

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

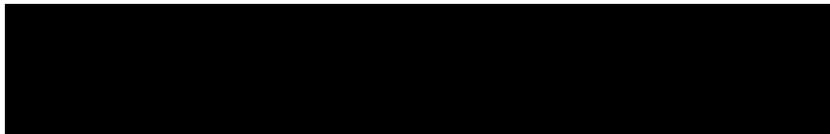


(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) Reporting Period: 01 June 2020 – 30 November 2020

April 2022

Classified By:
Derived From:
Declassify On:



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

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

**(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**

April 2022

(U) TABLE OF CONTENTS

(U) Executive Summary	1
(U) Section 1: Introduction	4
(U) Section 2: Oversight of the Implementation of Section 702	7
(U) I. Joint Oversight of NSA	7
(U) II. Joint Oversight of FBI	10
(U) III. Joint Oversight of CIA	13
(U) IV. Joint Oversight of NCTC	14
(U) V. Interagency/Programmatic Oversight	15
(U) VI. Training	16
(U) Section 3: Trends in Section 702 Targeting and Minimization	18
(U) I. Trends in NSA Targeting and Minimization	18
(U) II. Trends in FBI Targeting	23
(U) III. Trends in CIA Minimization	25
(U) IV. Trends in NCTC Minimization	27
(U) Section 4: Compliance Assessment – Findings	29
(U) I. Compliance Incidents – General	30
(U) II. Review of Compliance Incidents – NSA Targeting, Minimization, and Querying Procedures	45
(U) III. Review of Compliance Incidents – FBI Targeting, Minimization, and Querying Procedures	54
(U) IV. Review of Compliance Incidents – CIA Minimization and Querying Procedures	62
(U) V. Review of Compliance Incidents – NCTC Minimization and Querying Procedures	63
(U) VI. Review of Compliance Incidents – Provider Errors	64
(U) Section 5: Conclusion	65
(U) Appendix	A-1

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

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

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

(U) FACT SHEET

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

Joint Assessments

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as “Joint Assessments,” and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of April 2022, twenty-five 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: 01 December – 31 May or 01 June – 30 November. This joint assessment covers the reporting period of 01 June 2020 through 30 November 2020.
- (U) *Who receives it?* Each joint assessment is submitted to the following oversight entities: the Foreign Intelligence Surveillance Court (FISC), relevant congressional committees, and the Privacy and Civil Liberties Oversight Board (PCLOB).
- (U) *What is being assessed?* The Attorney General and the DNI jointly assess the Government’s compliance with Attorney General Guidelines and with FISC-approved “targeting,” “minimization,” and “querying” procedures.
- (U) *What are targeting, minimization, and querying procedures?* Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information. Querying procedures set rules for using United States person and non-United States person identifiers to query Section 702-acquired information.
- (U) *What compliance and oversight efforts underlie the joint assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, judicial, and constitutional requirements. A joint oversight team

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

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

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 assessments summarize trends and assess 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) implement Section 702. 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. It is carefully redacted for public release in the interest of transparency.
- (U) *What is the format of the joint assessment?* The joint assessment generally contains an Executive Summary, five sections, and an Appendix. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts, and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews in order to provide insight into the overall scope of the Section 702 program. Section 4 assesses targeting, minimization, and querying incidents representative of overarching trends. The joint assessment describes the extensive measures undertaken by the Government to ensure compliance with court-approved targeting, minimization, and querying procedures; accurately identify, record, and correct errors; take responsive actions to remove any erroneously obtained data; and minimize the chances that mistakes will reoccur.
- (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 dissemination 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

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

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

702(i) directive, the joint assessment includes a review of any compliance incidents by such service providers.

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

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

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

(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

April 2022

(U) Reporting Period: 01 June 2020 – 30 November 2020

(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 (AG) 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 25th Joint Assessment of compliance under the Section 702 program. This assessment covers the period from 01 June 2020 through 30 November 2020 (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 08 March 2021; it covers the same reporting period as the joint assessment.

(U) This joint assessment is based upon the compliance assessment activities that have been conducted by a joint oversight team consisting of experts from DOJ’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) (hereinafter, the “joint oversight team”).

(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) As the below metrics illustrate, this reporting period, which occurred during the coronavirus pandemic, saw a significant decrease in the total number of reported compliance incidents, as compared to periods that occurred prior to the pandemic. At the time of writing this joint assessment, the joint oversight team is not able to determine to what extent these compliance

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

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

trends reflect a decrease in the number of compliance incidents that occurred¹ – whether as a result of the coronavirus pandemic or other factors – as opposed to difficulties in discovering and reporting compliance incidents as a result of the pandemic. As it pertains to the latter, the joint oversight team’s onsite reviews were affected by the pandemic. Specifically, a number of reviews were conducted virtually and/or postponed for short periods of time. Due to travel restrictions, onsite reviews at FBI field offices were suspended during this reporting period.

(U) During this reporting period, the overall compliance incident rate – calculated as the total number of compliance incidents reported during the relevant reporting period, expressed as a percentage of the average number of facilities subject to acquisition on any given day during the reporting period – was 0.34 percent, which represents a decrease from the prior period (0.46 percent). As has been explained in past joint assessments and detailed later in this current assessment, the overall compliance incident rate is an imperfect metric and potentially misleading, in part because many of the compliance incidents included in the numerator do not bear a meaningful relation to the targeting activities in the denominator. For example, the number of FBI query errors is not related to the average number of facilities subject to acquisition. In order to provide a more nuanced and accurate assessment of compliance, future assessments will not continue to report this overall compliance incident rate and instead provide more specific compliance incidents rates that have been developed in the last few assessments.

(U) Two such more specific rates are featured in this assessment. The first is the targeting compliance incident rate for NSA (see Figure 14), which represents the number of NSA targeting compliance incidents, expressed as a percentage of the average number of facilities subject to acquisition on any given day during the reporting period. During this reporting period, the targeting compliance incident rate for NSA was 0.05 percent, a decrease from the prior reporting period (0.10 percent). The second is the query error rate for FBI (see Figure 18), which 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.² During this reporting period, the query error rate for FBI was 2.2 percent, an increase from the prior reporting period (0.82 percent).

¹ ~~(TS//SI//NF)~~ The joint oversight team assesses that a number of factors related to the coronavirus pandemic may have contributed to a decrease in the actual number of compliance incidents during this reporting period. As one example, reduced travel during the pandemic likely resulted in fewer Section 702 targets traveling to the United States, thus reducing the likelihood that detasking delays would occur as a result of such travel. 

² ~~(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’s  NSD has, in prior query audits, found that a small percentage of queries that were included in particular query logs were not run against unminimized FISA-acquired information, to include unminimized Section 702-acquired information.

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

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

(U) In recent years, FBI field office reviews have been responsible for discovering a significant portion of the FBI minimization and querying incidents that are reported in each joint assessment. Because FBI field office reviews were suspended during this reporting period, incidents that might typically be discovered by NSD during those field office reviews were not discovered while the reviews were suspended.³ Some of the most significant errors identified as a result of prior reviews have been those related to batch queries, a functionality available in an FBI system that permits users to query multiple identifiers in sequential queries as part of a single batch job. If a single batch job consists entirely or largely of noncompliant queries it can result in thousands of improper queries; as such, the discovery of a single noncompliant batch job can substantially affect both the overall and FBI query compliance incident rates. Just a handful of non-compliant batch queries have been responsible for the wide-ranging compliance incident rates over the last several reporting periods. Whether such a noncompliant batch job involving thousands of compliance incidents would or would not have been discovered during this reporting period had FBI field office reviews not been suspended is unknown. NSD resumed field office query reviews remotely in 2021 and has continued to identify query compliance issues in each field office reviewed.⁴ FBI has implemented a series of remedial measures beginning in the fall of 2019 and the joint oversight team continues to work with FBI to review progress and develop additional corrective actions to address query compliance issues. The remedial measures undertaken by FBI are discussed further below.

³ (U) FBI's minimization and querying incidents reported in this joint assessment were first reported to the FISC during this reporting period, but certain of those incidents were discovered in connection with field office reviews conducted during prior reporting periods.

⁴ (U) Onsite field office reviews were suspended in March 2020, at the onset of the coronavirus pandemic and related travel restrictions in the United States. Thus, during this reporting period, NSD did not conduct any field office reviews. NSD resumed field office reviews remotely in February 2021, at which time NSD selected for sampling a range of historical queries conducted throughout 2020 by users in multiple FBI field offices. The results of those reviews will be included in the reporting period in which they were reported to the FISC rather than the reporting period in which the compliance incident took place.

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

~~TOP SECRET//SI//NOFORN/FISA~~**(U) SECTION 1: INTRODUCTION**

(U) FISA Section 702(m)(1)⁵ requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 and to submit such assessments to the FISC and relevant congressional committees at least once every six months. To fulfill this requirement, a team of oversight personnel from the Department of Justice’s (DOJ) National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) (hereinafter, the “joint oversight team”) normally conducts compliance reviews to assess whether the authorities under Section 702 have been implemented in accordance with the applicable procedures and guidelines, discussed herein; however, as explained above, on-site compliance reviews during this reporting period were impacted by the coronavirus pandemic. This report sets forth NSD and ODNI’s 25th joint compliance assessment, based on regular and modified oversight activities during this reporting period, of Section 702 activities, covering the period 01 June 2020 through 30 November 2020 (hereinafter, the “reporting period”).⁶

(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.

(U) The Attorney General’s Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter, “the

⁵ (U) *See* 50 U.S.C. §1881a(m)(1).

⁶ (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702, which was previously submitted on 08 March 2021, as required by Section 707(b)(1) of FISA (hereinafter, the “Section 707 Report”). This 25th Joint Assessment covers the same reporting period as the 25th Section 707 Report.

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

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

Attorney General's Acquisition Guidelines") were adopted by the Attorney General, in consultation with the DNI, on 05 August 2008.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(h) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information. The foreign intelligence information must fall within a specific category of foreign intelligence information that has been authorized pursuant to the Section 702(h) certifications.⁷ Four agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and 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 U.S. Government employs to ensure compliance with targeting, minimization, and querying 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 discusses compliance incidents as they represent overarching compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the corresponding 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 reoccurrences. Finally, this joint assessment contains an Appendix, which as noted above, includes a general description of the oversight at each agency.

(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

⁷ ~~(TS//SI//NF)~~ These six Section 702(h) certifications, all targeting non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information, concerned the following categories of foreign intelligence information:

- Certifications 2019-A and 2020-A's [REDACTED]
- Certifications 2019-B and 2020-B's [REDACTED]
- Certifications 2019-C and 2020-C's [REDACTED]

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

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

the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying procedures caused a significant number of query errors.

(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. 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 ongoing efforts.

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

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

(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 acquires certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, CIA, and NCTC⁸ each handles Section 702-acquired data in accordance with its own minimization and querying procedures.⁹ 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 gained by leveraging preexisting systems and processes to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

(U) The joint oversight team, consisting of members from NSD, the ODNI Office of Civil Liberties, Privacy, and Transparency (CLPT), the ODNI Office of General Counsel (OGC), and the ODNI Mission Integration Directorate Mission Performance, Analysis, and Collection (MPAC), conducts independent Section 702 oversight activities. 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 DNI's certifications, all Section 702 targeting is initiated pursuant to NSA's targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities¹⁰ (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

⁸ (U) As discussed herein, CIA and NCTC receive Section 702-acquired data from NSA and FBI.

⁹ (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 2019 certifications in December 2019 and the 2020 certifications in November 2020. On 04 September 2020, the DNI released, in redacted form, each of the 2019 minimization procedures and the 2019 querying procedures for NSA, FBI, CIA, and NCTC, as well the 2019 targeting procedures for NSA and FBI. On 26 April 2021, the DNI released, in redacted form, the same documents for 2020. The 2019 and 2020 procedures are posted on *intel.gov* via ODNI's *IC on the Record* database.

¹⁰ (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 joint assessment uses the terms facilities and selectors interchangeably and does not make a substantive distinction between the two terms.

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

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 NSA’s targeting procedures require, as well as the investigation and reporting of specific compliance incidents. During this reporting period, onsite reviews were conducted at NSA on the dates shown in Figure 1.

(U) Figure 1: NSA Reviews

UNCLASSIFIED

Date of NSA Review	Targeting, Minimization, and Querying Reviewed
28 August 2020	01 June 2020 – 31 July 2020
23 October 2020	01 August 2020 – 30 September 2020
26 February 2021	01 October 2020 – 30 November 2020

(U) Figure 1 is UNCLASSIFIED.

~~(S//NF)~~ 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, and provide a detailed summary of the findings for that reporting period.

[REDACTED]

with the Section 707 Report, as required by

Section 707(b)(1)(F) of FISA;

[REDACTED] was provided to the congressional committees with the subsequent Section 707 report.

(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, which 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-United States 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.

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

(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 Cyber and Operations (OCCO), 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 and a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) NSA's Section 702 querying procedures provide that any use of United States person identifiers as terms to identify and select Section 702-acquired data must be accompanied by 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 procedures provide that the United States person identifier must first be approved by NSA's OGC. The joint oversight team reviews all approved United States person identifiers to ensure compliance with NSA's querying procedures.¹¹ 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 date that the United States person identifier was authorized to be used as a query term,¹² and any other relevant information. In addition, with respect to queries of Section 702-acquired *metadata* using a United States person identifier, NSA's querying procedures require that NSA analysts document the basis for each such metadata query prior to conducting the query. NSD reviews the documentation for 100 percent of such metadata queries that NSA provides to NSD.¹³

¹¹ (U) On 30 April 2021, the DNI publicly released ODNI's eighth annual Transparency Report[s]: *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2020* (hereinafter, the "CY2020 Transparency Report"). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(B)), the 2020 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 2020.

¹² (U) NSA's Section 702 querying procedures provide that NSA may approve the use of a United States person identifier to query Section 702-acquired *content* for no longer than a period of one year and that such approvals may be renewed for periods up to one year.

¹³ (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(C)), the CY2020 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 2020.

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

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

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with NSA's 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 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

Pursuant to its own authority, FBI is authorized to from electronic communication service providers by targeting facilities that NSA nafter, "Designated Accounts"). FBI conveys

from the electronic communications service providers for processing in accordance with the agencies' FISC-approved minimization procedures.

(U) ~~(S//NF)~~ Third, FBI may receive dual-routed,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.

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, "detasked" (*i.e.*, stopped collection against) the target's facility without delay, as is required by NSA's targeting procedures, the collection while the target was in the United States would not be considered a compliance incident under NSA's targeting procedures, although the collection would generally be subject to purge under the applicable minimization procedures. The joint oversight team carefully considers, and where appropriate, obtains additional facts regarding every reported detasking decision to ensure that NSA's tasking and detasking complied with its targeting procedures.

(U)¹⁵ ~~(S//NF)~~ Dual-routing is the process whereby CIA, FBI, or NCTC request NSA route data from Section 702 facilities tasked by another agency.

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

(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. The joint oversight team generally conducts monthly reviews at FBI headquarters of FBI’s compliance with its targeting procedures and quarterly reviews at FBI headquarters of FBI’s compliance with its minimization procedures. However, due to the coronavirus pandemic, the joint oversight team did not conduct onsite reviews at FBI headquarters. Instead, the joint oversight team conducted reviews of FBI’s application of its targeting and minimization procedures remotely. As a result of FBI’s reduced staffing due to the coronavirus pandemic, FBI was unable to gather the information necessary to finalize one of the reports before the production to Congress of the Section 707 Report; the remaining report was subsequently finalized with the help of FBI and was provided to the congressional committees with subsequent Section 707 reports. For this reporting period, reviews were conducted during the dates shown in Figure 2.

(U) Figure 2: FBI Reviews

UNCLASSIFIED

Dates of FBI Review	Targeting and Minimization Reviewed
October – November 2020	June and July 2020 targeting decisions
December 2020 – January 2021	August and September 2020 targeting decisions
February – March 2021	October and November 2020 targeting decisions

(U) Figure 2 is UNCLASSIFIED.

(U) In conducting targeting reviews, the joint oversight team reviews 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) In conducting FBI minimization reviews, the joint oversight team reviews documents related to FBI’s application of its Section 702 minimization procedures. The joint oversight 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 joint oversight 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 persons.

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 return 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]

[REDACTED] During this reporting period, the joint oversight team reviewed a sample of checklists and supporting documentation provided by FBI for approved requests for which information is returned by FBI’s database queries.

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

(U) During this reporting period, NSD had suspended its minimization and querying reviews at FBI field offices due to the coronavirus pandemic. As a result, NSD did not conduct any reviews at FBI field offices during this reporting period. Subsequent to this reporting period, in February 2021, NSD resumed conducting remote reviews of queries of unminimized FISA collection conducted by some FBI field offices. In minimization reviews conducted prior to March 2020, NSD reviewed a sample of retention decisions made by FBI personnel in connection with investigations involving the acquisition of data pursuant to Section 702 and a sample of disseminations of information acquired pursuant to Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons. During its querying reviews, NSD reviewed a sample of queries by FBI personnel in FBI systems that contain raw (unminimized) FISA-acquired information, including Section 702-acquired information. In addition, as a result of a Court-ordered reporting requirement first set forth in the FISC's 06 November 2015 Memorandum Opinion and Order¹⁷ for queries conducted after 04 December 2015, as well as certain requirements in 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.

~~(S//NF)~~ Separately, in order to evaluate FBI [REDACTED] acquisition [REDACTED] and provision of [REDACTED] the joint oversight team conducts an annual process review with FBI's technical personnel to ensure that those activities complied with applicable minimization procedures. The most recent annual process review occurred in June 2021 and a report regarding that review was submitted to Congress along with the relevant Section 707 Report.

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

¹⁷ (U) The FISC's 06 November 2015 Opinion and Order approved the 2015 FISA Section 702 Certifications. On 19 April 2016, the DNI, in consultation with the Attorney General, released in redacted form, this *Opinion and Order* on the ODNI public website *intel.gov* via the *IC on the Record* database.

(U) ~~(S//NF)~~ The title of the FISC's 06 November 2015 opinion is ~~(S//NF)~~ *In re DNI/AG 702(g) Certifications 2015-A, 2015-B-, 2015-C, and Predecessor Certifications*.

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

(U) Throughout the reporting period, the joint oversight team also investigates potential incidents of noncompliance with the FBI targeting, minimization, and querying procedures, the Attorney General’s Acquisition Guidelines, or other agencies’ procedures in which FBI is involved.¹⁸ Those investigations are coordinated with FBI’s 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 typically conducts onsite visits at CIA,¹⁹ 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.

~~(S//NF)~~ The reviews also focus on CIA’s application of its Section 702 minimization procedures and querying procedures.

[REDACTED]

[REDACTED] with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA; [REDACTED]

[REDACTED] provided to the congressional committees with the subsequent Section 707 report. For this reporting period, the joint oversight team conducted reviews of CIA’s application of its minimization and querying procedures during the dates shown in Figure 3.

