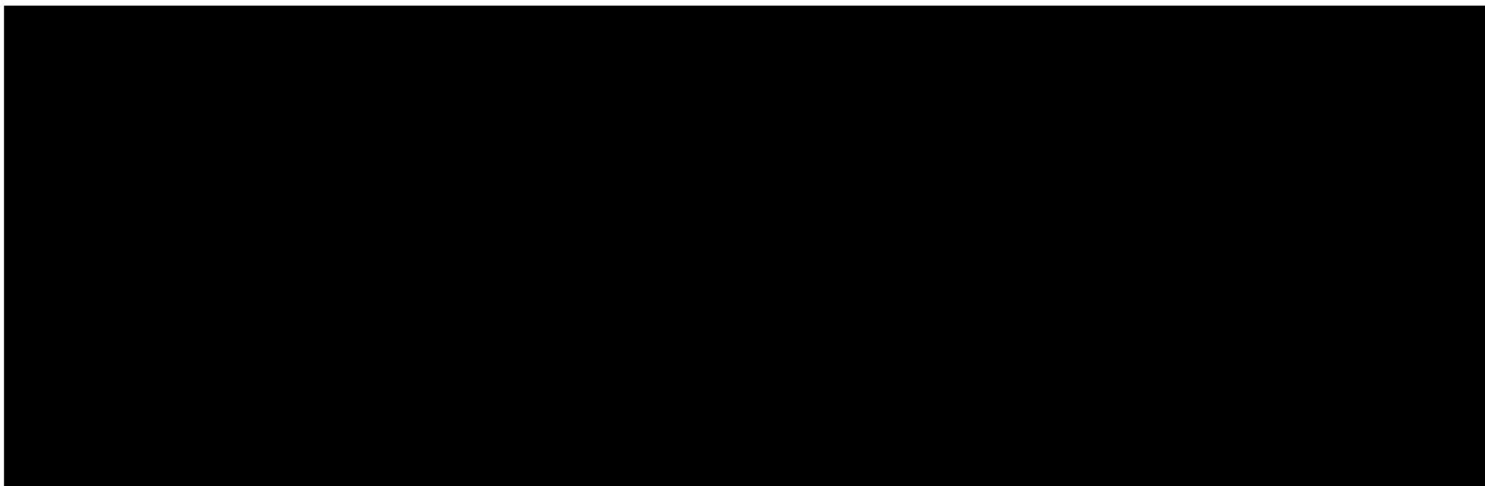
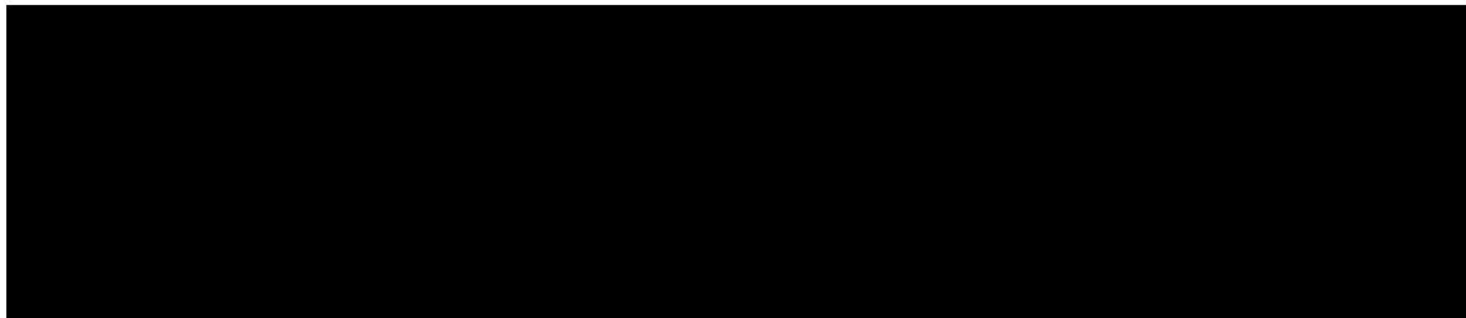
⁸ (U) Analysts also check this system as part of the “post-targeting” analysis described below.

