



Office of the Director of National Intelligence

ANNUAL STATISTICAL TRANSPARENCY REPORT

REGARDING THE INTELLIGENCE COMMUNITY'S
USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES

————— Calendar Year 2020 —————

Office of Civil Liberties, Privacy, and Transparency

April 2021



Table of Contents

- Executive Summary..... 4**
- Introduction 5**
 - A. Background 5*
 - B. Areas Covered in this Report 5*
 - C. Statistical Fluctuations Over Time..... 6*
 - D. Key Terms 6*
- FISA Probable Cause Authorities 9**
 - A. FISA Titles I and III..... 9*
 - B. FISA Title VII, Sections 703 and 704..... 9*
 - C. Statistics 10*
- FISA Section 702..... 12**
 - A. Section 702 12*
 - B. Statistics—Orders and Targets 15*
 - C. Statistics—U.S. Person Queries 16*
 - D. Section 702 and FBI Investigations..... 21*
 - E. NSA Dissemination of U.S. Person Information under FISA Section 702..... 21*
- IC Dissemination of U.S. Person Information 25**
 - A. ICPG 107.1 25*
 - B. Statistics 25*
- FISA Criminal Use and Notice Provisions 27**
 - A. FISA Sections 106 and 305 27*
 - B. Statistics 27*
- FISA Title IV—Use of Pen Register and Trap and Trace (PR/TT) Devices..... 28**
 - A. FISA Pen Register/Trap and Trace Authority..... 28*
 - B. Statistics 28*
- FISA Title V—Business Records 31**
 - A. Title V Business Records 31*
 - B. Statistics—Title V “Traditional” Business Records Statistics Orders, Targets & Identifiers 31*
- National Security Letters (NSLs)..... 34**
 - A. National Security Letters 34*
 - B. Statistics—National Security Letters and Requests for Information..... 34*

Table of Figures

Figures 1a and 1b: FISA “Probable Cause” Court Orders and Targets10

Figures 2a and 2b: FISA “Probable Cause” Targets Broken Down by U.S. Person Status 11

Figure 3: Section 702 Orders16

Figure 4: Section 702 Targets16

Figure 5: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Content17

Figure 6: U.S. Person Query Terms Used To Query Section 702 Content17

Figure 7: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Noncontents 18

Figure 8: U.S. Person Queries of Noncontents of Section 70218

Figure 9: FBI Review of 702 Query Results of Queries Not Designed To Return Foreign Intelligence Information..... 21

Figure 10: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition21

Figure 11: Section 702 Reports Containing USP Information Unmasked by NSA.....24

Figure 12: Section 702 USP Identities Disseminated by NSA24

Figure 13: Requests for USP Identities and Decisions Regarding those Requests per ICPG 107.125

Figure 14: Number of Criminal Proceedings in Which the Government Provided Notice of Its Intent To Use Certain FISA Information27

Figures 15a and 15b: PR/IT Orders, Targets, and Unique Identifiers Collected29

Figures 16: PR/IT Targets Broken Down By U.S. Person Status.....30

Figure 17a, 17b, and 17c: Business Records Orders, Targets, and Unique Identifiers Collected32

Figures 18a and 18b: NSLs Issued and Requests for Information35

Executive Summary

Today, consistent with the *Foreign Intelligence Surveillance Act of 1978* (FISA), as amended (codified in 50 U.S.C. § 1873(b)), and the Intelligence Community's (IC) [Principles of Intelligence Transparency](#), the government is releasing its **eighth** annual *Statistical Transparency Report Regarding the Intelligence Community Use of National Security Surveillance Authorities*. This transparency report provides statistics and contextual information concerning how the IC uses FISA and certain other national security authorities to accomplish its mission, describing the circumstances under which its national security activities are conducted and the rules that are designed to ensure compliance with the Constitution and laws of the United States. By providing statistics along with explanatory narratives, the report endeavors to add further context to other publicly released materials regarding the oversight framework, including oversight conducted by independent judicial and legislative entities, which collectively safeguards the civil liberties and privacy of United States person and non-U.S. person information.