(U) Figure 3: CIA Reviews

UNCLASSIFIED

Approximate Dates of CIA Review	Minimization and Querying Reviewed
September to October 2020	01 June 2020 – 31 July 2020
November to December 2020	01 August 2020 – 30 September 2020
January to February 2021	01 October 2020 – 30 November 2020

(U) Figure 3 is UNCLASSIFIED.

(U) As a part of the typical 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

¹⁸ (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.

¹⁹ (U) Due to the coronavirus pandemic, the joint oversight team did not conduct onsite reviews at CIA during this reporting period. Instead, the joint oversight team conducted reviews of CIA’s application of its minimization and querying procedures remotely over a period of several weeks.

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

United States person information that have been minimized and retained by CIA and discusses 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.²⁰ In addition, NSD reviews CIA's written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications to assess whether those queries were compliant with CIA's querying procedure requirements that such queries are reasonably likely to return foreign intelligence information, as defined by FISA.

~~(S//NF)~~ CIA may receive dual-routed 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 reviews CIA's original source documentation [REDACTED]

[REDACTED] the results of those reviews 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 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) ~~(S//NF)~~ NCTC is authorized to receive unminimized Section 702 data and also has access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism. NCTC's processing, retention, and dissemination of such information is subject to its Section 702 minimization procedures. Unlike NSA, FBI, and CIA, NCTC does not directly engage in targeting or acquisition, nor does it nominate potential Section 702 targets to NSA. NCTC may receive dual-routed unminimized Section 702-acquired communications. Such communications must be minimized pursuant to NCTC's minimization procedures. NCTC has established internal

(U) ²⁰ ~~(S//NF)~~ Due to the sensitive nature of these disseminations, they must be reviewed in person at CIA. On 23 and 24 March 2021, representatives from NSD and ODNI conducted an onsite review at CIA of the disseminations from this reporting period.

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 NSA's targeting procedures can also involve CIA.

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

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

compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. As part of the joint oversight of NCTC's access, receipt, and processing of unminimized Section 702 information and minimized Section 702 information from FBI, the joint oversight team typically conducts onsite visits at NCTC, and the results of those visits are included in bimonthly NCTC review reports. However, due to the coronavirus pandemic, the joint oversight team conducted the bimonthly reviews during the review period remotely.

(U) The reviews focus on NCTC's application of its Section 702 minimization procedures 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, reviews of NCTC's application of its minimization and querying procedures were conducted on the approximate dates shown in Figure 4.

(U) Figure 4: NCTC Reviews

UNCLASSIFIED

Approximate Date of NCTC Review	Minimization and Querying Reviewed
July 2020	01 May 2020 – 30 June 2020
September 2020	01 July 2020 – 31 August 2020
November 2020	01 September 2020 – 31 October 2020
January 2021	01 November 2020 – 31 December 2020

(U) Figure 4 is UNCLASSIFIED.

(U) As a part of the reviews, 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 they contain United States person information, and discusses with personnel issues involving the proper application of NCTC's minimization procedures. The team also reviews all NCTC disseminations identified as containing United States person information acquired under Section 702. In addition, the joint oversight team reviews 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, throughout the reporting period 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.²² Investigations are coordinated through NCTC's Compliance and Transparency Group and NCTC Legal, a forward deployed component of 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.

²² (U) Insofar as NCTC reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve NCTC.

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

~~TOP SECRET//SI//NOFORN/FISA~~**(U) V. Interagency / Programmatic Oversight**

(U) Because the implementation and oversight of the Government's Section 702 authorities are multi-agency efforts, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence information, and comply with all legal requirements. For those reasons, NSD and ODNI generally lead calls and meetings on relevant compliance topics, including calls or meetings with representatives from all agencies implementing Section 702 authorities, so as to address interagency issues affecting compliance with the statute and applicable procedures.

(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, querying, or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review and, where appropriate, seek modifications of their targeting and minimization procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance.

(U) VI. Training

(U) In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have continued their training efforts to ensure compliance with the targeting, minimization, and querying procedures. During this reporting period, NSA continued to administer the compliance training course dated November 2016.²³ All NSA personnel who require access to Section 702 data are required to complete this course on an annual basis in order to gain or maintain that access. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders and compliance advisories to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. Those training reminders and compliance advisories are e-mailed to individual analysts and targeting adjudicators and maintained on internal agency websites where personnel can obtain information about specific types of Section 702-related issues and compliance matters.

(U) During this reporting period, FBI similarly continued implementing its online training programs regarding Section 702 nominations, minimization, querying, and other related requirements. Completion of those FBI online training programs is required of all FBI personnel

²³ (U) NSA released the transcript associated with this training, dated August 2016, in response to a Freedom of Information Act (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"). The transcript was posted, in redacted form, on *intel.gov* via ODNI's *IC on the Record* database on 22 August 2017. The transcript is titled *OVSC1203: FISA Amendments Act Section 702* (Document 17, NSA's Training on FISA Amendments Act Section 702). The November 2016 training is in the process of being revised, with an expected rollout in 2022.

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

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

who request access to Section 702 information. Prior to the pandemic, NSD and FBI also conducted in-person trainings at multiple FBI field offices. For example, NSD and FBI provided additional focused training at FBI field offices on the Section 702 minimization procedures, including training FBI field personnel on the application of the querying standard.

(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 enhance compliance with those procedures as well as statutory provisions of Section 702. This training was mandatory for FBI personnel who are authorized to access unminimized Section 702-acquired information. FBI conducted this training between November and December 2019. Users who did not complete this training by mid-December 2019 would have had their access to unminimized Section 702-acquired information temporarily suspended until they took the training. Information about more recent guidance developed by NSD and ODNI, and training on such guidance developed by FBI, is discussed below.

(U) During this reporting period, CIA provided targeted FISA training to attorneys it embeds with CIA operational personnel who regularly address FISA matters, and continued to provide FISA training to any attorney beginning an assignment that may involve the provision of legal advice on FISA matters. Additionally, CIA has a required training program for anyone handling unminimized Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA or minimize Section 702-acquired communications. Furthermore, CIA has issued guidance to its personnel about how to properly conduct United States person queries that are reasonably likely to return foreign intelligence information.²⁴

(U) 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 unminimized 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 unminimized Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed unminimized Section 702-acquired information in its system to confirm that those personnel who access unminimized Section 702-acquired information have received training on the NCTC Section 702 minimization and querying procedures.

²⁴ (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 *intel.gov* via the *IC on the Record* database on 11 April 2017, see ACLU April 2017 Production 5, Document 15 "CIA's United States Person Query Guidelines for Personnel."

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

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

(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 collection of this data has been compiled in order to identify overall trends in the agencies' targeting, minimization, and compliance.

~~(S//NF)~~
(U) This reporting period was again disrupted by the coronavirus pandemic. This section and Section 4 report trends compared with the previous reporting period. The joint assessment team believes many of the changes during this reporting period, as compared to reporting periods that preceded the pandemic, are attributable, at least in part, to the disruption [REDACTED] caused by the pandemic.

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

(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,²⁵ the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.²⁶

²⁵ (U) The provided number of facilities, on average, subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released by the ODNI in its *CY2020 Transparency Report*. The classified numbers estimate the average number of *facilities* subject to Section 702 acquisition at any given time during the reporting period, whereas the unclassified numbers provided in the Transparency Report estimate the number of Section 702 *targets* subject to acquisition throughout the reporting period. 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.

²⁶ (U) The two previous reporting periods in which the average number of facilities under collection decreased are not captured in Figure 5, as both occurred prior to 2015.

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

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

(U) Figure 5 is classified ~~SECRET~~

~~(TS//SI//NF)~~ NSA reports that, on average, approximately [redacted] facilities²⁷ were under collection pursuant to the applicable certifications on any given day during the reporting period. This represents a 1.2 percent increase from the approximately [redacted] facilities under collection on any given day in the last reporting period. The 1.2 percent increase is significantly lower compared with recent reporting periods; over the previous five reporting periods, the percentage increase ranged from 9.5 percent to 24.4 percent. [redacted]

~~(S//NF)~~ [redacted] certifications (2019-A and 2020-A); [redacted] certifications (2019-B and 2020-B); [redacted] certifications (2019-C and 2020-C). [redacted]

²⁷ ~~(TS//SI//NF)~~ The Government counts the tasking of [redacted] to ensure consistency with how it counts other tasked facilities.

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

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

(U) The above statistics describe the *average* number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.²⁸ Figure 6 charts the average monthly numbers of newly tasked facilities from 2015 through 2019 and the total monthly numbers of newly tasked facilities from January 2020 through November 2020.

(U) Figure 6: New Taskings by Month (Yearly Average for 2015 through 2019)

(U) Figure 6 is classified ~~SECRET~~

~~(S//SI//NF)~~ NSA provided documentation of approximately [REDACTED] new taskings during the reporting period. As noted elsewhere in this report, the continued decline from the previous reporting period [REDACTED]. However, as shown in Figure 6, the number of new taskings increased every month during this reporting period except for November 2020, and the number of new taskings in October and November were generally [REDACTED]. Previous joint assessments included metrics presenting the number of newly tasked facilities broken down by type of facility

²⁸ (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/FISA~~

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

(e.g., electronic communication accounts or telephony facilities). These metrics are not included in this joint assessment because the joint oversight team assesses that the fluctuations in the number of tasking decisions during the coronavirus pandemic make it difficult to discern meaningful trends.

(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. Figure 7 contains the classified number of serialized reports and reports identified as containing United States person information over the last 10 reporting periods. The joint oversight team reviews revealed that the United States person information was at least initially masked in the vast majority of circumstances.²⁹ The number of serialized reports NSA has identified as containing United States person information increased slightly when compared with the previous reporting period.

²⁹ (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/FISA~~

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

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



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

~~(S//NF)~~ For this reporting period NSA identified to NSD and ODNI approximately [REDACTED] serialized reports based upon minimized Section 702-acquired data. The overall number of reports identified by NSA was at the lowest level it has been over the past five years. The number of serialized reports identified as containing United States person information increased from [REDACTED] in the prior reporting period, to the current [REDACTED] but remains below pre-pandemic levels.³⁰

³⁰ (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/FISA~~

~~TOP SECRET//SI//NOFORN/FISA~~**(U) II. Trends in FBI Targeting**

(U) Under Section 702, NSA submits Designated Accounts to FBI 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 Designated Accounts. As detailed below, the number of Designated Accounts decreased significantly from the prior reporting period, which may be due, at least in part, to the coronavirus pandemic.

(U) As Figure 8 details, FBI approves the vast majority of NSA's Designated Accounts and the percentage of approved Designated Accounts has been consistently high across reporting periods. The high level of approval can be attributed to the fact that the Designated Accounts have already been evaluated and found to meet the NSA targeting procedures. FBI may not approve NSA's request for acquisition of a Designated Accounts for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the Designated Account 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 portion³¹ were rejected on the basis that they were ineligible for Section 702 collection.

(U) The yearly average number of Designated Accounts approved by FBI increased each year from 2016 through November 2019. The number of Designated Accounts approved by FBI each month in this reporting period has varied.

³¹ ~~(S//NF)~~ such accounts is rejected on the basis that it is ineligible for Section 702 collection.

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

~~(S//NF)~~ Figure 8:



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

~~(S//SI//NF)~~ FBI reports that NSA designated approximately [redacted] accounts [redacted] during the reporting period – an average of approximately [redacted] Designated Accounts per month.³² FBI approved approximately [redacted]³³ requests [redacted] during the reporting period. In the previous reporting period, NSA designated [redacted]

³² [redacted]

(U) ³³ ~~(S//NF)~~ As previously noted, beginning with the joint assessment covering the reporting period December 2017 through May 2018, the Government changed its counting methodology to ensure statistical accuracy for the number of designated accounts approved.

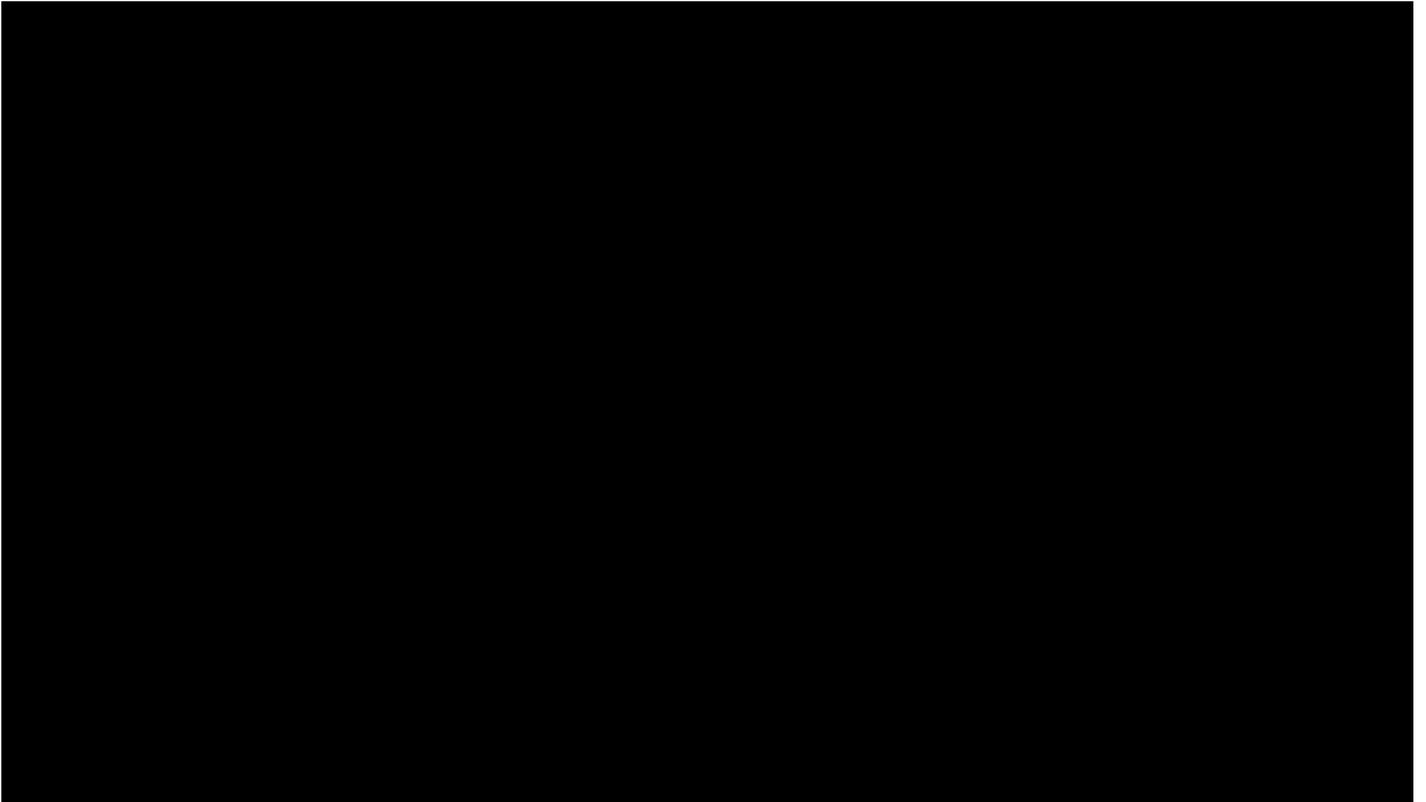
~~TOP SECRET//SI//NOFORN/FISA~~

approximately [REDACTED] accounts for [REDACTED] and the FBI approved approximately [REDACTED] requests. Figure 8 shows that both numbers declined substantially starting in April 2020 (but [REDACTED] generally increased again starting in July 2020), likely due, at least in part, to the pandemic. In addition, Figure 8 illustrates that in these same months, FBI approved more requests [REDACTED] than the number of accounts designated by NSA; this reflects FBI's continued processing of requests submitted by NSA in prior months.

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

(U) CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Figure 9 compiles the number of such disseminations of reports containing United States person information identified in the reporting periods from December 2015 to May 2016 through the current period of June 2020 to November 2020. 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.

(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. [REDACTED]
[REDACTED] CIA also permits some [REDACTED]

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

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

[REDACTED]

[REDACTED] As noted above, due to CIA initially cancelling all in-person visits in response to the coronavirus pandemic, NSD and ODNI were unable to review the referenced disseminations [REDACTED] to ensure compliance with CIA's minimization procedures during this reporting period. NSD and ODNI reviewed these [REDACTED] during a review that took place after the reporting period.

(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.³⁴ 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 acquired pursuant to Section 702. This current assessment reports the total number of files CIA transferred from June 2020 through November 2020. For reference, however, the number of files retained from prior reporting periods is also displayed in Figure 10. The percentage of retained or transferred files identified by CIA as potentially containing United States person information has remained consistently low.³⁵

³⁴ (S//NF) [REDACTED]

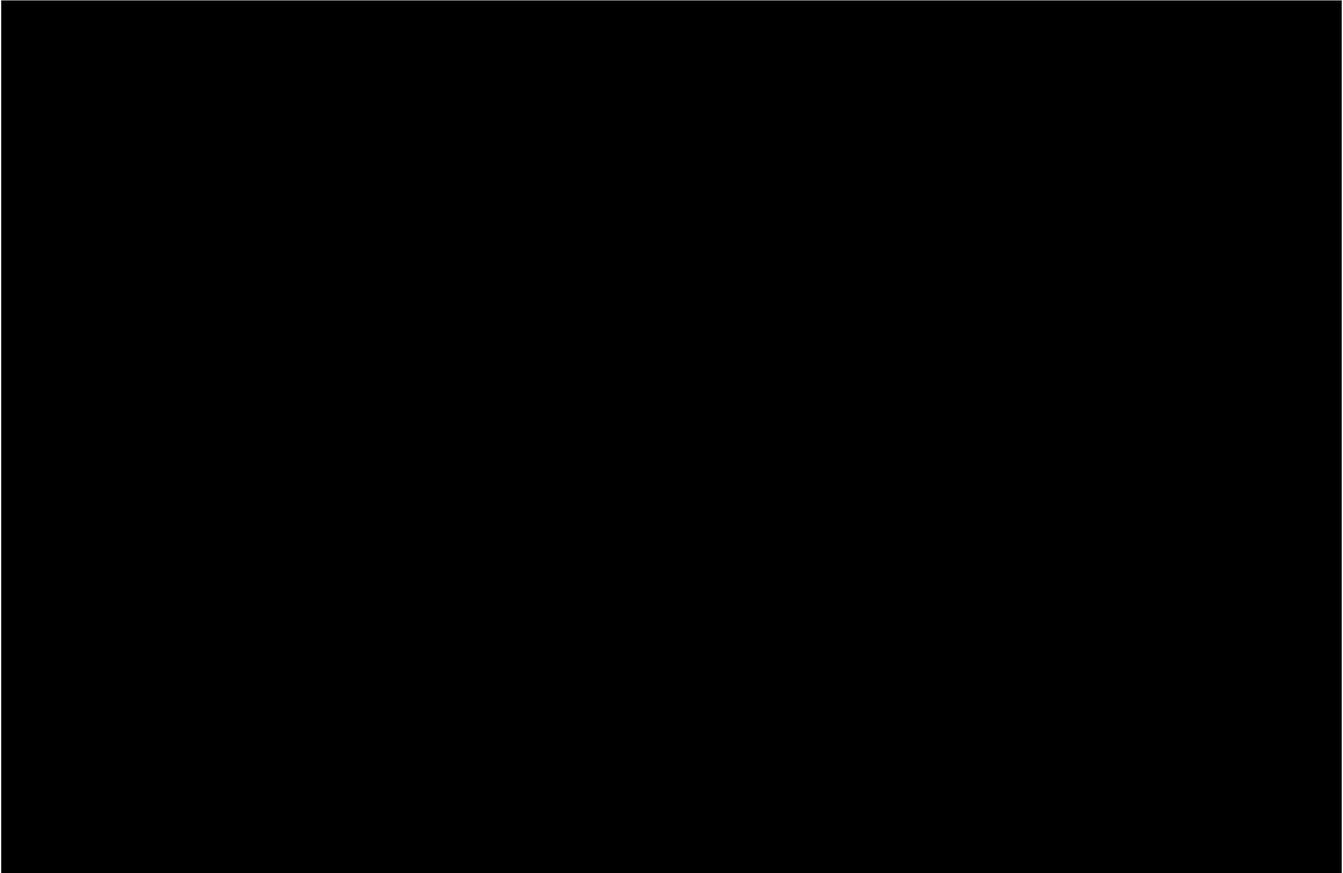
[REDACTED] In making those retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

³⁵ (S//NF) For this reporting period, CIA analysts transferred approximately [REDACTED] (2.8 percent) of which were identified by CIA as containing a communication with potential United States person information.