9



A-4

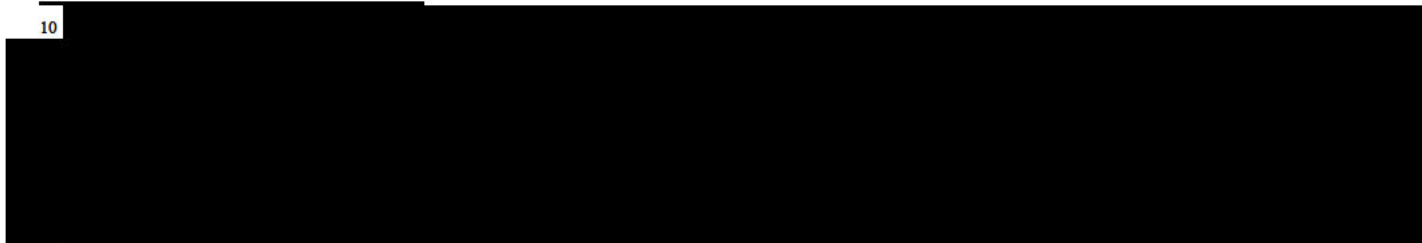
~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(U) B. Pre-Tasking Determination of United States Person Status****(U) C. Post-Tasking Checks**

(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] [REDACTED]¹¹ a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority. [REDACTED]

[REDACTED] Should traffic not be viewed 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



¹¹ (S//NF) NSA's automated notification system to ensure analysts have reviewed collection is currently implemented for [REDACTED] and as of approximately October 2018, for [REDACTED]

A-5

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~**(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]

[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]
[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.

A- 6

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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



(U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA OGC and OCO training program; review the targeting, minimization, and querying procedures as well as other documents filed with the certifications; and 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 spot 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

A-7

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

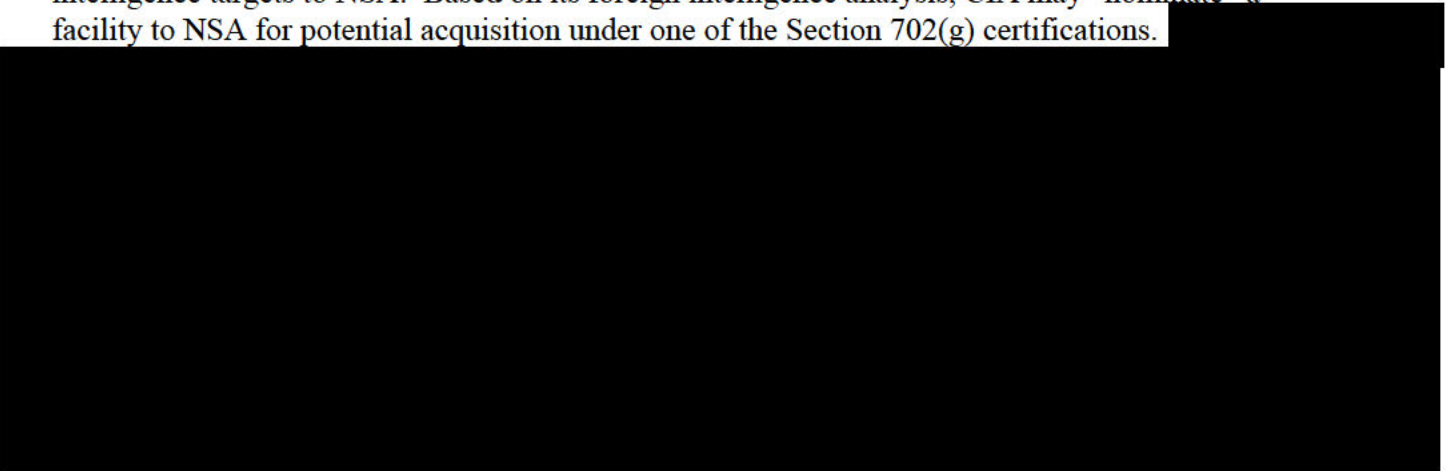
(CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protections during NSA missions. The Compliance Group complements and reinforces the intelligence oversight program of the NSA OIG and oversight responsibilities of NSA OGC.

(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 has developed a risk assessment process to assess the potential risk of non-compliance with the rules designed to protect United States person privacy. The assessment is conducted and reported to the NSA Deputy Director and NSA senior leadership team biannually.