While the full report provides the same categories of statistics as prior years, the following table is a quick reference of the calendar year (CY) 2020 statistics for categories of historic interest:

Authority	CY2020 Number of Court Orders	CY2020 Number of Targets
FISA Titles I and III and Sections 703 and 704 "Probable Cause"	524	451
FISA Section 702	1	202,723 (Non-US persons only)
FISA Title IV "Pen Register and Trap and Trace"	15	8
FISA Title V – Section 501(b)(2)(B) "Traditional Business Records"	28	25

FISA Section 702 – Queries	CY2020
U.S. Person Terms Used by NSA, CIA, and NCTC to Query Section 702 Content	7,218
U.S. Person Queries of Noncontents of Section 702	9,051

Introduction

Today, consistent with the *Foreign Intelligence Surveillance Act of 1978* (FISA), as amended (codified in 50 U.S.C. § 1873(b)), and the Intelligence Community's (IC) *Principles of Intelligence Transparency*, the government is releasing its **eighth** annual *Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities* presenting statistics on how often the government uses certain national security authorities, including FISA. These statistics add further context regarding the rigorous and multi-layered oversight framework, including by independent judicial and legislative entities, that safeguards the civil liberties and privacy of the persons whose information is acquired pursuant to these national security authorities. Both United States Persons (U.S. person or USP) and non-United States Persons are afforded privacy protections based on the different authorities discussed herein.

This report goes beyond FISA's statutory reporting regime by providing the public with detailed explanations as to how the IC uses its national security authorities. This document should be read in conjunction with the national security-related materials that the government has already released publicly, especially the documents that have been highlighted through the hyperlinks embedded in this report, as well as the statistical report provided by the Director of the Administrative Office of the U.S. Courts, *see* 50 U.S.C. § 1873(a) (available on the [AOUSC website](#)).

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, [www.dni.gov](#), the IC's public website, [www.intel.gov](#), and ODNI's public Tumblr site, *IC on the Record* at [IContheRecord.tumblr.com](#). *ODNI's Guide to Posted Documents* is another resource to find information that has been released to the public.

A. Background

In June [2014](#), the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including FISA, in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the Annual Statistical Transparency Report). Subsequent Annual *Statistical Transparency Reports* were released in [2015](#), [2016](#), [2017](#), [2018](#), [2019](#), and [2020](#).

On June 2, 2015, the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015* (USA FREEDOM Act) was enacted, amending FISA by requiring the government to publicly report, consistent with the protection of national security information, many of the statistics already reported in the *Annual Statistical Transparency Report*. The USA FREEDOM Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning U.S. person search terms and queries of certain FISA-acquired information. *See* 50 U.S.C. § 1873(b). On January 19, 2018, the *FISA Amendments Reauthorization Act of 2017* was signed, further codifying the release of additional statistics, including many statistics that the government previously reported pursuant to its commitment to transparency. *See id.*

B. Areas Covered in this Report

While this report provides statistics concerning a variety of national security authorities, the report predominantly covers FISA. As background, FISA (50 U.S.C. §§ 1801, et seq.) authorizes electronic surveillance and other forms of collection to obtain foreign intelligence information. Over the years, it has been amended, most recently by the *FISA Amendments Reauthorization Act of 2017*. FISA is divided into Titles, each containing

sections, which specify the means, requirements, and limitations on the collection of foreign intelligence information. Title I of FISA concerns electronic surveillance, Title III applies to physical searches, Title IV regulates the use of Pen Registers and Trap and Trace devices, Title V regards accessing certain Business Records, and Title VII applies to various forms of collection concerning persons located outside the United States. Each of these authorities is detailed below and throughout this report.

As explained below, the Foreign Intelligence Surveillance Court (FISC) authorizes and oversees the government's use of the FISA authorities. Additionally, Title VI of FISA, along with other various FISA provisions, details the independent oversight by the legislative branch. FISA requires certain reports be submitted to Congress, including reports containing all identified compliance incidents and various compliance trends. Finally, FISA also requires certain transparency reporting, such as the statistics in this transparency report, be provided to the public.