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

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

(U) Figure 10: Total CIA Files Retained or Transferred and Total CIA Files that Were Retained or Transferred which Contained Potential United States Person Information³⁶



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

(U) IV. Trends in NCTC Minimization

(U) 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 Figure 11. Starting in November 2018, NCTC identified and provided to NSD and ODNI only disseminations containing minimized United States person information, rather than all disseminations of Section 702-acquired information. Because NCTC only began obtaining unminimized Section 702-acquired data after the FISC approval of such in April 2017, there are only seven six-month periods to report in this assessment.³⁷ This current joint assessment reports that the number of disseminations containing minimized Section 702-acquired United States person information, while low, increased by 66.1 percent from the previous reporting period.

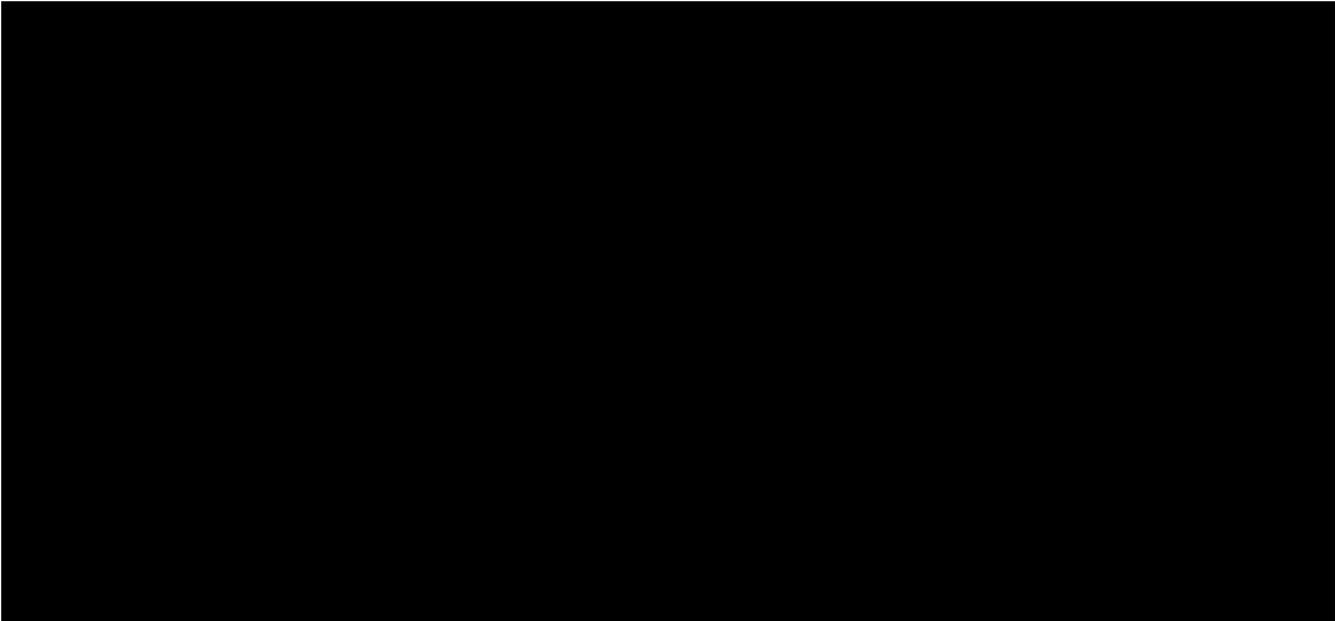
³⁶ ~~(S//NF)~~ [REDACTED]

³⁷ ~~(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 May [REDACTED]

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

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

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



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

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

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

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement their procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the Section 702 authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes.

(U) However, notwithstanding a focused and concerted effort by FBI personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying requirements continued to cause a significant number of query errors. While the number of FBI compliance incidents decreased compared to the previous reporting period, this assessment still reports a significant number of FBI compliance incidents related to querying.³⁸ Although reported to the FISC during this reporting period, some of these query incidents occurred prior to certain remedial steps taken by FBI at the end of 2019. In addition, these query incidents occurred prior to FBI's implementation in 2021 of corrective measures to mitigate the query compliance issues. These corrective measures are addressed further below.

(U) As noted in prior joint assessments, 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. For example, an "NSA compliance incident" could be caused by typographical errors contained in another agency's nomination to NSA for tasking.

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

³⁸ (S//NF) The number of FBI minimization and querying errors for the current reporting period was [REDACTED] compared to the [REDACTED] minimization and querying errors in the previous reporting period. All of the [REDACTED] minimization and querying incidents reported during this reporting period involved violations of the querying procedures; there were no violations of the minimization procedures reporting during this reporting period.

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

of such measures, some of which are detailed below, especially as it pertains to investigating whether additional or new system automation may assist in preventing compliance incidents.

(U) I. Compliance Incidents – General

(U) A. Statistical Data Relating to Compliance Incidents

(S//NF) As noted in the Section 707 Report, during this reporting period, there were a total of [REDACTED] compliance incidents that involved noncompliance with NSA’s targeting, minimization, or querying procedures and [REDACTED] compliance incidents involving noncompliance with FBI’s targeting, minimization, or querying procedures.³⁹ In addition, during this reporting period, there were [REDACTED] incidents of noncompliance with CIA’s querying procedures. There were [REDACTED] incidents of noncompliance with NCTC’s minimization and querying procedures. There were no 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 day⁴⁰ during the reporting period.

(U) Figure 12: Overall Compliance Incident Rate

~~SECRET~~ [REDACTED]

[REDACTED]	
(U) All compliance incidents during reporting period (01 June 2020 – 30 November 2020)	[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) 0.34 percent

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

³⁹ (U) As is discussed in the Section 707 report and below, 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 that such actions violated.

⁴⁰ [REDACTED]

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

(U) The 0.34 percent overall compliance incident rate represents a decrease from the 0.46 percent overall compliance incident rate in the prior reporting period. While this is an improvement over prior reporting periods, as with the previous incident rate, the current reporting period's overall compliance incident rate was predominantly impacted by FBI personnel misunderstanding the query standard in FBI's querying procedures. These incidents – including the remedies – are discussed in detail below. 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. Additionally, as noted elsewhere, this reporting period occurred during the coronavirus pandemic, and the joint oversight team is not able to determine to what extent the decrease in the overall compliance incident rate reflects a decrease in the actual number of compliance incidents – whether as a result of the pandemic or improvements in compliance – as opposed to difficulties in discovering and reporting compliance incidents.

(U) The number of notification delays substantially decreased during this reporting period. As discussed below, notification delays are incidents in which 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. If the notification delay incidents are not included in the calculation, the overall compliance incident rate for this reporting period remained the same (0.34 percent).

(U) The joint oversight team assesses that the compliance incident rate – with and without the notification delay incidents – remained low and is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting, minimization, and querying procedures. The joint oversight team also believes the compliance incident rate during this reporting period may have been lower than previous reporting periods, in part, because of the effects of the coronavirus pandemic.

(U) As it pertains to FBI querying incidents, the joint oversight team identified a significant number of non-compliant queries, though far fewer than in prior reporting periods. The joint oversight team believes that the suspension of NSD's FBI field office reviews in March 2020 was likely a significant factor in the decrease in identified incidents.⁴¹ Notably, NSD did not conduct query audits during this reporting period and conducted far fewer audits in all of 2020 than in past years. In 2020, NSD conducted query audits of only six field offices (none of which occurred during this reporting period), whereas NSD conducted query audits of 27 field offices in 2019 and 29 field offices in 2018. In prior reporting periods, these field office reviews were responsible for

(U)⁴¹ ~~(U//FOUO)~~ As discussed above, NSD generally conducts onsite reviews at FBI field offices. However, in response to the coronavirus pandemic, NSD temporarily suspended its onsite reviews in or about the middle of March 2020. NSD began conducting remote reviews in February 2021. During this reporting period, NSD did not conduct any field office reviews.

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

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

discovering the majority of FBI's query compliance incidents, including "batch queries," which have the potential to substantially affect the FBI query compliance incident rate as well as the overall compliance incident rate. The batch query function in a certain FBI system permits users to conduct multiple queries as part of a single batch job, meaning a single action can result in thousands of improper queries. Whether such a noncompliant batch job would or would not have been discovered in the temporarily suspended FBI field office reviews is unknown. As a result, the joint oversight team is unable to evaluate how FBI's compliance with its querying procedures during this reporting period compares to other reporting periods. NSD and ODNI do assess, however, that query issues were a pervasive compliance challenge during the period of time covered by this joint assessment based on the results of NSD's audits conducted during prior reporting periods, as well as the results of NSD's remote audits in 2021, which reviewed historical queries conducted throughout 2020.⁴² The joint oversight team continues to work with FBI to reduce non-compliant queries and improve training and guidance regarding this issue.

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

(U) While tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint, it remains an imperfect proxy. A flaw with using this particular proxy is that certain types of incidents included in the numerator do not 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 average number of tasked facilities as contained in the denominator compares closely similar factors – both are directly related to tasking and must meet the requirements of the targeting procedures. However, the factors are not similar when comparing an improper dissemination incident or an improper query (which are incidents resulting from non-compliance with minimization and querying procedures) to the average number of tasked facilities. Minimization and querying incidents implicate the requirements of the minimization and querying procedures, whereas the tasking of a facility implicates the requirements of the targeting procedures. In addition, the number of query and dissemination incidents that can occur in a reporting period are largely independent from the number of facilities tasked during a period, as queries and disseminations can involve facilities that are no longer tasked – or were never tasked – pursuant to Section 702, and multiple queries or disseminations can be made in relation to a single facility. Conceivably, minimization incidents should be compared to the number of total minimization actions, but the Government is currently unable to count or track minimization actions in that manner. Adding to the dissimilarity is that multiple agencies' (NSA, FBI, CIA, and NCTC)

(U) ⁴² ~~(U//FOUO)~~ As per standard practice for incident reporting, the results of these query audits will be included in the joint assessment reporting period in which the incidents are first reported to the FISC, rather than the reporting period in which they took place. The results from the 2021 query audits will be included in subsequent joint assessments.

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

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

incidents – as well as incidents by service providers – are counted in the overall compliance incident rate, but only two agencies (NSA and FBI) actually conduct targeting activity pursuant to their respective targeting procedures, and only NSA’s targeting activities are included in the denominator.

(U) As with prior reporting periods, the number of compliance incidents in the numerator that do not bear a relation to the denominator (in particular, FBI query errors) 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 0.34 percent overall compliance incident rate is an imperfect representation of the error rate for the Section 702 program during this reporting period, particularly in light of the impact of the pandemic on certain oversight reviews. Indeed, the joint oversight team considers the overall compliance incident rate to be artificially low for the prior and current joint assessment periods. As the imprecision of the overall compliance incident rate had been a persistent problem that predates the pandemic, and has been highlighted by the joint oversight team since at least the 19th Joint Assessment, the joint oversight team will discontinue reporting this overall compliance incident number in future assessments in favor of more specific compliance incident rates that have been developed and used in the last several joint assessments.

(U) These more specific compliance rates include the NSA targeting compliance incident rate (see Figures 14 and 15, first introduced in the 19th Joint Assessment); and a query error rate for FBI (see Figure 18, first introduced in the 21st Joint Assessment). The Government provides these additional metrics to advance the understanding of the incidents’ impact and the causes of those incidents. The joint oversight team also continues to research other metrics which may be indicative of compliance trends.

(U) Notwithstanding the issues discussed above, the current assessment provides the overall compliance incident rate in Figure 12 so that readers can see the size of the movements as compared to historical periods in order to place the number of FBI query errors reported during this reporting period in the context of a rate that has been used historically, as these query errors were the driving factor in the rate movements over the last few reporting periods.⁴³

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

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

⁴³ (U) Note that because of the imperfections described above, and because FBI query errors are only one factor in the overall compliance incident rate, a period-on-period comparison of the rate will still not provide an entirely accurate measure of the increases and decreases in FBI query errors.

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

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

(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.⁴⁴
- (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, minimization, or querying procedures and account for those incidents accordingly.

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

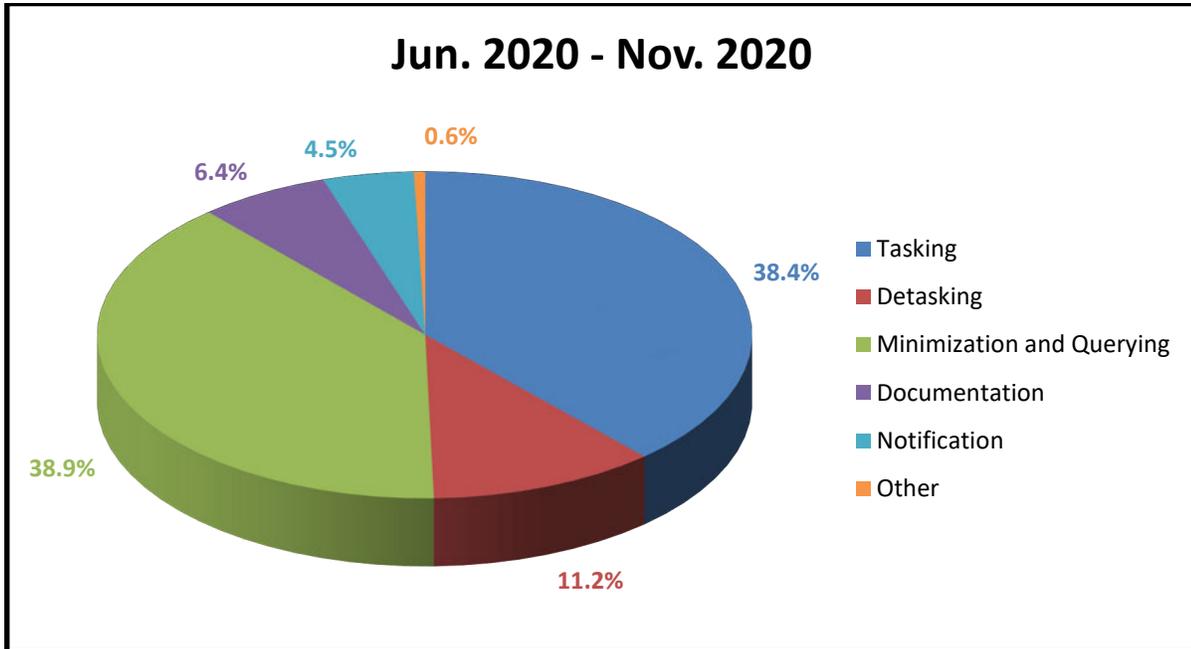
(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 13A depicts the percentage of NSA compliance incidents in each category that occurred during this reporting period, whereas Figure 13B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

⁴⁴ (U) A compliance incident may involve both a failure to meet the notification requirement and a substantive error (for example, a tasking or detasking error). However, in those instances, the substantive error was counted separate from the notification delay. For the majority of delayed notification incidents, the only incident of non-compliance was the failure to comply with the notification requirement.

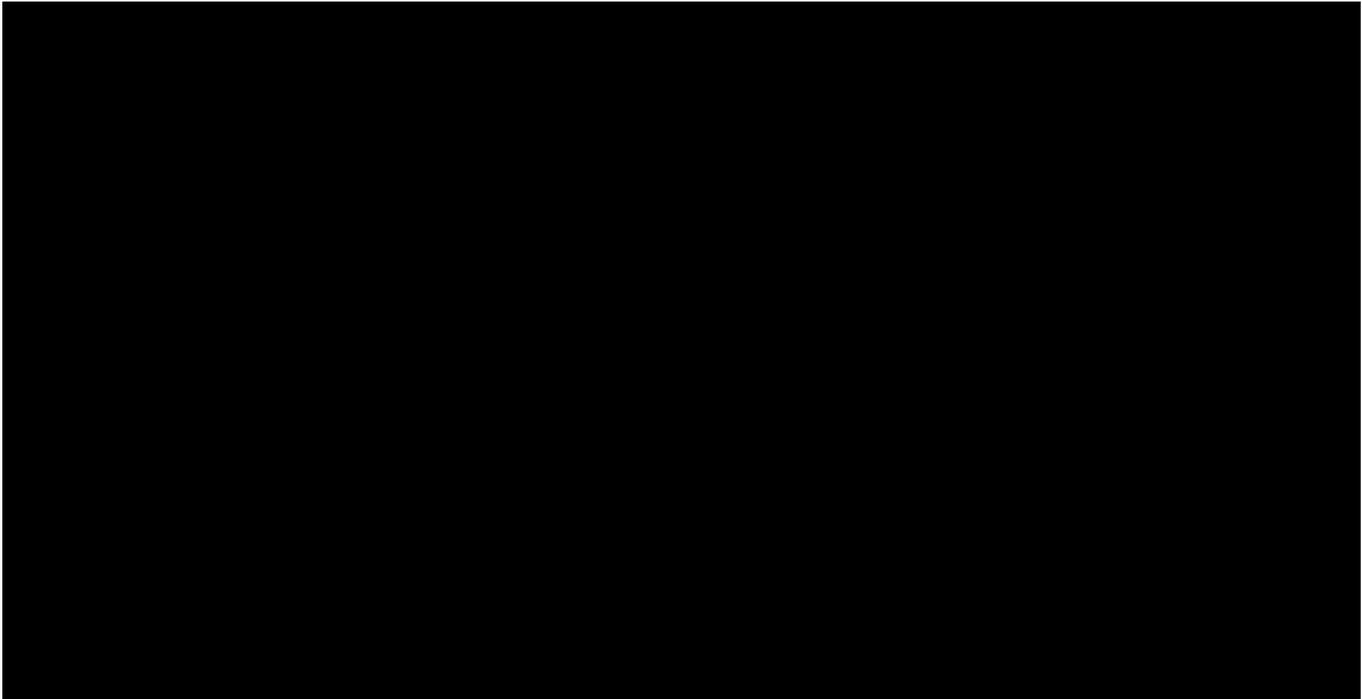
~~TOP SECRET//SI//NOFORN/FISA~~

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

UNCLASSIFIED



(U) Figure 13A is UNCLASSIFIED.