(U) II. Overview – CIA

(U) A. CIA’s Role in Targeting

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

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

[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]

[REDACTED]

(S//NF) The FISA Program Office was established in December 2010 [REDACTED] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA, and FBI. In addition, the office leads the day-to-day FISA compliance efforts [REDACTED]. The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

(U) B. Oversight and Compliance

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

(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]

A-9

~~TOP SECRET//SI//NOFORN/FISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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 raw FBI-collected FISA-acquired information in accordance with NCTC's Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act. In consultation with NSD, ODNI, NSA, and FBI, NCTC modified [REDACTED] to (i) provide additional compliance capabilities in support of [REDACTED] FISA Section 702-acquired counterterrorism data and (ii) monitor compliance with NCTC's minimization procedures for Section 702-acquired counterterrorism data (Section 702 minimization procedures). In addition to documenting compliance with the Section 702 minimization procedures requirements, [REDACTED] also documents the requests for [REDACTED] of Section 702-acquired information. This documentation includes the 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 minimization procedures 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 minimization procedures or querying procedures, as applicable. By internal policy, [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 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]

A-10

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

and other products are recalled. NCTC's purge completion date reflects the date when all data identified using the above protocol has been removed from the systems accessible to NCTC analytical personnel.

(S//NF)

Pursuant to Section A.6 of NCTC's minimization procedures,

(U) B. Oversight and Compliance

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

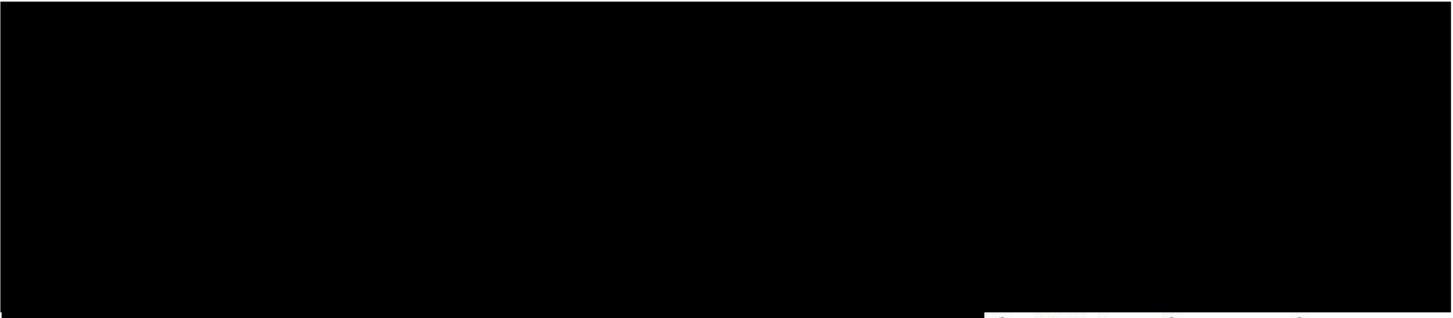
(U) A. FBI's Role in Targeting – Nomination for Acquiring In-Transit Communications

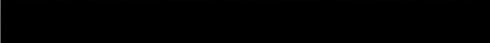
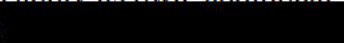
(S//NF) Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition [REDACTED] communications. [REDACTED]