In addition to reporting statistics regarding the use of FISA authorities, this report provides statistics regarding the handling of requests for the identities of U.S. persons whose identities were originally masked in a disseminated intelligence report, regardless of the legal authority under which the information was collected, as well as certain statistics regarding National Security Letters (NSLs).

C. Statistical Fluctuations Over Time

The statistics provided in this report fluctuate from year to year for a wide variety of reasons, many of which cannot be explored in detail in an unclassified setting without divulging information necessary to protect national security. In some instances, there may be no relationship between a decrease in the use of one authority and an increase in another. At a high level, statistics may

fluctuate due to changes in collection and operational priorities of the U.S. government, world events, technical capabilities, target behavior, the dynamics of the ever-changing telecommunications sector, and the use of technology to automate the delivery of marketing and other communications. In particular, ODNI assesses that in calendar year 2020, the impact of the COVID-19 pandemic likely influenced target behavior, which in turn may have impacted some of the numbers reported for that year.

D. Key Terms

Certain terms used throughout this report are described below. Other terms are described in the sections in which they are most directly relevant. These terms will be used consistently throughout this report.

- **U.S. PERSON.** As defined by Title I of FISA, a U.S. person is “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*), 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 [50 U.S.C. §§ 1801(a)(1), (2), or (3)].” 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.
- **TARGET.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is used as a noun and defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses a selec-

tor, e.g., a telephone number or email address, subject to collection.

The IC also uses the term “target” as a verb. For example, Section 702 authorizes 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 for each target, Section 702 requires targeting procedures that are applied to each individual targeting decision. Additional information on targeting is detailed below in the Section 702 discussion.

Despite the different meanings, collecting foreign intelligence about a target for foreign intelligence purposes must be informed by intelligence needs specified by the [National Intelligence Priorities Framework \(NIPF\)](#). The NIPF is the high-level mechanism to manage and communicate national intelligence priorities, facilitating the IC’s ability to allocate finite resources to address the most pressing intelligence questions and mission requirements. Guidance from the President and the Assistant to the President for National Security Affairs (commonly referred to as the National Security Advisor), with formal input from cabinet-level heads of departments and agencies, determine the overall priorities of the top-level NIPF issues.

First, the IC must determine that a particular target meets a particular intelligence need under the NIPF. Once the IC determines that a particular target meets a particular intelligence need, the IC may collect intelligence regarding that target only if authorized by applicable legal authorities (e.g., certain acquisitions authorized under FISA or Executive Order 12333).

- **FISC.** The FISC was established in 1978 when Congress enacted FISA (*see* 50 U.S.C. §§ 1801-1885c). The Court is composed of eleven federal district court judges who are desig-

nated by the Chief Justice of the United States. Pursuant to FISA, the Court entertains applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. The FISC conducts oversight of the government’s use of FISA authorities by requiring, among other things, reporting of all identified compliance incidents and a variety of reports concerning compliance and oversight actions. In its oversight role, the FISC assesses the government’s compliance with and use of the FISA authorities. Based upon its assessment, the FISC can terminate, modify, or limit the government’s authority to use FISA, including through binding remedial decisions.

- **ORDERS.** There are different types of orders that the FISC may issue in connection with FISA cases, including orders granting or modifying the government’s applications to conduct foreign intelligence collection pursuant to FISA; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the FISC with specific information. As with past years, this report only counts orders granting the government’s applications.

The FISC may *amend* an order one or more times after it has been granted. For example, an order may be amended to add a newly discovered account used by the target. This report does not count such amendments separately.