~~TOP SECRET//SI//NOFORN/FISA~~**(U) Figure 13B: Number of Compliance Incidents Involving the 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 errors accounted for the largest portion of incidents across all categories, followed closely by tasking errors. Detasking incidents accounted for the third largest percentage of incidents. 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 of reasons, especially as it pertains to more substantive tasking and detasking compliance incidents that can (but do not always) involve collection obtained from 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 and querying procedures because these types of incidents may involve information concerning United States persons.

~~(S//NF)~~ More specifically, the number of tasking incidents increased from [REDACTED]; detasking incidents decreased from [REDACTED]; minimization and querying incidents decreased from [REDACTED] documentation incidents decreased from [REDACTED]; and “other” category incidents decreased from [REDACTED]. The number of notification delays decreased from [REDACTED]. There were no overcollection incidents in this period or the prior 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

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

targeting compliance incident rate for this current reporting period. This metric compares similar factors: NSA’s number of “targeting incidents” (*i.e.*, the “numerator”) to the average number of 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, and overcollection incidents (if any). 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~~ [REDACTED]

[REDACTED]	
(U) NSA compliance incidents relating to NSA’s targeting procedures, during reporting period (01 June 2020 – 30 November 2020)	[REDACTED]
(U) Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
(U) NSA targeting compliance incident rate: Number of targeting incidents, divided by average number of facilities tasked to acquisition	(U) 0.05 percent

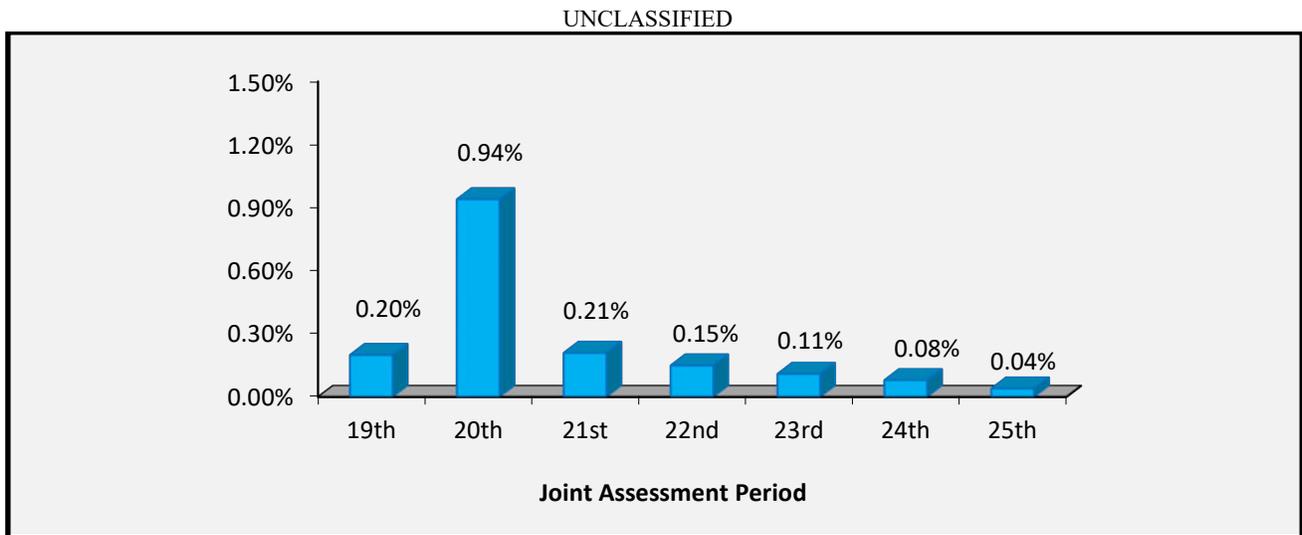
(U) Figure 14 is classified ~~SECRET~~ [REDACTED]

(U) This NSA targeting compliance incident rate percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may involve multiple facilities. Also, a single action may result in numerous incidents. 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) The joint oversight team has determined that excluding NSA’s notification delays incidents from the NSA’s targeting compliance incident rate provides another measure of compliance. Thus, Figure 15 shows an adjusted NSA targeting compliance incident rate of 0.04 percent, not including notification delay errors (as compared to 0.05 percent of NSA Targeting Compliance Incident Rate, including notification errors).⁴⁵

⁴⁵ (U) As described in prior joint assessments, the increase from 0.20 percent in the 19th reporting period to 0.94 percent in the 20th reporting period was primarily a result of one NSA office’s misunderstanding regarding how a targeting tool functioned, which resulted in an abnormally large number of targeting incidents.

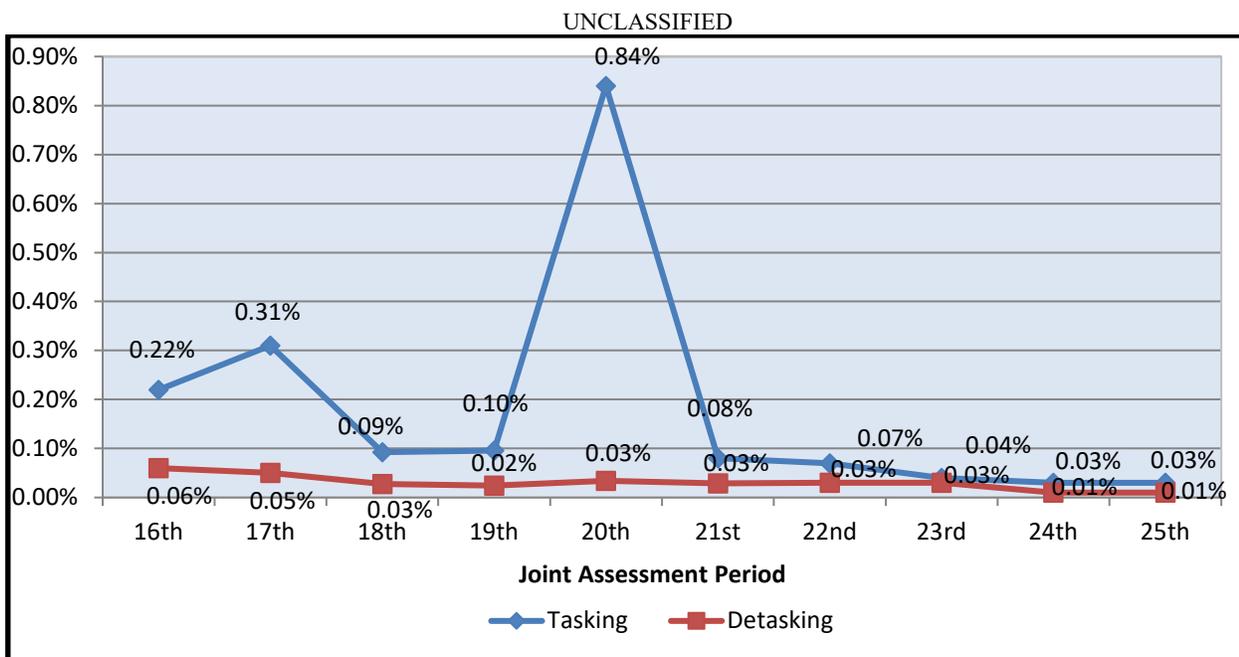
(U) Figure 15: NSA Targeting Compliance Incident Rate, *not* including Notification Delays



(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 rates compare the number of tasking errors and detasking delays, as applicable, to the average number of facilities on collection for the given reporting period. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other (*i.e.*, an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate).

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



(U) Figure 16 is UNCLASSIFIED.

(U) It is important to note that, while Figure 16 provides a visual representation of trends of non-compliance, the non-compliance rate is less than 1 percent. The tasking and detasking compliance incident rate has varied by fractions of a percentage point as compared to the average size of the collection.⁴⁶ The tasking incident rate remained 0.03 percent during this reporting period, which is historically low.⁴⁷ The tasking compliance incident rate involving facilities used by United States persons remained almost zero. The percentage of compliance incidents involving detasking incidents has also remained consistently low. The detasking compliance incident rate involving facilities used by United States persons was also close to zero.

⁴⁶ (U) Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have reasonably known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. Detasking errors often involve delays in detasking a facility that the Government learns is used by a United States person or an individual located in the United States, who may or may not have been the targeted user. In addition, a single detasking delay may involve multiple facilities that were not timely detasked.



⁴⁷ (U) As previously noted, the increase in the tasking incident rate reported in the 20th Joint Assessment was primarily due to a single NSA targeting office misunderstanding how to use a targeting tool.

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

(U) The total number of compliance incidents identified relating to FBI's targeting procedures increased slightly as compared to the last period. The number of errors relating to FBI's minimization and querying procedures decreased this reporting period. The joint oversight team believes that the temporary suspension of NSD's FBI field office reviews starting in mid-March 2020, due to the coronavirus pandemic, and the potentially related non-identification of extremely large batch query errors were significant factors in this decrease. In recent years, FBI field office reviews have been responsible for discovering a significant portion of FBI's minimization and querying incidents that are reported in each joint assessment. Because FBI field office reviews were suspended during this reporting period, incidents that would typically be discovered by NSD during those field office reviews would not have been discovered while the reviews were suspended.⁴⁸

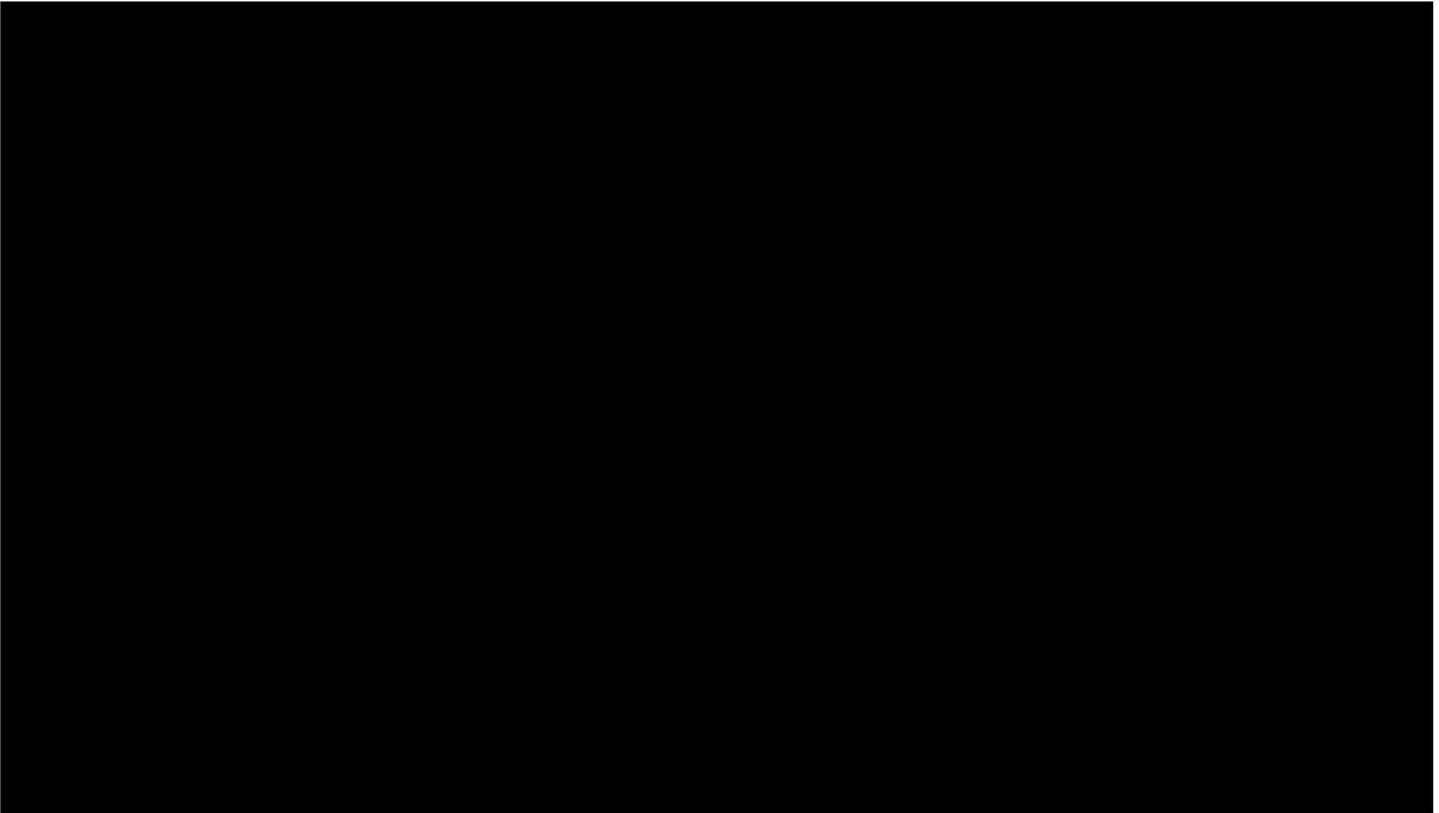
(U) Figures 17 and 18 show the classified number of incidents for the last 10 reporting periods (*i.e.*, from the 16th through the 25th reporting periods). The joint oversight team assesses that the increase in FBI errors beginning in the 19th reporting period is attributable to NSD's increased focus on reviewing FBI querying practices; this focus resulted in NSD's increased experience in evaluating those types of FBI queries and NSD's increased knowledge of FBI systems storing Section 702-acquired information. The joint oversight team believes that this increased focus and experience, along with other factors, resulted in NSD identifying a larger number of non-compliant queries.

⁴⁸ ~~(S//NF)~~ During this reporting period, [REDACTED] incidents of non-compliance with the FBI targeting, minimization, or querying procedures were identified, as compared to [REDACTED] incidents in the prior reporting period. Nearly all of these incidents pertain to non-compliant queries.

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

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

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



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

(U) During this reporting period, the FBI targeting compliance incident rate was 0.01 percent, a slight increase from the previous period (0.007 percent).⁴⁹ 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) Figure 18 provides the FBI query compliance incident rate, which is calculated as the total number of FBI query compliance incidents reported by NSD to the FISC during the reporting period, expressed as a percentage of the total number of FBI queries audited by NSD in connection with the field office reviews during which NSD identified the FBI query compliance incidents reported to the FISC during the reporting period. As noted above, due to the pandemic, NSD had suspended its query reviews during the entirety of this reporting period; the query reviews that

⁴⁹ ~~(S//NF)~~The FBI targeting compliance incident rate is calculated as the total number of FBI targeting errors reported during the reporting period, expressed as a percentage of the total number of facilities for which FBI approved a request during the reporting period. As noted above, the joint oversight team does not review all such approved requests. The joint oversight team only reviews checklists and supporting documentation relating to approved requests for which information was returned by FBI's database queries. In addition, during this reporting period, the joint oversight team only reviewed checklists and supporting documentation for a sample of such approved requests.

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

contributed to the FBI query compliance incident rate during this reporting period were all conducted prior to March 2020, but the query compliance incidents were first reported during this reporting period.

(U) Figure 18: FBI Query Compliance Incident Rate

~~SECRET//NOFORN~~

(U) FBI query compliance incidents reported to the FISC during the reporting period (01 June 2020 – 30 November 2020)	
(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	
(U) FBI query compliance incident rate: number of query incidents reported, divided by number of queries audited	(U) 2.2 percent

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

(U) The FBI compliance incident rate of 2.2 percent is an increase from the prior reporting period’s 0.82 percent, but a significant decrease from the 36.59 percent incident rate reported in the period before that. The number of improper FBI queries decreased by 41.78 percent during this reporting period, but the total number of queries audited by NSD decreased by 69.82 percent, a decrease attributable to the temporary suspension of reviews due to the pandemic, resulting in an increase in the FBI query compliance incident rate. While rates remain low, the joint oversight team assesses that query compliance continues to be a pervasive problem. NSD identified query compliance issues in each field office audited in calendar years 2019 and 2020.⁵⁰ And, since NSD resumed its query audits in 2021, NSD has continued to identify query compliance incidents during each field office remote audit. FBI implemented certain remedial measures in fall 2019 to address query compliance issues and, since that time, the joint oversight team has continued to work with FBI to take additional corrective actions to address the query compliance issues. The remedial measures undertaken by FBI are discussed further below.

(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

⁵⁰ (U) In 2018, NSD identified query compliance incidents in 26 of 29 field offices audited. In 2019, query errors were identified in all 27 field offices audited, and in 2020, query errors were identified in all six offices audited.

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

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. 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, those would be counted as two compliance incidents.

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

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

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

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

~~(S//NF)~~ There were [REDACTED] incidents during this reporting period that involved CIA's querying procedures,⁵¹ a decrease from the [REDACTED] incidents reported in the previous reporting period that involved its procedures. The joint oversight team assesses that CIA's compliance is a result of its training, systems, and processes that were implemented to ensure compliance with Section 702 and its minimization and querying procedures and the work of its internal oversight team.