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

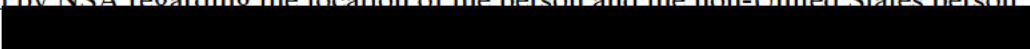
A- 11

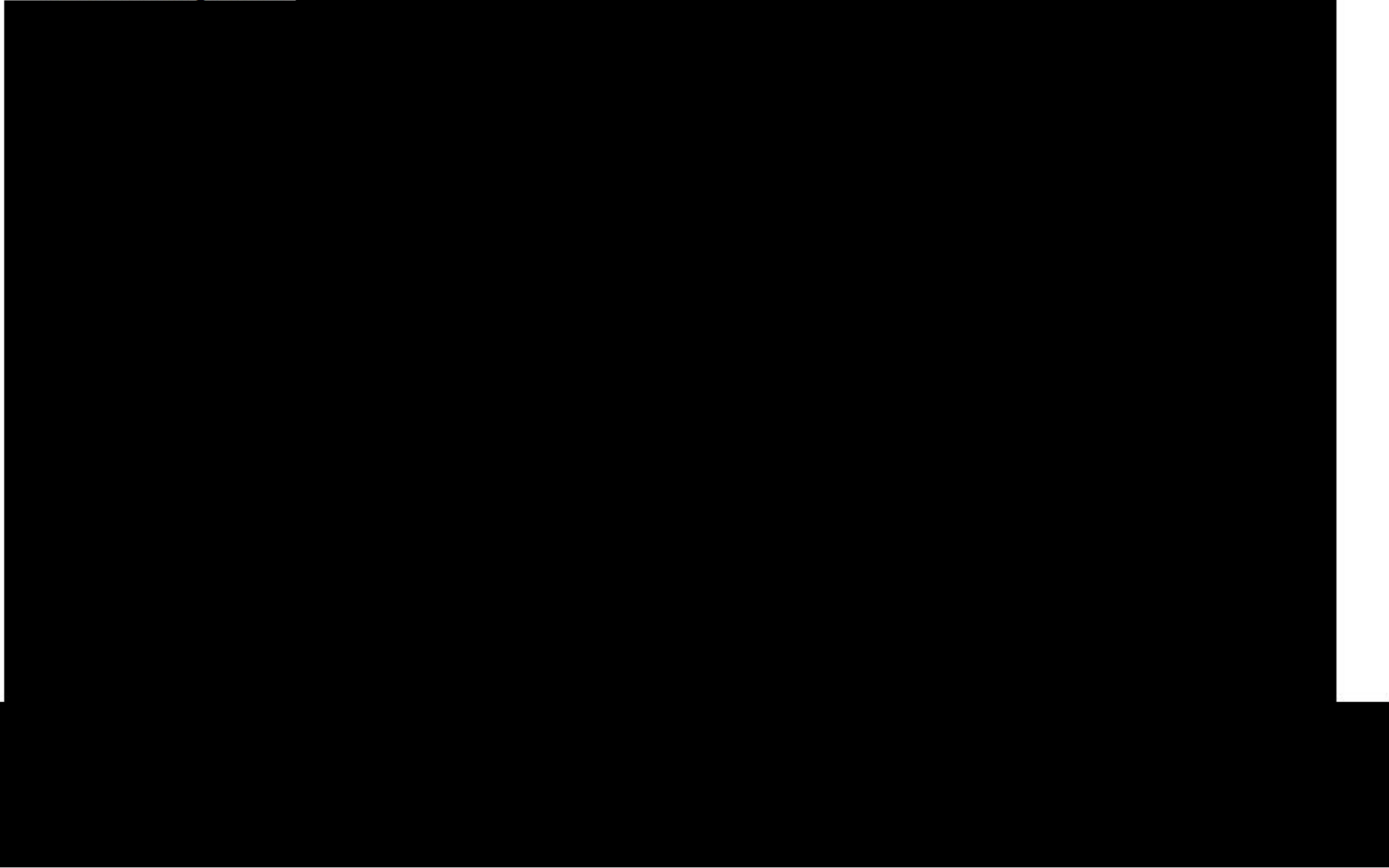
~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

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



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



A- 12

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

[REDACTED]

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

[REDACTED]

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

[REDACTED]

(U) C. Documentation

(S//NF) The targeting procedures require that FBI retain the information [REDACTED] in accordance with its records retention policies [REDACTED]

[REDACTED] FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its internal operating procedures, commencing with [REDACTED] extending through [REDACTED] and culminating in approval or disapproval of the acquisition. In addition, the FBI's internal 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 Exploitation Threat Section (XTS), FBI's [REDACTED] and FBI's Inspection [REDACTED]

A- 13

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/TISA~~

Division (INSD). [REDACTED]

[REDACTED] TS has the lead responsibility in FBI for [REDACTED] requests [REDACTED] XTS personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests [REDACTED] XTS also has the lead responsibility for facilitating FBI's nominations to NSA [REDACTED] XTS, NSCLB, NSD, and ODNI have all worked on training FBI personnel to ensure that FBI nominations and post-tasking review comply with the NSA targeting procedures. Numerous such trainings were provided during the current reporting period. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in the FBI [REDACTED]

[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. XTS 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

A- 14

~~TOP SECRET//SI//NOFORN/TISA~~

~~TOP SECRET//SI//NOFORN/FISA~~

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.

~~TOP SECRET//SI//NOFORN/FISA~~