The FISC may *renew* some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target outside of the United States may last no longer than 90 days, but FISA permits the order to be

- renewed, *see* 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Unlike amendments, this report counts each such renewal as a separate order granting the requested FISA authority.
- **ESTIMATED NUMBER.** Throughout this report, when numbers are *estimated*, the estimate comports with the statutory requirements to provide a good faith estimate of a particular number.
 - **MINIMIZED INFORMATION.** Minimized information is lawfully collected information to which an agency (such as NSA) has applied its minimization procedures.
 - **DISSEMINATION.** Dissemination refers to the sharing of minimized information.
 - **MASKED U.S. PERSON INFORMATION.** IC element's rules and procedures (such as agency minimization procedures) generally provide for the substitution of a U.S. person identity with a generic phrase or term so the reader cannot ascertain the U.S. person's identity, unless the dissemination of the U.S. person's identity would be consistent with the applicable legal authorities (e.g., because the identity is necessary to understand the foreign intelligence information). "Masking" the identity of the U.S. person (i.e., omitting identifying information from the intelligence report) allows the IC element to disseminate the intelligence in accordance with its procedures, while protecting the U.S. person's civil liberties and privacy.
 - **UNMASKING U.S. PERSON INFORMATION.** After an IC element disseminates an intelligence report with a U.S. person's identifying information masked, recipients of the report may request that the masked information in the report be revealed or "unmasked." The requested identity information is released only if the requesting recipient has established a "need to know" the identity of

the U.S. person and if the dissemination of the U.S. person's identity would be consistent with the applicable legal authorities.

- **AMICUS CURIAE.** In 2015, the USA FREEDOM Act codified a framework under which a qualified individual can be appointed as an amicus curiae to assist the FISC and the Foreign Intelligence Surveillance Court of Review (FISC-R) in any instance the Court "deems appropriate" (including matters that present a novel or significant interpretation of the law or matters requiring technical expertise) before those courts. *See* 50 U.S.C. § 1803. Individuals designated as amici must have expertise in privacy and civil liberties, intelligence collection, communications technology, or other areas that may lend legal or technical expertise to the FISC and FISC-R and must also be eligible for access to classified information. When appointed, an amicus curiae provides those courts, as appropriate, with legal arguments that advance the protection of individual privacy and civil liberties; information related to intelligence collection or communications technology; or legal arguments or information regarding any other area relevant to the issue presented to the court.

FISA Probable Cause Authorities

A. FISA Titles I and III

With limited exceptions (e.g., in the event of an emergency), to conduct electronic surveillance or physical search of any individual, regardless of U.S. person status, under FISA Title I or FISA Title III, a probable cause court order is required. Title I of FISA permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power when the government has a significant purpose to obtain foreign intelligence information. See 50 U.S.C. §§ 1804, 1823. Title I (electronic surveillance) and Title III (physical search), commonly referred to as “Traditional FISA.” Both Title I and Title III require that, following submission of a government application, the FISC make a probable cause finding, based upon a factual statement in the government’s application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA, and (ii) the facility being targeted for electronic surveillance is used by or about to be used by, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1804(a), 1823(a). Because these authorities require individual orders based on probable cause, bulk collection is not permitted. FISC orders and opinions authorizing the government’s use of these authorities may be found on *IC on the Record* (e.g., in postings in [September 2017](#) and on [September 11, 2020](#) and [September 23, 2020](#)) and on [Intel.Gov’s Intel Vault](#) page.

B. FISA Title VII, Sections 703 and 704

Sections 703 and 704 of FISA Title VII similarly

FISA Title I, Title III, and Title VII Sections 703 and 704

- All of these authorities require individual court orders based on probable cause.
- Titles I and III apply to FISA collection targeting persons within the United States.
- Sections 703 and 704 apply to FISA collection targeting U.S. persons outside the United States.
- Because individual courts orders are required, bulk collection is not permitted.

require a court order based on a finding of probable cause for the government to conduct FISA collection targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data inside the U.S., in a manner that otherwise requires an order under FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes. Both Sections 703 and 704 require that the FISC make a probable cause finding, based upon a factual statement in the government’s application, that the target is (i) a U.S. person reasonably believed to be located outside the United States and (ii) a foreign power, agent of

a foreign power, or officer or employee of a foreign power. Additionally, the government’s application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1881b(b), 1881c(b).