⁵¹ (U) Recall that CIA does not have targeting procedures and may not target. Because CIA only has minimization procedures and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

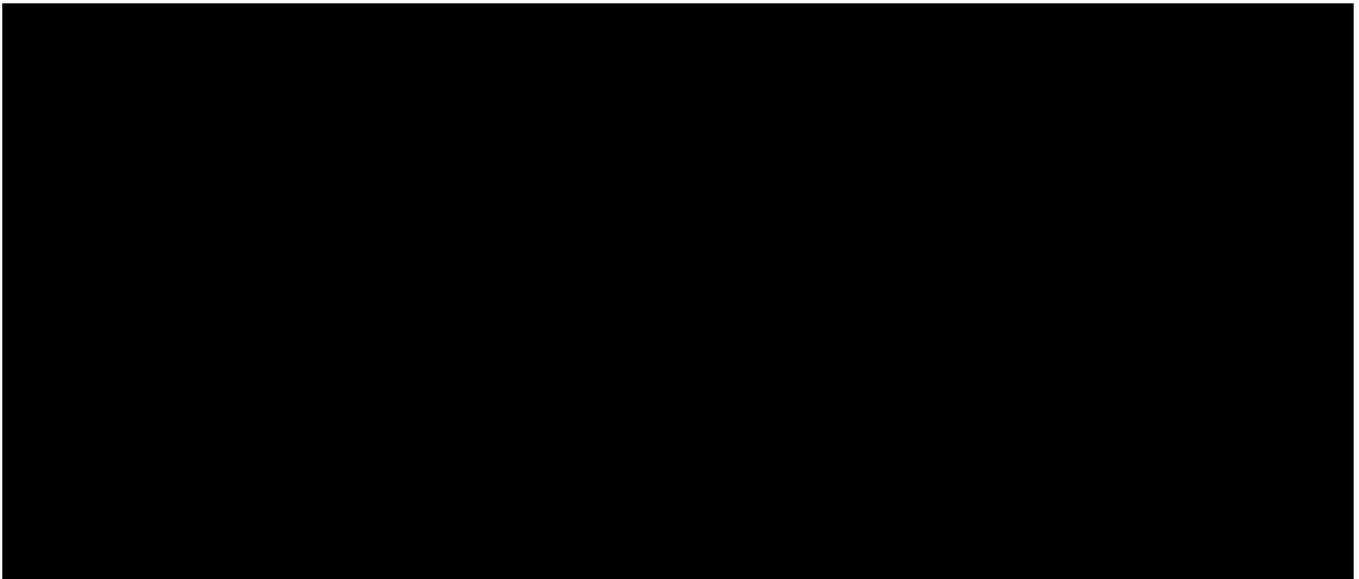
~~TOP SECRET//SI//NOFORN/FISA~~

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

~~(S//NF)~~ There were [REDACTED] incidents during this reporting period that involved NCTC's minimization and querying procedures, which is an increase from the zero incidents reported for the previous reporting period.⁵² The joint oversight team assesses that NCTC's overall compliance is a result of its training, systems, and processes that were implemented when NCTC was authorized to receive certain unminimized Section 702-acquired information.

(U) Figure 19 provides the classified number of minimization and querying errors that involved CIA for the last 10 reporting periods and NCTC for reporting periods beginning with the 19th assessment period.

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



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

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

(U) ~~(S//NF)~~ Finally, there were no incidents of non-compliance caused by errors made by communications service providers in this reporting period, which is the same as in the prior reporting period. The joint oversight team assesses that the generally low number of errors by the communications service providers across reporting periods 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.

⁵² (U) Recall that NCTC does not have targeting procedures and may not target. Because NCTC only has minimization procedures and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

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

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

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

(U) As with prior joint assessments, 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. For each individual incident, the Section 707 Report provides details as to how any erroneously acquired, disseminated, or queried information was handled through various purge, recall, and deletion processes. Information is also provided about personnel remediation and, when applicable, wider training efforts to address incidents. In certain instances, processes or technical tools are adjusted, as appropriate, to remedy the incidents, to mitigate impact, and to reduce the potential for future incidents.

(U) The joint oversight team believes that analyzing the trends of those incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance. The joint assessment primarily focuses on incidents involving NSA's targeting, minimization, and querying procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA's targeting, minimization, and querying procedures.

(U) The NSA compliance incident rate for this reporting period (calculated as the total number of compliance incidents involving NSA's Section 702 procedures, *divided by* the average number of tasked facilities) is 0.07 percent and represents a decrease from the NSA compliance incident rate of 0.10 percent in the previous reporting period.

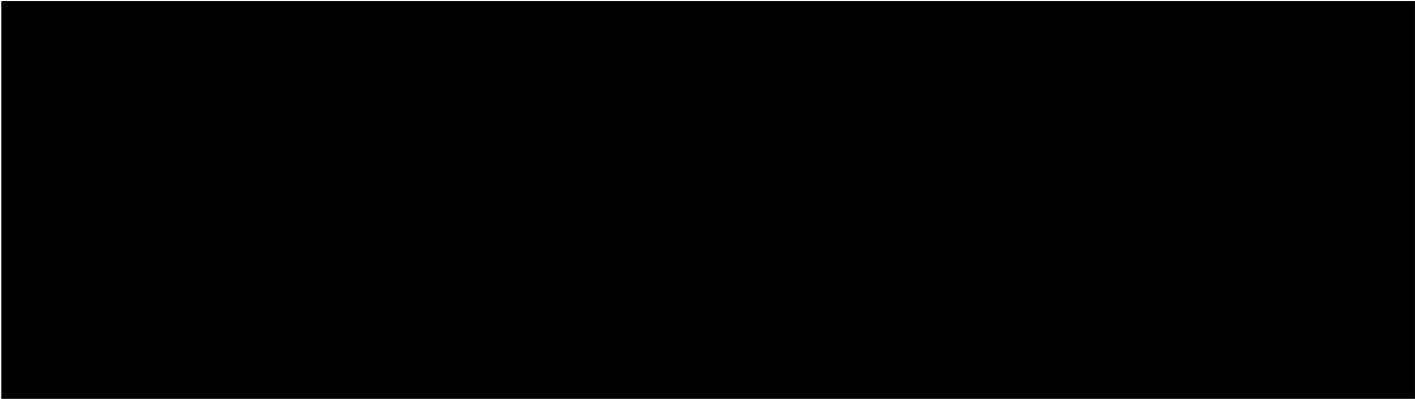
(U) Most of those incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or improper queries which were not reasonably likely to return foreign intelligence information due to their design. Regardless of United States person status, robust oversight is conducted to ensure compliance with all aspects of the targeting, minimization, and querying procedures; all identified incidents are reported to the FISC and to the Congress, and all incidents are required to be appropriately remedied. As with all incidents, the joint oversight team works closely with NSA to identify causes of incidents in an effort to prevent future incidents, regardless of United States person status.

(U) In the subsections that follow, this joint assessment examines some of the underlying causes of incidents of non-compliance. This joint assessment begins by examining and explaining incidents impacting United States persons' privacy interests, even though those incidents represent a minority of the overall incidents. This joint assessment then discusses other types of human errors and communication issues. The joint oversight team believes that analyzing the trends of these incidents, especially with regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance.

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

(U) A primary concern of the joint oversight team is the impact of certain compliance incidents on United States persons. United States persons were primarily impacted by (1) tasking

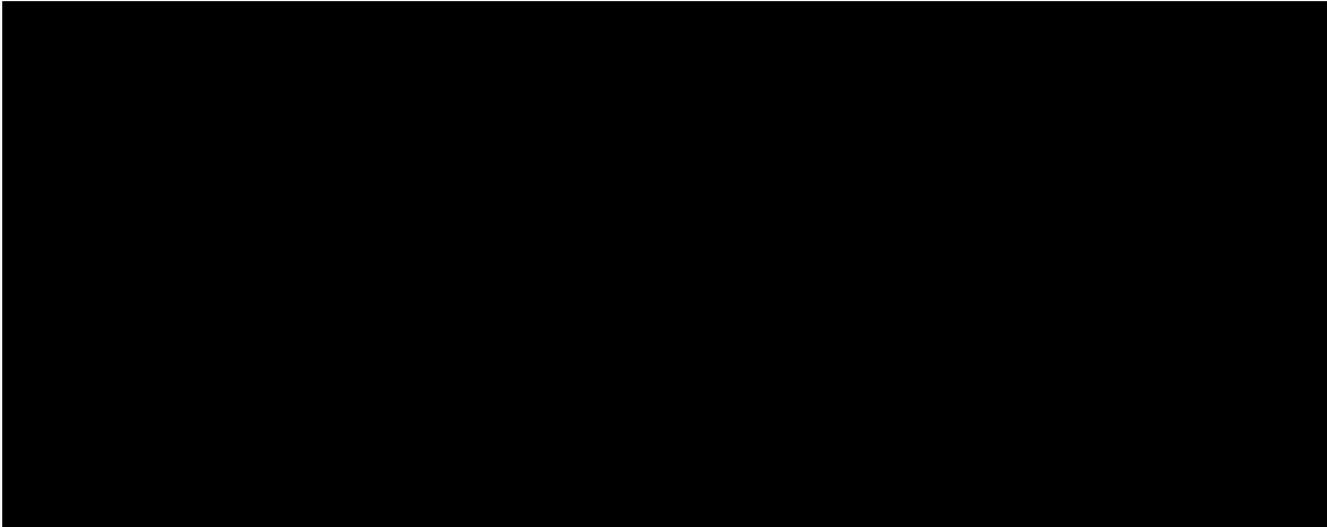
~~TOP SECRET//SI//NOFORN/FISA~~

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

(U) These incidents represent isolated instances of insufficient due diligence and did not involve an intentional effort to target a United States person. 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. In all of the incidents, personnel were reminded of the Section 702 tasking requirements, and the collection was purged as required by NSA's targeting and minimization procedures.

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

(U) Twenty-five percent of the total number of detasking delays involved facilities used by a United States person.⁵⁶ This percentage represents a significant increase from the previous three reporting periods, which reported rates in the range of 4 to 8 percent.



(U) The other detasking delay incidents impacting United States persons in this reporting period were caused by unintentional human errors (*e.g.*, misunderstandings of the detasking

⁵⁶ 

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

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

requirements and analysts' faulty analysis of information that erroneously led them to continue to assess that the target was a non-United States person located outside the United States). In all of the incidents, personnel were reminded of the Section 702 detasking requirements, any applicable collection was purged, and no reporting was identified based on the collection.

(U) B. Effect of Human Error

(U) Unlike in the immediately prior section, which focused exclusively on incidents impacting United States persons, this section addresses incidents that impacted *both* United States persons and non-United States persons. Each of the agencies has established processes to both reduce human errors and to identify such errors when they occur. Some human errors, such as those resulting from misunderstanding the rules and procedures, can be mitigated with additional training and guidance. These processes and trainings have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated.

(U) (1) Tasking & Detasking Errors

(U) This section discusses some of the common types and causes of tasking errors and detasking delays from this reporting period, along with the corresponding compliance trends.⁵⁷

- (U) The majority of the detasking delays during this reporting period involved (i) non-United States persons who either traveled to the United States or appeared to have traveled to the United States, or (ii) unexplained indications that a Section 702-tasked account appeared to have been accessed from within the United States.
- (U) “Foreignness determination” errors – Certain tasking errors result from NSA not properly establishing a sufficient basis to assess that a target was located outside the United States (otherwise referred to as the “foreignness determination”) or not sufficiently addressing conflicting information that calls into question whether a target was located outside the United States. During this reporting period, approximately 8 percent of tasking errors were the result of insufficient foreignness determinations (an increase from the previous reporting period, which reported approximately 5 percent of these tasking errors).⁵⁸ Certain of these incidents involved the failure to conduct a necessary foreignness check prior to tasking, or involved too long of a delay between the necessary foreignness checks and the tasking of the facility. In many of these incidents, NSA advised that it acquired no data from the erroneous tasking; however, if data was acquired, it was purged.
- (U) “Foreign intelligence information purpose” errors – Certain tasking errors result from NSA’s failure to establish a valid “foreign intelligence information purpose” for the tasking (*i.e.*, that the targeted user is reasonably expected to possess, receive, and/or

57

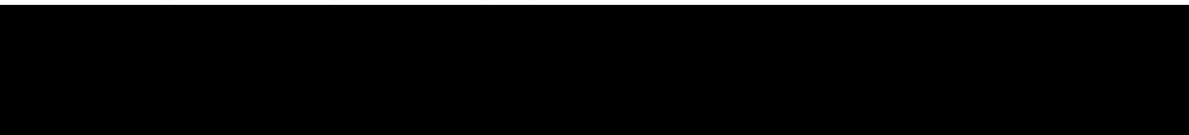
58

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

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

is likely communicate foreign intelligence information as defined in 50 U.S.C. § 1801(e)) in relation to the categories of foreign intelligence information specified in the Section 702 certifications. During this reporting period, approximately 31 percent were the result of NSA not having a sufficient foreign intelligence purpose for the tasking (an increase from the previous reporting period which reported 16 percent).⁵⁹ The joint assessment team attributes the increase from the previous period to a few tasking decisions involving multiple facilities. In 86 percent of these incidents, NSA advised that there is no indication that the facilities were used by a United States person or by someone in the United States. Any erroneously collected information was purged, and no reporting was identified.

- (U) Typographical errors – During this reporting period, approximately 13 percent of tasking errors involved such typographical or similar errors (a decrease from 20 percent in the previous reporting period). In each case, NSA advised that there was no indication that the relevant facilities were used by a United States person or by someone in the United States. NSA and CIA further advised that each had completed any required purges and had identified no reporting based on this collection.⁶⁰
- (U) Incorrect providers – Certain tasking errors result from NSA inadvertently tasking a facility to an incorrect provider. During this reporting period, approximately 1 percent of tasking errors involved tasking a facility to an incorrect provider (a decrease from 3 percent in the previous reporting period). NSA, CIA, and FBI advised that they each completed any required purges, and that each has identified no reporting based on this collection.
- (U) Incomplete detaskings – Certain detasking delays result from NSA detasking (or another agency requesting that NSA detask) some, but not all, of a target's facilities. During this reporting period, 10 percent of detasking delays involved such incidents where certain of a target's facilities were not timely detasked (a decrease from 22 percent in the previous reporting period). Again, any data acquired as a result of such detasking errors is required to be purged.



- (U) Non-existent facilities – Approximately 10 percent of detasking delays occurred because the relevant provider indicated that a tasked facility did not exist, but NSA or another agency did not promptly detask the facility.

(U) As noted above, some of the above tasking and detasking errors were caused by personnel misunderstanding or misapplying the rules or procedures related to tasking or detasking, while others were caused by inadvertent human errors. In each case, the relevant agency had

59

60

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

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

advised that it reminded its personnel about the Section 702 tasking and detasking requirements, or to exercise care when completing tasking and detasking processes, as applicable.

(U) (2) *Minimization and Querying Errors*

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

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

- 1) NSA's Section 702 querying procedures in effect during this reporting period required 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,⁶¹ it constituted a compliance incident, regardless of whether the query term used a non-United States person identifier or a United States person identifier.
- 2) Although NSA's Section 702 querying procedures in effect during this reporting period permitted queries of unminimized Section 702 collection using United States person identifiers, such queries *must be approved by NSA OGC*. If an NSA analyst used a United States person identifier that had not been approved by NSA OGC to query Section 702-acquired data, it constituted a compliance incident.

(U) During this reporting period, NSA minimization and querying incidents accounted for 39 percent of all NSA incidents of noncompliance, as compared to 23 percent from the previous reporting period.⁶² The total number of minimization and querying incidents remained relatively stable during this reporting period; the joint oversight team assesses that the increase in the percentage is due to the decrease in the total number of incidents during this reporting period. As with prior joint assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization and querying procedures. In the previous reporting period, approximately 88 percent of NSA's minimization and querying incidents involved improper queries. During this reporting period, out of all of NSA's total minimization and querying errors, approximately 94 percent involved improper queries, of which:

⁶¹ (U) For example, this type of query error occurs when an analyst mistakenly inserts an "or" instead of an "and" when constructing a Boolean query, resulting in an improperly tailored query that would potentially receive overly broad results and was unlikely to retrieve foreign intelligence information.

⁶² ~~(S//NF)~~ Minimization incidents decreased slightly to [REDACTED] incidents in the previous reporting period.

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

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

- (U) Approximately 40 percent of the minimization and querying errors involved queries that were not reasonably likely to return foreign intelligence information.⁶³
- (U) Approximately 54 percent of the minimization and querying errors involved NSA analysts conducting queries using a United States person identifier without approval.⁶⁴

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

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

(U) Dissemination Rules: NSA's minimization procedures set forth requirements for the dissemination of United States person information. In the current reporting period, incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in NSA's minimization procedures represented approximately 4 percent of the total number of minimization and querying incidents (compared to 8 percent of minimization and querying incidents during the last reporting period).⁶⁵ Improper disseminations of United States person information are usually the result of a human error oversight, generally because United States person information that is not necessary to understand foreign intelligence information is included in the dissemination. For example, in one instance, NSA issued a report that included an attachment with the name of a United States person whose identity was not necessary to understand foreign intelligence information.⁶⁶ While the United States person identity was appropriately masked in the text of the report, it was not masked in the report's attachment. NSA recalled the report and did not reissue it and advised that the relevant personnel have been reminded of the Section 702 dissemination requirements. Another dissemination was improper because the dissemination of United States person information was distributed to a broader group of recipients than is permitted by NSA's Section 702 minimization procedures. The joint oversight team has reviewed the human errors that caused the dissemination errors during this reporting period and has not identified any discernible patterns in the types or causes of these errors.

⁶³ (TS//SI//NF) There were [REDACTED] such non-compliant queries during this reporting period, compared to [REDACTED] in the previous reporting period.

⁶⁴ (S//NF) There were [REDACTED] United States person query incidents involving NSA during this reporting period, compared to [REDACTED] in the previous reporting period and [REDACTED] two reporting periods ago. All [REDACTED] incidents involved NSA analysts using United States person identifiers that had not been approved to query Section 702-acquired data.

⁶⁵ (S//NF) There [REDACTED] incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in the NSA SMPs, compared to [REDACTED] in the previous reporting period.

⁶⁶ [REDACTED]

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

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

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

~~(S//NF)~~ Access Restriction Rules: There were [REDACTED] incidents during this reporting period involving improper access, or potential access, to information acquired pursuant to Section 702 by individuals without the proper access credentials and training. According to NSA's Section 702 targeting procedures, unminimized Section 702-acquired data must be stored in authorized repositories and accessed only by authorized personnel. [REDACTED] NSA issued a report containing unminimized Section 702-acquired information to unauthorized individuals.⁶⁷ The error occurred because the responsible NSA analyst disseminated the report, which was intended to be internal to NSA, to another Government agency. NSA advised that all unauthorized recipients have confirmed that they deleted the relevant information [REDACTED] files containing unminimized Section 702-acquired information were saved to a directory accessible to individuals not authorized to handle unminimized Section 702-acquired information.⁶⁸ When NSA discovered the error, NSA moved the files to an appropriate directory that same day. NSA advised that the relevant personnel have been reminded of the Section 702 data access requirements.

(U) (3) *Other Errors*

(U) Documentation Errors: The NSA targeting procedures require that for each tasked facility NSA document the source of the "foreignness determination" and identify the foreign power or foreign territory about which NSA expects to obtain foreign intelligence information. The targeting procedures also require a written explanation of the basis for assessment, at the time of targeting, that the target is expected to possess, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked. The number of documentation errors decreased to approximately 6.4 percent of the total number of compliance incidents in this period from 30.1 percent in the prior reporting period.⁶⁹ While this represents a significant decrease in documentation errors, that decrease is due almost entirely to NSD's internal processes for identifying and reporting documentation errors. Implementation of those processes was slowed as a result of the coronavirus pandemic. 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 information 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.

67 [REDACTED]

68 [REDACTED]

⁶⁹ ~~(S//NF)~~ [REDACTED] incidents resulted from documentation errors, representing a significant decrease from the last reporting period, [REDACTED]. The number of documentation errors resulting from the tasking of a facility to a different DNI/AG Section 702(h) certification than intended remained a relatively large percentage of documentation errors but decreased to [REDACTED] in the prior reporting period.

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

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

(U) Notification Delays: Finally, there were a number of reported incidents where NSA failed to timely provide the required notice to NSD and ODNI after NSA has discovered that a tasked selector was used from within the United States or by a United States person. Notification errors decreased significantly, composing 4.5 percent of NSA compliance incidents in this reporting period, a decrease from 19 percent in the last reporting period.⁷⁰ The significant decrease in the number of reporting delays during this reporting period was due in large part to modifications to the reporting requirement to accommodate staffing issues related to the coronavirus pandemic.

(U) C. Inter-Agency and Intra-Agency Communications

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

(U) In this reporting period, approximately 31 percent of the detasking delays were attributable to miscommunications or delays in communicating relevant facts.⁷¹ This is a substantial increase from the last reporting period (14.6 percent), though the overall number of such incidents decreased significantly as compared to the prior period. The joint oversight team assesses that there is still room to improve agency communication. The detasking delays caused by miscommunications typically involved travel or possible travel of non-United States persons to the United States.

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

⁷⁰ ~~(TS//SI//NF)~~ There were [REDACTED] reporting delays in this reporting period, and in [REDACTED] of the incidents the only violation was a failure to provide the required notice to NSD. These reporting delays ranged from one to 232 business days, with an average delay of approximately 126 business days and a median delay of approximately 202 business days.

⁷¹ ~~(S//NF)~~ There were [REDACTED] such incidents in this reporting period, a reduction from the [REDACTED] reported in the previous period.

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

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

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

(U) There was a decrease in the number of incidents involving noncompliance with the FBI targeting, minimization, and querying procedures. However, as with the previous reporting period, a large majority of those incidents involved querying errors.⁷²

(U) A. Targeting Incidents

~~(S//NF)~~ During this reporting period, there were [REDACTED] incidents involving non-compliance with FBI's targeting procedures, [REDACTED] from the previous reporting period.⁷³ In one case, FBI personnel approved a request [REDACTED] from a Designated Account prior to completing all searches of FBI systems required by the FBI targeting procedures. The other [REDACTED] incidents involved FBI's improper approval of [REDACTED] from accounts without properly taking into account that the facilities [REDACTED] potentially inappropriate for tasking pursuant to Section 702. In all of the incidents, FBI personnel were reminded of the Section 702 requirements for tasking.

(U) B. Minimization and Querying Incidents

(U) With respect to FBI's minimization and querying procedures, the total number of compliance incidents decreased from the previous reporting period and remained relatively low, as compared to recent periods.⁷⁴ As discussed above, the joint oversight team believes that the reduction in compliance incidents is, in part, due to the suspension of reviews at FBI field offices.⁷⁵ Details about remedial actions are provided below. In general, personnel involved in these compliance incidents were reminded of the requirements under FBI's querying procedures.

⁷² ~~(S//NF)~~ As noted above, [REDACTED] compliance incidents involved violations of FBI's targeting, minimization, or querying procedures. Out of the total FBI compliance incidents for this reporting period, only [REDACTED] were targeting errors, and the remaining [REDACTED] were querying errors. Because FBI field office reviews were suspended during this reporting period, incidents that would typically be discovered by NSD during those field office reviews would not have been discovered while the reviews were suspended. In addition, because FBI field office reviews were suspended, the joint oversight team is also unable to evaluate whether changes to FBI systems and procedures have resulted in improved compliance.

⁷³ [REDACTED]

⁷⁴ ~~(S//NF)~~ The number of minimization and querying errors for the current reporting period was [REDACTED] all of which involved querying errors, compared to [REDACTED] in the previous reporting period.

⁷⁵ (U) In response to the coronavirus pandemic, NSD and ODNI temporarily suspended reviews at FBI field offices during this reporting period. In recent years, these field office reviews had been responsible for discovering a significant portion of FBI's minimization and querying incidents that are reported in each Section 707 Report. As a result, incidents that would typically be discovered by NSD during those field office reviews were not discovered during this reporting period. FBI's minimization and querying incidents discussed in this joint assessment were first reported to the FISC during this reporting period, but certain of those incidents were discovered in connection with field office reviews conducted during prior reporting periods. In February 2021, NSD resumed its audits of queries conducted by FBI personnel; these audits are being conducted remotely due to the pandemic. Any incidents discovered will be discussed in future joint assessments.

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

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

(U) (1) *Batch Query Errors*

~~(S//NF)~~ During prior reporting periods, NSD identified noncompliant batch queries conducted by FBI personnel that resulted in thousands of noncompliant queries attributable to a single decision by a user. As described in prior joint assessments, because a certain FBI system permits users to conduct multiple queries as part of a single batch job, a single action can result in thousands of improper queries. For example, if a user wanted to conduct a query based on 100 e-mail accounts that had been in contact with a FISA target, the user could use the batch query tool, which would result in 100 queries being conducted using each e-mail account as a query term. In these incidents, although the FBI analysts conducted the queries for work-related purposes, such as attempts to investigate threats, the analysts misunderstood the application of the query requirements. Thus, as the FISC explained in its October 2018 opinion, “a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including United States persons.”⁷⁶ To address batch query compliance incidents where a single improper decision or assessment by FBI personnel results in noncompliant queries corresponding to a large number of individuals, subsequent to the reporting period, FBI imposed a requirement that individual queries conducted using the batch query tool [REDACTED] of 100 or more identifiers require FBI attorney approval prior to the queries being conducted. This change became effective [REDACTED] as of June 2021. Further remedial steps applicable to all queries, including batch query incidents, are discussed in a subsection below.

~~(S//NF)~~ (U) Unlike prior reporting periods, there was no single large batch query responsible for most of the FBI querying incidents. During this reporting period, NSD identified one noncompliant batch job involving [REDACTED] queries. This batch job was conducted in connection with an FBI predicated criminal investigation. These queries were not reasonably likely to return foreign intelligence information or evidence of a crime. This batch query incident was a result of personnel misunderstanding the query requirements.

(U) (2) *Other Query Errors Caused by Misunderstandings of the Query Standard or a Lack of Awareness that a Query Would Run against FISA-Acquired Data*

(U) During this reporting period, most of the improper query incidents resulted from FBI personnel misunderstanding the querying rules even though the queries were conducted for work-management purposes or work-related purposes. These queries were not, however, reasonably likely to retrieve foreign intelligence information or evidence of a crime and, thus, constituted incidents. In most of the instances, FBI personnel did not fully understand the application of the query rules.

(U) 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. This is particularly the case with respect to query incidents that have been identified with queries run in a specific FBI database that contains non-FISA acquired and unminimized FISA-acquired information. As a result, for these queries, FBI personnel did not think

⁷⁶ (U) See the FISC’s 18 October 2018 Opinion and Order at 68.

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

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

to apply the query standard to their proposed queries before conducting queries in that particular FBI database, or failed to opt out of conducting queries against unminimized FISA-acquired information.

(U) For example, some of the improper queries involved FBI personnel conducting queries, including using United States person identifiers, to research prospective law enforcement personnel or potential sources without a reasonable basis to believe the queries would be likely to return foreign intelligence information or evidence of a crime.⁷⁷ These and other similar query compliance incidents during this period were due to personnel conducting queries to vet individuals or entities for any derogatory information. NSD has observed this common scenario in numerous query compliance incidents in this, as well as prior and subsequent reporting periods. These types of queries can impact United States persons.

(U) FBI personnel also conducted queries that, while reasonably likely to return foreign intelligence information, were overly broad as constructed.⁷⁸ In all of these incidents, FBI personnel misunderstood the application of the query rules, and they were subsequently reminded of how to correctly apply the query rules.

~~(S//NF)~~ A change that FBI implemented subsequent to this reporting period, to make [REDACTED] a default opt-out for searches of FISA-acquired information, is designed to prevent incidents that occur because FBI personnel were unaware that their queries would be running against unminimized FISA-acquired information. At the time the relevant queries were conducted, [REDACTED]

⁷⁷ ~~(S//NF)~~ In one incident, an intelligence analyst conducted approximately [REDACTED] queries [REDACTED] using the names of new police officers to be deputized. [REDACTED] In another example, FBI conducted queries using the names and other identifiers of an individual who had applied to work at FBI as a linguist, an individual who was in contact with that applicant, and an individual from a foreign country who had listed the applicant as a point of contact on the person's application for a non-immigrant visa. [REDACTED] In a third example, personnel at an FBI field office conducted approximately [REDACTED] improper queries. [REDACTED] of the improper queries were conducted using the identifiers of FBI bomb technician candidates, potential sources, task force officers identified to work on an FBI joint task force, FBI job applicants, and a visitor to an FBI field office. In each case, the queries were conducted to determine if there was any derogatory information on the individuals, but, at the time of the queries, there was no reason to suspect that FBI would have any such derogatory information, and the relevant personnel did not realize that these queries would run against raw FISA-acquired information. In addition, [REDACTED] of the improper queries were conducted using the identifiers of individuals identified as potential employees of critical infrastructure systems as part of FBI's [REDACTED]. The queries were conducted to ensure that all applicants met the criteria for [REDACTED], but the individual conducting the queries had no reason to suspect that FBI would have any derogatory information regarding these individuals and did not realize that the queries would run against raw FISA-acquired information. [REDACTED]

⁷⁸ ~~(S//NF)~~ For example, [REDACTED] conducted queries that NSD determined were not reasonably likely to retrieve foreign [REDACTED] they were improperly tailored. [REDACTED] Between 18 December 2019 and 06 January 2020, [REDACTED] conducted approximately [REDACTED] queries in [REDACTED] using generic terms without any limiting terms or qualifiers. [REDACTED] advised that he conducted these queries in order to retrieve information related to a research project. Although these queries were conducted for the purpose of retrieving foreign intelligence information or evidence of a crime, NSD determined that the queries were improperly tailored because they did not include any limiting terms or qualifiers and ran against all raw FISA-acquired information in [REDACTED] to which [REDACTED] had access.

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

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

was configured to automatically include FISA datasets – including data acquired pursuant to Titles I, III, and V as well as Section 702 of FISA – and any other datasets the user was authorized to access unless personnel intentionally excluded such data. Pursuant to a change FBI has implemented, a user will now have to intentionally decide to opt-in to unminimized FISA datasets if the user wants to query those datasets. This change [REDACTED] became effective as of June 2021.

(U) (3) Query Errors Caused by FBI System Errors

~~(S//NF)~~ During this reporting period, there were [REDACTED] incidents involving FBI systems failing to comply with the FBI Section 702 querying procedures.⁷⁹ Section III.A of the FBI Section 702 querying procedures defines “query” to mean “the use of one or more terms to retrieve the unminimized contents or noncontents (including metadata) of section 702-acquired information that is located in an FBI system,” and further provides that “such terms may include the use of keywords, identifiers, formulas, attributes, or other data exploitation techniques.” Section IV.A.3 of the FBI Section 702 querying procedures requires, in relevant part, that “[p]rior to reviewing the unminimized contents of section 702-acquired information retrieved using a United States person query term, FBI personnel will provide a written statement of facts showing that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime.” Section IV.B.1 of the FBI Section 702 querying procedures requires FBI to “generate and maintain an electronic record of each United States person query term used for a query of unminimized content or noncontent information acquired pursuant to section 702,” and further specifies that these records must include the query term used, the date of the query, and the identifier of the user who conducted the query. Section IV.B.4 of the procedures requires FBI to maintain a record of each statement of facts required by Section IV.A.3 in a manner that enables oversight by NSD and ODNI.

^(U) ~~(S//NF)~~ In August 2020, FBI discovered an error in a particular system that tracked user queries and presented FISA-acquired information to users in response to user input.⁸⁰ Specifically, since approximately December 2017, this system had been providing information, which included FISA-acquired metadata, to users as they began to type the characters in their query term(s). As a user typed their query term(s), the system began to auto-preview metadata associated with the characters that the user had typed, approximately every half-second. Although the system logged actions of users in half-second intervals, the system did not log full query terms if a user did not finish typing their term, but instead selected a result provided by the auto-preview feature. In query logs provided to NSD for oversight purposes, the system provided only the actions of those users who clicked onto auto-previewed metadata (viewing the individual product, which could include content). If a user did not click on a product (presented either through the auto-preview function or

⁷⁹ ~~(S//NF)~~ Unminimized Section 702-acquired data generally resided in three primary FBI systems: [REDACTED]

⁸⁰ [REDACTED]

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

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

through a full/complete query term that the user submitted), the system did not include their actions in the logs provided to NSD for oversight purposes as a query, even though the user would have been exposed to unminimized FISA-acquired metadata stored there. The FBI reports that it first detected this issue through an internal audit that it conducted of queries and that it disabled this feature in August 2020.

(U) In addition, in early October 2020, FBI discovered that another FBI system was not in compliance with the requirements of FBI's Section 702 querying procedures involving the documentation of United States person queries.⁸¹ In late November 2019, FBI implemented changes to this system that were designed to enable users to comply with the requirements of FBI's querying procedures when conducting queries in this system. Specifically, these system changes required users to record whether their query term was a United States person query term by selecting "USPER" or "Presumed USPER." If the user selected "USPER" or "Presumed USPER," and Section 702-acquired content was returned in response to the query, that content was hidden from the user on the results page. In order to access the content, the user was required to enter a justification (either by using pre-populated justifications or by writing their own). However, in October 2020, FBI determined that under certain circumstances, the system was not requiring users to identify their queries as United States person query terms and was not requiring them to enter justifications to access Section 702-acquired content. This issue occurred only if a user utilized the system's advanced search page and selected the "bulk" query option, which is a specific function in one FBI system and is different from the batch job function discussed above (which is specific to a different FBI system). The FBI's investigation of this incident revealed that the system had operated in this manner since the previous changes to the system were deployed in late November 2019.⁸² In October 2020, FBI implemented changes to the system to correct the issue.

(U) (4) *Errors related to Queries Conducted Solely for an Evidence of a Crime Purpose*

~~(S//NF)~~ Additionally, there were [REDACTED] incidents involving violations of the requirement⁸³ that the Government promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.⁸⁴ In addition, these [REDACTED] incidents violated Section 702(f)(2)(A) of FISA

⁸¹ [REDACTED]

⁸² ~~(S//NF)~~ FBI now advises that its investigation revealed that this issue involved approximately [REDACTED] queries, by approximately [REDACTED] users, and approximately [REDACTED] unique query terms. FBI notes that the difference between the total number of queries and the total number of unique query terms reflects that some of the query terms were run multiple times by the same user.

⁸³ (U) This particular requirement is not contained in FBI's querying procedures. Rather, it was contained in each of the FISC's opinions approving the relevant annual certifications, beginning with the 06 November 2015 Opinion and Order approving the 2015 FISA Section 702 Certifications. In its 06 December 2019 Opinion and Order approving the 2019 FISA Section 702 certifications, the FISC made certain changes to this particular requirement. The queries discussed here were conducted prior to the FISC's 06 December 2019 changes to this reporting requirement.

⁸⁴ [REDACTED]

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

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

which provides that FBI may not access the contents of communications acquired pursuant to Section 702 that were retrieved pursuant to a query made in connection with a predicated criminal investigation using a United States person query term that was not designed to find and extract foreign intelligence information unless FBI applies for an order from the FISC, based on probable cause, and the FISC enters an order approving the application. In these instances, NSD determined that these queries had been conducted solely to find and extract evidence of a crime as part of predicated criminal investigations. The [REDACTED] incidents were discovered by NSD while conducting oversight reviews at two FBI field offices. Of the [REDACTED] incidents, [REDACTED] occurred at one field office, many of which related to investigations of health care fraud, transnational organized crime, violent gangs, bribery, public corruption, and domestic terrorism unrelated to foreign intelligence activity. Subsequent investigation by FBI into these queries revealed that they returned Section 702-acquired information, and NSD presumed that such information was reviewed by FBI personnel absent specific information to the contrary.⁸⁵

(U) ~~(S//NF)~~ The system that was involved with these particular incidents was configured, at the time of the incidents, to preview content of responsive information for users when they executed a query. Subsequent to when these queries were conducted, FBI reconfigured the system at issue so that it no longer presents a preview of the content of unminimized Section 702-acquired information in response to a query. The users who executed these queries were unaware of the particular requirements of Section 702(f)(2), and of an option provided by the system to indicate that their queries were being run solely to extract evidence of a crime in support of a predicated criminal investigation. Because the queries were run using United States person query terms, in order to find and extract evidence of a crime, in support of predicated criminal investigations, and because NSD presumed, based on this system design issue, that FBI personnel reviewed the Section 702-acquired information, without first obtaining an order from the FISC, NSD reported these incidents to the FISC as potential violations of Section 702(f)(2)(A) of FISA. In these incidents, NSD reminded the personnel about the Section 702 query requirements and discussed these requirements with other personnel during NSD's training conducted for the field offices.

85

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

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

(U) In addition, to the reconfiguration of the system at issue as noted above, if the user seeks to access Section 702-acquired content returned from a query, the system forces the user to complete the query in another FBI system. That other FBI system requires the user to answer a question in a pop-up box that asks whether the query is being done only to retrieve evidence of a crime. An information icon also is provided, providing the user with information relating to the requirements of Section 702(f)(2) of FISA. When FBI initially redesigned this system (between September and November 2019), it designed the radio buttons, however, to automatically default the answer to this question in the system to “No.” At that time, if a user proceeded from that default “No,” they were able to select from a series of pre-populated justifications for their query, or select “other” and provide their own, written justification. Once the system received that justification from the user, it allowed the user to access the contents of the Section 702-acquired information. If, however, the user answered “Yes” to the question as to whether it was a query being done to retrieve evidence of a crime, the user was provided with three drop-down justifications for their query: “Court Order,” “Exigent Circumstances,” or “Neither.” If a user selected “Court Order” or “Exigent Circumstances,” they were allowed to proceed to access the contents of the Section 702-acquired information. At that same time, an alert was sent to FBI’s NSCLB, which then conducted additional research into the nature of the query, and coordinated as necessary with NSD. If the user selected “Neither,” they were prevented from accessing the contents of the Section 702-acquired information, and were provided with an alert indicating that they either needed to obtain an order from the FISC or have exigent circumstances to be able to review the contents of the Section 702-acquired information. This alert also directed the user to contact NSCLB or their field office Chief Division Counsel with any questions.