cal search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

C. Statistics

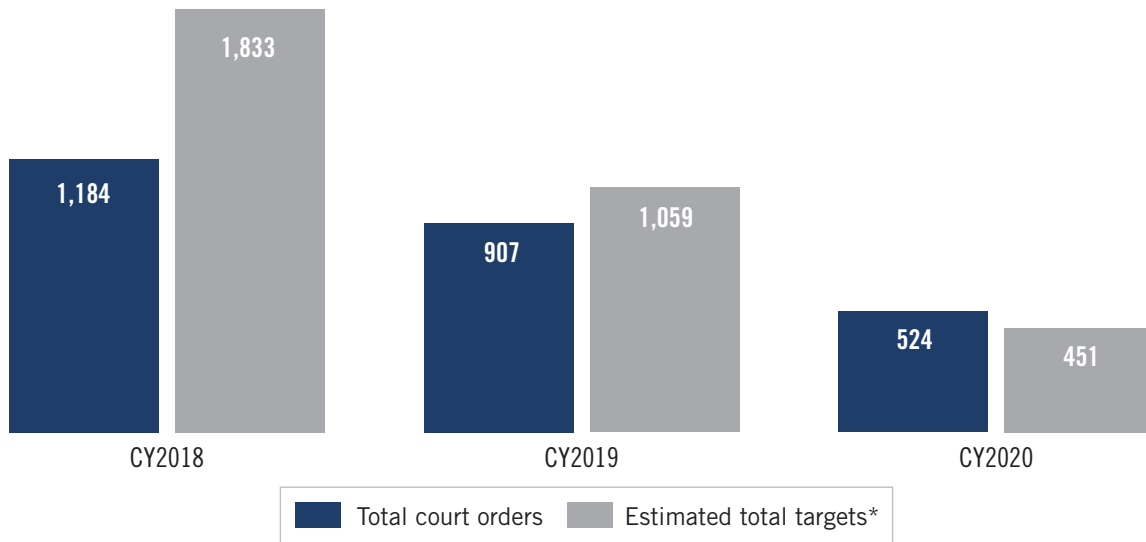
HOW TARGETS ARE COUNTED. If the IC received authorization to conduct electronic surveillance or physi-

Figure 1a: FISA “Probable Cause” Court Orders and Targets

Titles I and III and Sections 703 and 704 of FISA	CY2018	CY2019	CY2020
Total number of orders	1,184	907	524
Estimated number of targets of such orders*	1,833	1,059	451

See 50 U.S.C. §§ 1873(b)(1), 1873(b)(1)(A).

Figure 1b: FISA “Probable Cause” Court Orders and Targets



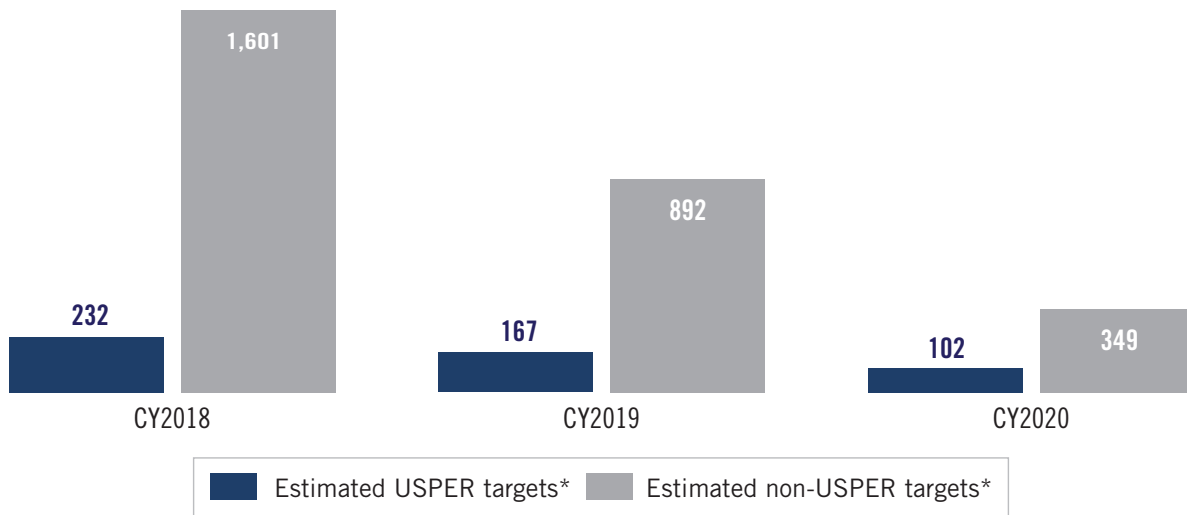
See 50 U.S.C. §§ 1873(b)(1), 1873(b)(1)(A).