(U) Although outside this reporting period, FBI changed the system design pertaining to the question of whether the query is being done only to retrieve evidence of a crime. The system has now been reconfigured to eliminate a default answer, so that FBI personnel must affirmatively indicate whether or not a query is being conducted solely to retrieve evidence of a crime before they may proceed to conduct a query. This change will help ensure users do not mistakenly accept a default answer that could lead to them accessing the contents of unminimized Section 702-acquired information under circumstances that would otherwise require a Court order or require a report to the FISC pursuant to a reporting requirement for such queries.

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

(U) The joint oversight team has worked with FBI to address the query compliance issues through training, guidance, and system changes. **All of the above-described noncompliant queries were conducted prior to the recent opt-in system change, batch query approval requirement, NSD query guidance, and FBI mandatory 2021 query training detailed below. In addition, the noncompliant queries reported in the prior joint assessments similarly were conducted prior to the recent training, guidance, system change, and other remedial measures implemented in 2021.**

(U) *Historical Remedial Measures*

(U) In June 2018, FBI, in consultation with the joint oversight team, issued guidance to all components where personnel had access to unminimized FISA-acquired information. This

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

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

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” job function. Additional emphasis was provided concerning issues involving queries run against unminimized 702-acquired information to find and extract only evidence of a crime (and not foreign intelligence information). Each FBI field office was instructed to train its personnel on the June 2018 guidance. In January 2019, FBI and NSD conducted joint training for all FBI NSCLB personnel and all field office legal personnel, on FBI’s querying procedures. FBI field office legal personnel were instructed to provide this training to all personnel with access to unminimized FISA-acquired information.

(U) In fall 2019, FBI, in consultation with NSD, developed and deployed mandatory training for FBI personnel on the query standard and on the system changes FBI made to address the query issues. All personnel with access to unminimized FISA-acquired information were required to complete the training by mid-December 2019, and all personnel who subsequently require such access must first complete this training prior to being granted access. In addition, prior to the temporary suspension of NSD query audits in March 2020, NSD generally conducted query training during field office query audits. This training occurred during one-on-one sessions with the individuals being audited and as part of a larger group training at the field office. This training included, among other things, multiple hypothetical examples derived from actual query incidents, as well as guidance on how to use FBI’s systems to allow FBI to better track and comply with requirements involving queries run against unminimized 702-acquired information.

(U) FBI’s Section 702 amended querying procedures adopted by the Attorney General in 2019 included new recordkeeping and documentation requirements for United States person queries. In response the FISC ordered the Government to periodically provide updates on FBI’s implementation of the new requirements. Between September and November 2019, FBI implemented changes requiring FBI personnel to provide a justification explaining how their query meets the query standard when running queries of United States person query terms and when they seek to access Section 702-acquired contents returned by such queries. All query terms and justifications are logged for oversight purposes. In addition, FBI, in consultation with NSD, developed and deployed new training, as detailed above, for FBI personnel on the query standard and system changes.

(U) Recent Training and Guidance

(U) In 2021, NSD resumed remote query audits of FBI users at multiple FBI field offices and FBI Headquarters. Those audits sampled queries conducted in 2020 and 2021 and revealed additional query compliance incidents. As a result of the findings from NSD’s audits and observations of the FISC related to these query incidents, NSD, in consultation with ODNI, developed a guidance document on the query standard for FBI personnel. This guidance supplements existing training on the querying standard; provides a robust explanation of the query standard; and explains the specific requirements imposed by Section 702(f)(2). The guidance document also includes multiple examples of the application of the guidance to particular factual scenarios. On 01 November 2021, NSD provided this guidance document to FBI, and FBI distributed it to all users with access to raw FISA-acquired information to facilitate the correct

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

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

application of the querying standard. Additionally, based on this guidance, FBI developed and deployed additional training that focused specifically on querying requirements. This additional training and guidance, in combination with the below-described changes to FBI's systems used to query unminimized Section 702-acquired information should more adequately address the query compliance issues. FBI requires all personnel with access to unminimized FISA-acquired information to verify that they have completed the required training.

(U) *Recent Technical Changes*

(U) As detailed above, in June 2021 FBI took additional steps to address the batch query compliance incidents and instances where users do not intend to query unminimized FISA-acquired information but fail to opt-out of such datasets. In October 2021, FBI also began redesigning its systems that contain unminimized Section 702-acquired information to include a requirement that users write case-specific justifications for United States person queries designed to retrieve foreign intelligence information that return Section 702-acquired contents if they want to access the contents. The applicable FBI systems also currently require case-specific justifications to access the results of queries designed to return evidence of a crime only. Historically, users have been able to choose pre-populated justifications from a drop-down menu in lieu of entering a free text justification in certain circumstances. The joint oversight team assesses that user understanding of the querying standard can be enhanced if users are required to write their own case-specific justification for a Section 702 query, thus demonstrating their understanding of the querying standard. The joint oversight team also assesses that reviewing these case-specific justifications will enable both internal FBI overseers and external overseers at NSD and ODNI to better determine whether FBI personnel understand the querying standard.

(U) Because some of FBI's remedial measures did not come into effect until June 2021, the joint oversight team is unable, at this time, to assess their overall effectiveness. The joint oversight team will provide updates on its assessment in future joint assessments.

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

(U) During this reporting period, there were no incidents involving noncompliance with the CIA minimization procedures.⁸⁶ There were, however, a small number of incidents involving improper queries of Section 702-acquired information by CIA personnel, although these improper queries did not involve queries of United States person identifiers.⁸⁷ CIA advised that the relevant personnel have been reminded of the Section 702 querying requirements.

⁸⁶ (S//NF) CIA receives unminimized communications from selectors that it nominates to NSA for targeting [REDACTED]

⁸⁷ (S//NF) There were [REDACTED] instances of noncompliance with CIA's querying procedures during the reporting period. In these incidents, a CIA officer queried [REDACTED]

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

~~TOP SECRET//SI//NOFORN/FISA~~**(U) V. Review of Compliance Incidents – NCTC Minimization and Querying Procedures**

~~(S//NF)~~ During the reporting period, there were [REDACTED] incidents involving violations of NCTC's minimization and querying procedures.⁸⁸ These incidents involved an improper query and the improper storage of Section 702-acquired data. The personnel involved in these incidents were reminded of the Section 702 query and minimization requirements. Additionally, NCTC implemented technical systems updates to prevent the improper storage at issue.

~~(S//NF)~~ In one incident, NCTC discovered that NCTC analysts had inadvertently downloaded unminimized Section 702-acquired information and had temporarily retained such information on their desktops because of the configuration of certain web-browsers used to access an NCTC system.⁸⁹ [REDACTED]

[REDACTED] NSD assessed that the retention of unminimized FISA-acquired information on a desktop was not consistent with the NCTC Section 702 minimization procedures because a desktop does not comply with the processing, retention, auditing, and other requirements of those procedures. NCTC implemented a system update in late August 2020, and an additional safeguard in December 2020. Based on its investigation of this incident, NCTC advised that of the [REDACTED] users who have queried the relevant NCTC system, [REDACTED] users identified [REDACTED] suspected downloaded files⁹⁰ of Section 702 raw FISA-acquired information. Upon identifying these files, the users immediately deleted the files from their desktops. Also in late August 2020, NCTC issued guidance to users regarding the above issue and the system updates and safeguards.

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

(U) During the reporting period, there were no reported instances of non-compliance by a "specified person" to whom the Attorney General and DNI have issued directives pursuant to Section 702(i) of FISA.

[REDACTED] Because the CIA assessed that there was no reasonable basis to conclude that [REDACTED] the queries were not reasonably likely to return foreign intelligence information. The responsible officer was counseled on querying requirements. [REDACTED]

88

89

90

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

~~TOP SECRET//SI//NOFORN/FISA~~**(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 implemented to address the causes of compliance incidents during the next reporting period.

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

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

(U) APPENDIX

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

(U) 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: Certification 2019-A or 2020-A, [REDACTED]

[REDACTED] Certification 2019-B or 2020-B, [REDACTED]

[REDACTED] Certification 2019-C or 2020-C, [REDACTED]

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

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

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

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in 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 [REDACTED]

4 [REDACTED]

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

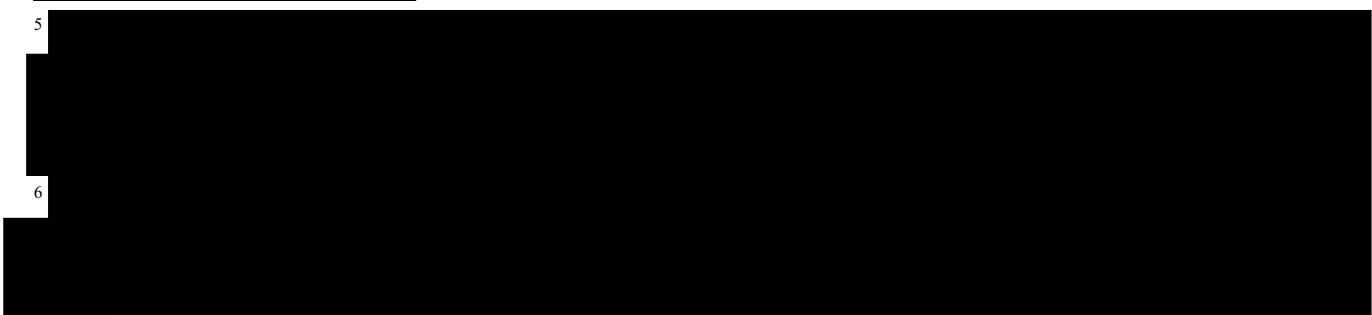
(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, 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

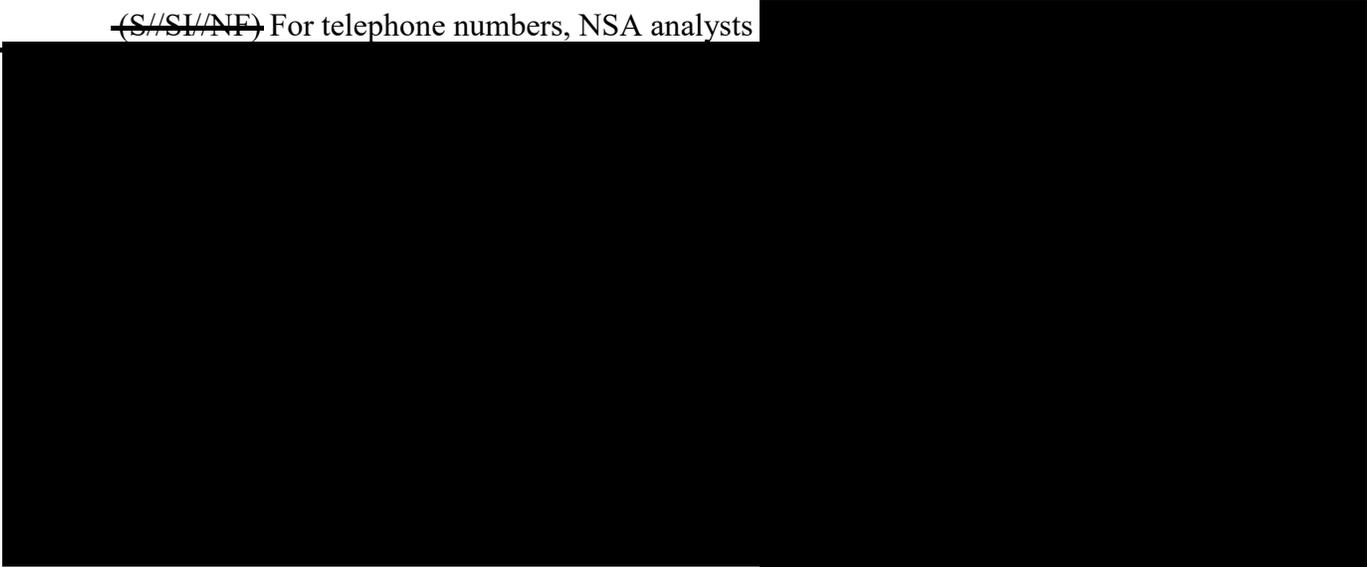
~~TOP SECRET//SI//NOFORN/FISA~~

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

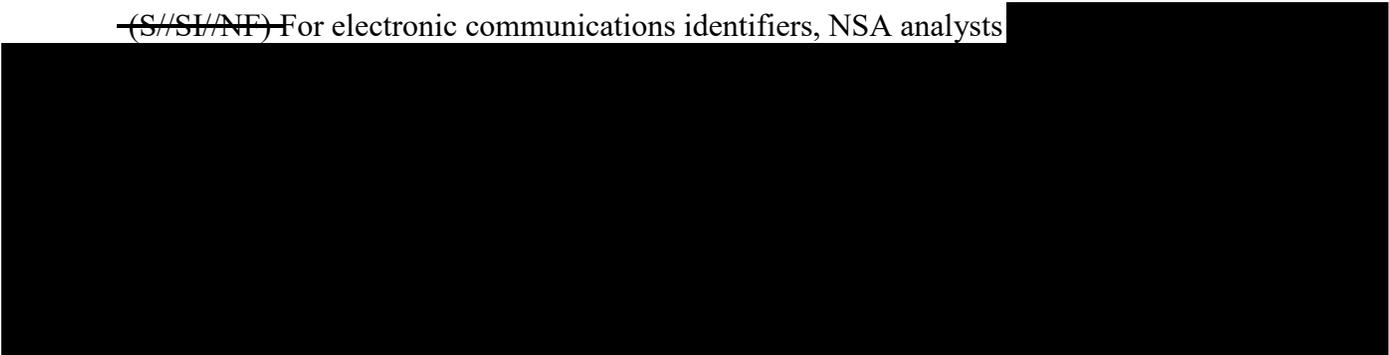
(U) 1. Telephone Numbers

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



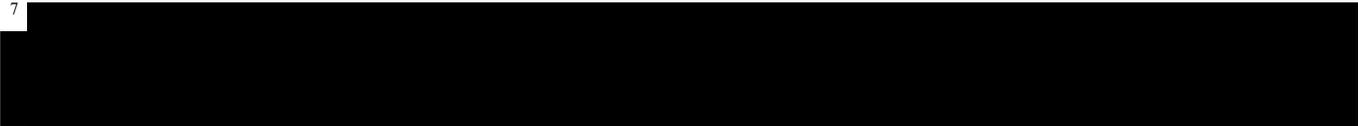
(U) 2. Electronic Communications Identifiers

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



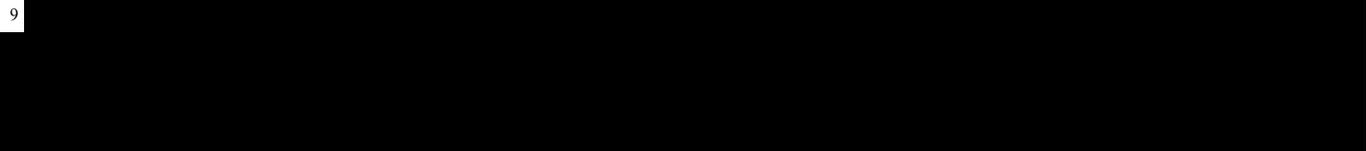
(U) B. Pre-Tasking Determination of United States Person Status

7



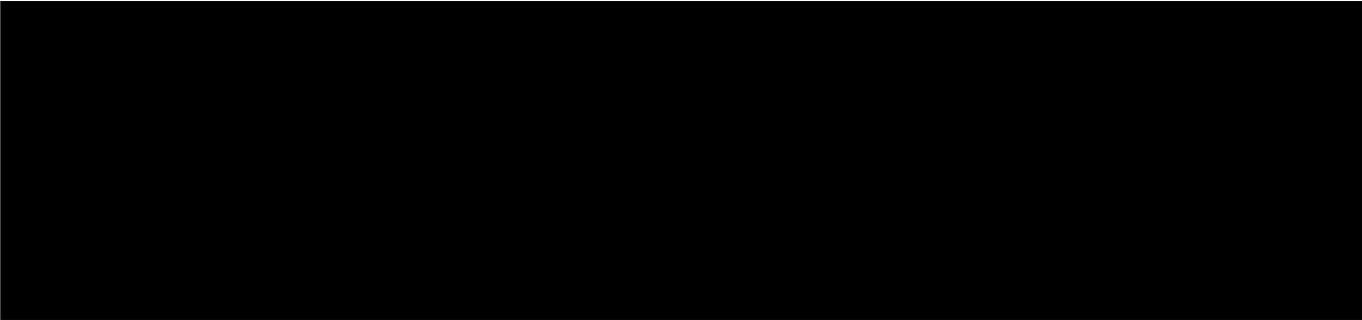
⁸ (U) Analysts also check this system as part of the “post-targeting” analysis described below.

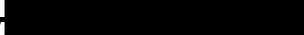
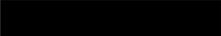
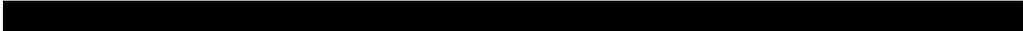
9

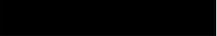


~~TOP SECRET//SI//NOFORN/FISA~~

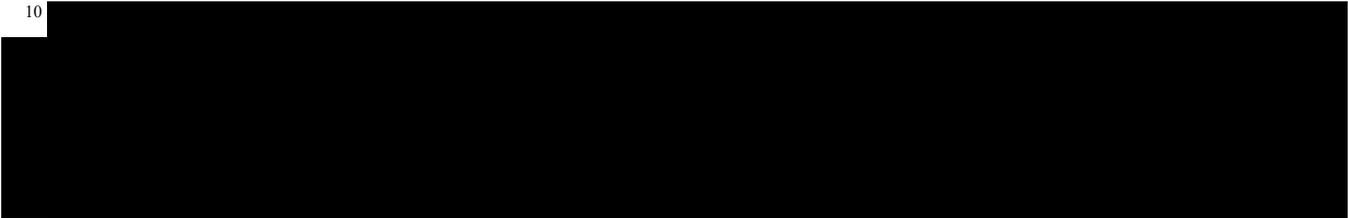
(U) C. Post-Tasking Checks



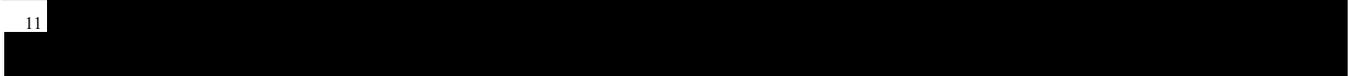
(S ) NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA's review of 
¹¹ a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five 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. 

 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

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

~~TOP SECRET//SI//NOFORN/FISA~~**(U) D. Documentation**

~~(S//NF) (U//FOUO)~~ 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] for 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.