Figure 2a: FISA “Probable Cause” Targets Broken Down by U.S. Person Status

Titles I and III and Sections 703 and 704—Targets	CY2018	CY2019	CY2020
Estimated number of targets who are <i>non</i> -U.S. persons	1,601	892	349
Estimated number of targets who are U.S. persons	232	167	102
Percentage of targets who are estimated to be U.S. persons	12.7%	15.8%	22.6%

See 50 U.S.C. §§1873(b)(1)(B), 1873(b)(1)(C) for rows one and two, respectively.

Figure 2b: FISA “Probable Cause” Targets Broken Down by U.S. Person Status



FISA Section 702

A. Section 702

Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) who are reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. See 50 U.S.C. § 1881a. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures, minimization procedures, and querying procedures that they attest satisfy the statutory requirements of Section 702 and are consistent with the Fourth Amendment. Absent exigent circumstances (see 50 U.S.C. § 1881a(c)(2)), before the government may use Section 702, the government must apply for approval from the FISC (detailed below) by submitting a type of application package containing a certification with targeting, minimization, and querying procedures. To ensure compliance with statutory requirements, individual targeting decisions are required and, thus, bulk collection is not permitted. Additional information on how the government uses Section 702 is posted on *IC on the Record*, including FISC orders and opinions approving the government's use of this authority, most recently in [April 2021](#), and on [Intel.Gov's Intel Vault](#) page.

SECTION 702 TARGETS AND "TASKING." Under Section 702, the government "targets" a particular non-U.S. person, including non-U.S. person groups or entities, reasonably believed to be located outside the United States to acquire foreign intelligence information by "tasking" selectors (e.g., telephone numbers and email addresses). Before tasking a selector for collection under Section 702, the government must make individual targeting decisions for each individual selector and apply its FISC approved targeting procedures to ensure

FISA Title VII Section 702

- Commonly referred to as "Section 702."
- Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.
- Because individual targeting decisions are required, bulk collection is not permitted.

that each selector is used by a non-U.S. person who is reasonably believed to be located outside the United States and who is expected to possess, receive, and/or is likely to communicate foreign intelligence information. The foreign intelligence information sought must fall within a specific category of foreign intelligence information that has been authorized for acquisition by the Attorney General and the DNI as part of a Section 702 certification, described below. The government must record, in every targeting decision, the specific rationale for targeting a specific person to obtain foreign intelligence information.

In addition to the requirement that the type of foreign intelligence information sought must be authorized as part of a certification approved by the FISC, as a matter of policy, agencies must also apply protections required by [Presidential Policy Directive 28 \(PPD-28\)](#), [Signals Intelligence Activities](#) to Section 702-acquired information. PPD-28 reinforces longstanding intelligence practices that protect privacy and civil liberties, while requiring

agencies to implement new procedures to ensure that U.S. signals intelligence activities continue to include appropriate safeguards for the personal information of all individuals, regardless of nationality or residency.

NSA and FBI task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized (i.e., “raw”) Section 702 data—NSA, FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC)—handle the Section 702-acquired data in accordance with minimization and querying procedures, which are explained below.

THE FISC’S ROLE. Under Section 702, the FISC determines whether certifications executed jointly by the Attorney General and the DNI, as well as accompanying targeting, minimization, and querying procedures, meet all the requirements of Section 702 and the Fourth Amendment. The FISC’s review is not limited to the procedures as written, but also includes an examination of how the procedures have been and will be implemented. Specifically, every identified compliance incident is reported to the FISC by the government through notices and reports; additionally, the government reports other implementation and compliance information such as the number of targets and other statistical information, the results of oversight reviews, and assessment of compliance trends. More information about oversight is provided in the Attorney General and DNI’s joint [Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act](#) (commonly referred to as the Joint Assessment of Section 702 Compliance or the Joint Assessment), most recently released in [April 2021](#), on *IC on the Record*, as well as a [Summary of Oversight](#) and a [September 2020 White Paper](#) discussing Section 702.