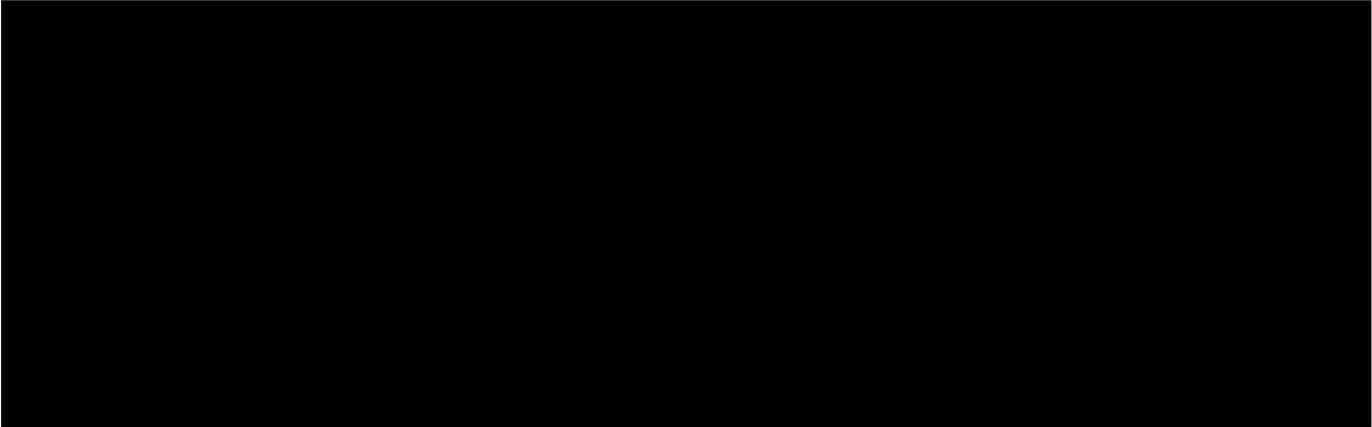
~~(S//NF)~~ [REDACTED]
[REDACTED] Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation 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

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

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

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

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



(U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only authorized personnel who have received certain types of training and authorizations are provided access to the Section 702 program data. These authorized personnel must complete a comprehensive training program as approved by NSA OGC and NSA Compliance Group; review the targeting, minimization, and querying procedures as well as other documents filed with the certifications; and pass a competency test. The databases personnel use are subject to audit and review by NSA’s Compliance Group. For guidance, authorized personnel must consult standard operating procedures, supervisors, NSA Compliance Group 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 OCCO reviews all Section 702 taskings and conducts spots checks of disseminations based in whole or in part on Section 702-acquired information. The Directorate of Operations Information and Intelligence Analysis organization also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

(U) NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. Compliance officers work with NSA analysts and CIA and FBI points of contact, as necessary, to compile incident reports that are forwarded to both the NSA OGC and OIG. NSA OGC forwards the incidents to NSD and ODNI.

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

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

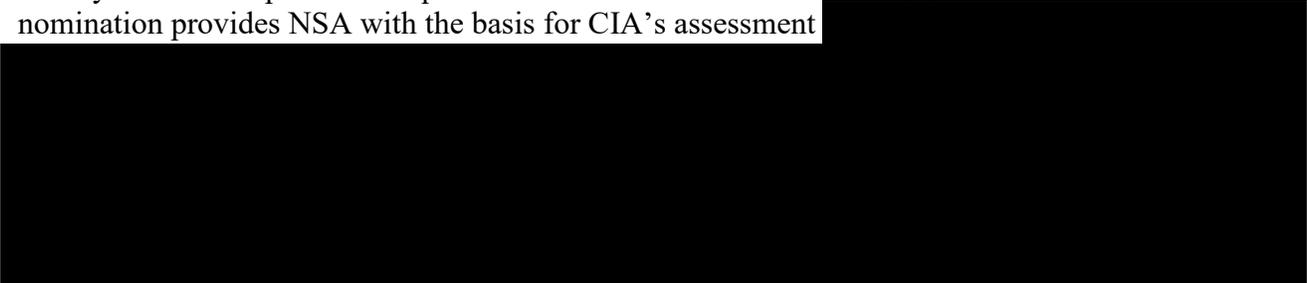
(U) On a more programmatic level, under the guidance and direction of the Compliance Group, NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protections during NSA missions. The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

(U) A key component of the CMCP is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort, known as “Rules Management,” focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA; and (2) technological solutions to support (and simplify) Rules Management activities. The Authorities Integration Group coordinates NSA’s use of the Verification of Accuracy process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy, and compliance officials within NSA. NSA has also developed a Verification of Interpretation review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA’s FISA activities. The Compliance Group conducts the Mission Compliance Risk Assessment (MCRA) that assesses the risk of non-compliance with the rules designed to protect privacy and to safeguard information. Risks are assessed annually by authority and/or function for SIGINT and Cybersecurity missions. The results are used to inform management decisions, priorities, and resource allocations regarding the NSA/CSS CMCP.

(U) II. Overview – CIA

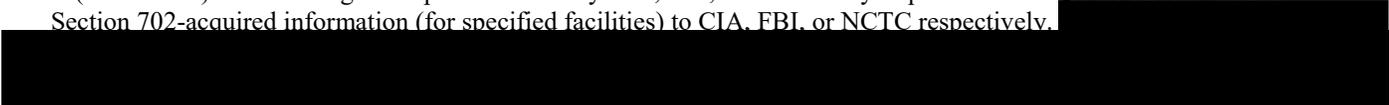
(U) A. CIA’s Role in Targeting

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



(U) ~~(S//NF)~~ In addition to nominations, CIA may also request unminimized data from Section 702 facilities already tasked by NSA, a process referred to as “dual-routing.”¹² CIA applies its Section 702 minimization procedures to both the Section 702 nominated and dual-routed data.

¹² ~~(TS//SI//NF)~~ Dual-routing is the process whereby CIA, FBI, or NCTC may request that NSA route already tasked Section 702-acquired information (for specified facilities) to CIA, FBI, or NCTC respectively.

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

~~TOP SECRET//SI//NOFORN/FISA~~~~(S//NF)~~

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.¹³

~~(S//NF)~~ The FISA Program Office was established in December 2010

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. 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

NSA does not dual-route upstream collection to CIA, FBI, or NCTC

(U)¹³ ~~(S//NF)~~ This nomination approval process was the one in place during the reporting period. However, on 21 October 2021, CIA's nominations process was revised to require approval by only the targeting officer's first line manager and the FISA Program Office. Throughout the process, both component legal officers and CIA's FISA attorneys are available for consultation regarding whether the nomination is in compliance with Section 702 of FISA and NSA's targeting procedures. The Government assesses this change eliminates redundancy in CIA's nomination process.

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

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

respond to inquiries regarding nomination, minimization, and querying. 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

(U) A. 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 dual-routed on unminimized data (pertaining to counterterrorism) from Section 702 facilities already tasked by NSA. NCTC applies its Section 702 minimization and querying procedures to Section 702 dual-routed data.

~~(S//NF)~~ NCTC, in consultation with NSD, developed an electronic and data storage system, known as ██████████ 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 ██████████ to (i) provide additional compliance capabilities in support of dual-routing FISA Section 702-acquired counterterrorism data and (ii) monitor compliance with NCTC's minimization and querying procedures for Section 702-acquired counterterrorism data. In addition to documenting compliance with the Section 702 minimization and querying procedures requirements, ██████████ also documents the requests for dual-routing of Section 702-acquired information. This documentation includes the foreign intelligence justification (pertaining to counterterrorism) for dual-routing the facility and supervisory concurrence with an analyst's request.

~~(S//NF)~~ Dual-routed unminimized communications from Section 702 tasked facilities are stored within ██████████ 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 ██████████, all dual-route requests and minimization actions must be reviewed and approved within ██████████ by the analyst's supervisor.

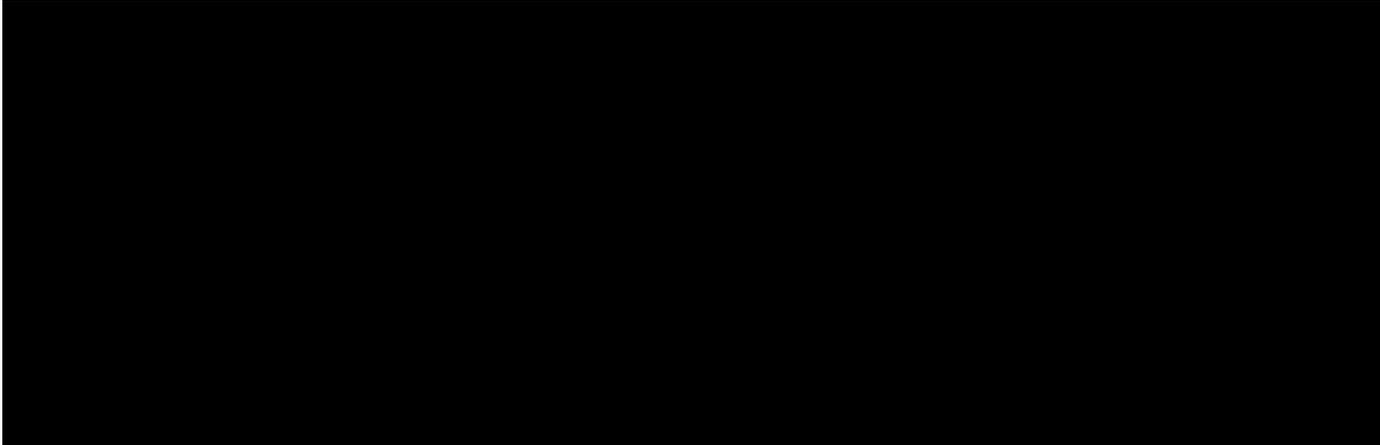
(U) NCTC personnel may disseminate Section 702-acquired information of or concerning an unconsenting United States person if that information meets the standard for dissemination pursuant to Section D of NCTC's minimization procedures.

~~(S//NF)~~ ██████████ 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

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

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

procedures and identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.

~~(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 and querying procedures are reported to NSD and ODNI generally by NCTC Compliance or NCTC Legal personnel.

(U) ~~(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

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

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

NCTC Section 702 collection is properly dual-routed, 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 of [REDACTED] communications. [REDACTED]

[REDACTED] Like CIA, FBI may be dual-routed the unminimized data from Section 702 facilities already tasked by NSA. FBI applies its Section 702 minimization procedures to both the Section 702 nominated and dual-routed data.

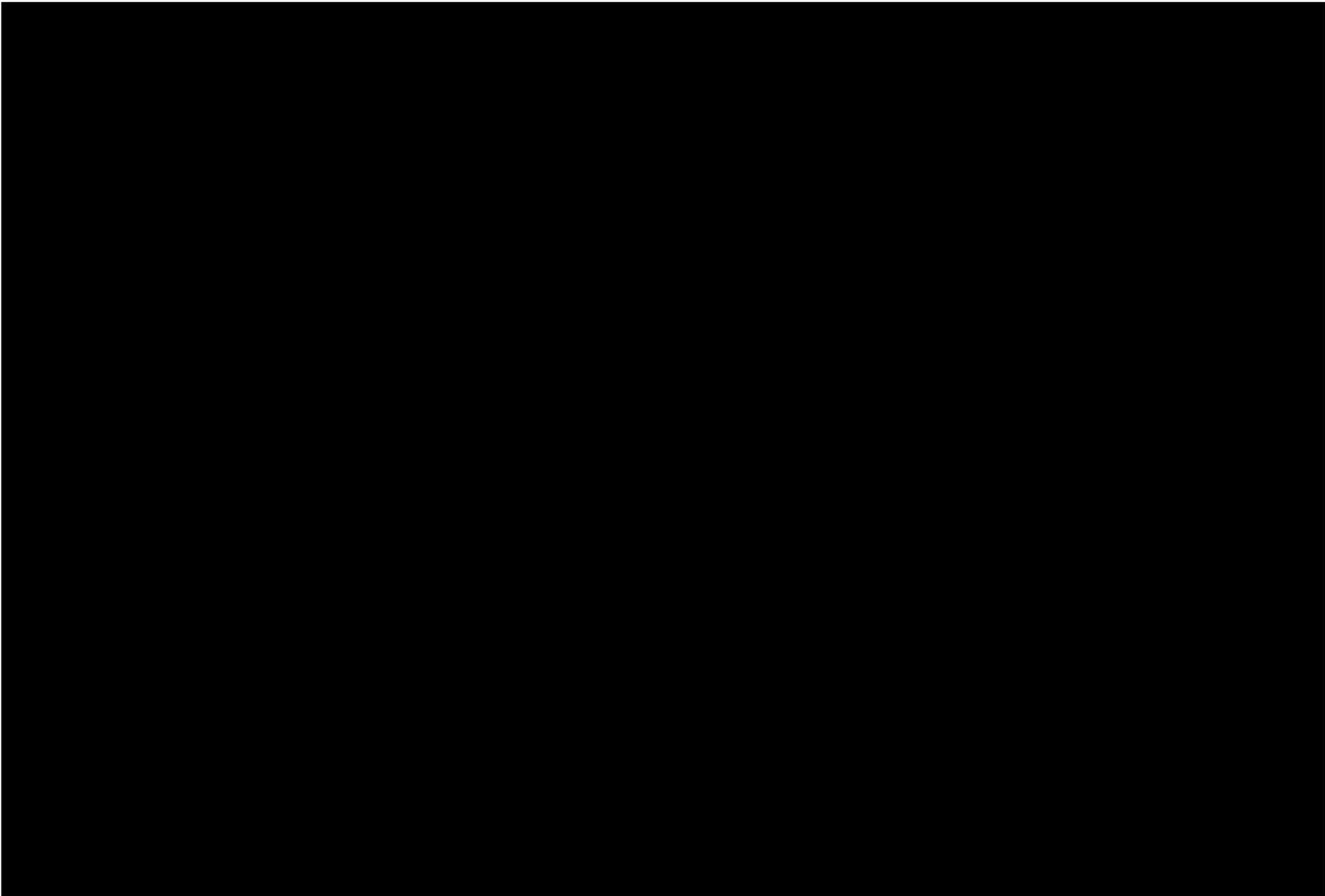
[REDACTED]

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

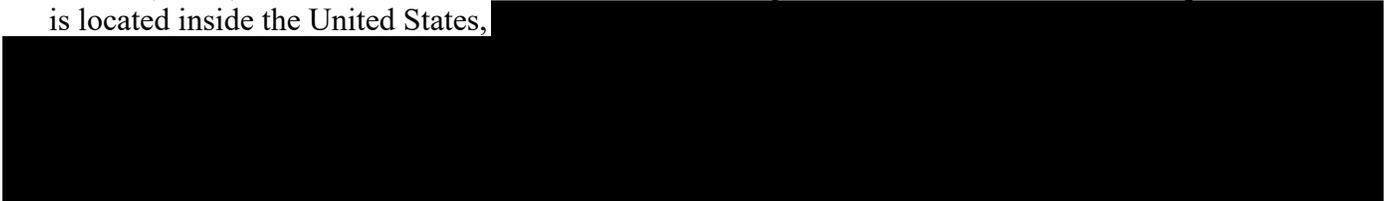
[REDACTED] FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a United States person. NSA is also responsible for determining that a significant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

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

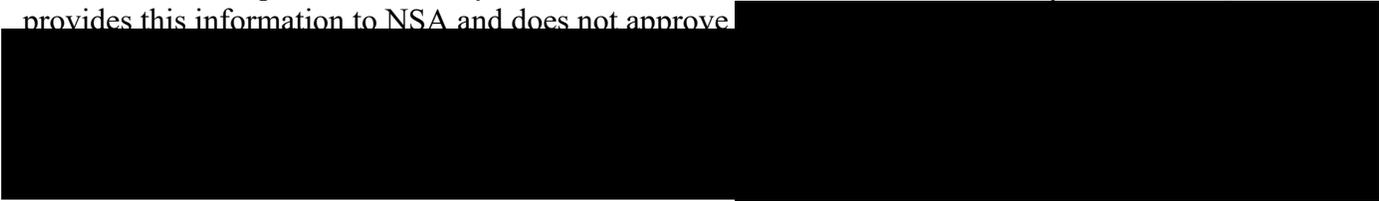
~~TOP SECRET//SI//NOFORN/FISA~~



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

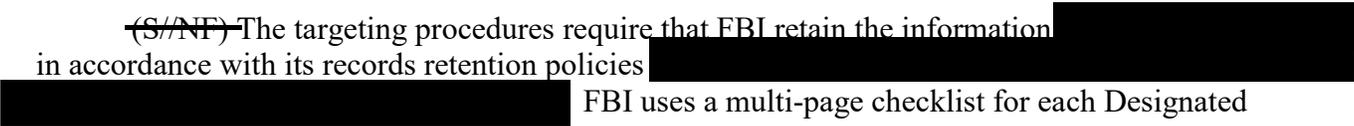


~~(S//NF)~~ If FBI identifies information indicating that NSA's determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve. [REDACTED]



(U) C. Documentation

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



FBI uses a multi-page checklist for each Designated

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

Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [REDACTED] extending through [REDACTED] and culminating in approval or disapproval of the acquisition. In addition, FBI standard operating procedures call for [REDACTED] depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications [REDACTED] regarding its review [REDACTED] information. Additional checklists have been created to capture information on requests withdrawn by [REDACTED] or not approved by FBI.

(U) D. Implementation, Oversight, and Compliance

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI OGC, particularly the National Security and Cyber Law Branch (NSCLB), as well as FBI's Technology and Data Innovation Section (TDI), FBI's [REDACTED] and FBI's Inspection Division (INSD). [REDACTED]

[REDACTED] TDI has the lead responsibility in FBI [REDACTED] requests [REDACTED] TDI personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests [REDACTED] TDI also has the lead responsibility for facilitating FBI's nominations to NSA [REDACTED] TDI, NSCLB, NSD, and ODNI have all worked on training FBI personnel to ensure that FBI nominations and post-tasking review comply with the NSA targeting procedures. 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 FBI [REDACTED] In addition, NSD conducts training on the Section 702 minimization procedures at multiple FBI field offices each year.¹⁴

(U) 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 FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. TDI and NSCLB are the lead FBI elements in ensuring that NSD and ODNI receive 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-

¹⁴ (U) As noted above, onsite field office reviews were suspended in March 2020. NSD resumed field office reviews remotely in February 2021. Thus, NSD only conducted onsite training at field offices for a portion of this reporting period.

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

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

acquired information. Prior to the FISA Amendments Reauthorization Act of 2017 codification, the minimization procedures contained querying rules. The 2018 certifications were the first certifications to contain the newly required querying procedures.

(U) As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, CIA and NCTC. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

(U) Section 702 minimization procedures do, however, impose additional obligations or restrictions as compared with the minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

(U) NSA, CIA, NCTC, and FBI have created systems to track the purging of information from their systems. CIA, NCTC, and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.

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

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

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

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

(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 OGC 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~~