Based on these reports, the FISC conducts its own compliance analysis and – in oral hearings or

through written responses – can require the government to further explain compliance incidents and describe how the incidents have been remedied. This type of reporting occurs throughout the year to ensure that the FISC remains aware of how the government is implementing Section 702. Accordingly, as part of its annual review to approve the government’s use of its Section 702 procedures, the FISC considers all the compliance incidents reported to it throughout the year and the government’s overall implementation of Section 702.

If the FISC determines that the government’s certification application package meets the statutory requirements of Section 702 and is consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. If the FISC is not satisfied with the government’s certification application, the government’s compliance record, or the government’s implementation of Section 702, the FISC can terminate, modify, or limit the government’s authority to use Section 702, including through binding remedial decisions. The FISC approved the 2020 certifications in a [November 2020 opinion](#), which was publicly released together with the procedures in April 2021 and posted on *IC on the Record*.

CERTIFICATIONS. Under Section 702, the Attorney General and DNI jointly execute certifications under which the IC intends to acquire specified foreign intelligence information. The certifications identify categories of foreign intelligence information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction. Each annual certification must be submitted to the FISC for approval in a certification application

package that includes the Attorney General's and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, minimization procedures, and querying procedures.

TARGETING PROCEDURES. The targeting procedures detail the steps that the government must take before and after tasking a selector to ensure that the government is lawfully targeting the user of the tasked selector. Specifically, the government must reasonably assess that the user is a non-U.S. person who is reasonably believed to be located outside the United States. Additionally, the government must reasonably assess that tasking the selector is likely to acquire foreign intelligence information that falls within an approved Section 702 certification. Further, the targeting procedures require the government to provide written, fact-based explanations of its assessments that support individual determinations that each tasked selector meets the requirements of the targeting procedures. All incidents of non-compliance with the targeting procedures are reported to the FISC regardless of a target's citizenship or U.S. person status. Even improper targeting of a non-U.S. person located outside the United States - such as when the government does not have a sufficient basis to assess whether the non-U.S. person target is reasonably likely to possess, receive, or communicate foreign intelligence information - is reported to the FISC.

Each set of targeting procedures is adopted by the Attorney General, in consultation with the DNI, and then submitted to the FISC as part of the certification package. The FISC assesses the legal sufficiency of each agency's targeting procedures as well as how the IC has complied with past procedures. Only agencies that have FISC approved targeting procedures may task selectors pursuant to Section 702; only two agencies, NSA and FBI, have targeting procedures and thus are permitted to task selectors.

NSA includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular selector was requested. The intent of the TAR is to memorialize why the analyst is requesting tasking; it provides a linkage between the user of the selector and the foreign intelligence purpose covered by the certification under which it is being tasked. The TAR is reviewed by the Department of Justice oversight team as part of their routine review of the tasking records. More information about these oversight reviews is provided in the Attorney General and DNI's [Joint Assessment of Section 702 Compliance](#) released on *IC on the Record* in April 2021. [NSA's 2020 targeting procedures](#) and [FBI's 2020 targeting procedures](#) were also publicly released on *IC on the Record* in April 2021.

Non-U.S. persons benefit from many of the protective rules prescribed by the targeting procedures. Under Section 702, collection is targeted (i.e., not bulk), and must be limited to non-U.S. person targets located outside the United States who are expected to possess, receive, and/or are likely to communicate foreign intelligence information that is specified in one of the FISC-approved certifications. See [Status of Implementation of PPD-28: Response to the PCLOB's Report, October 2018](#) at 9. Further, all identified compliance incidents are reported to the FISC, regardless of U.S. person status.

MINIMIZATION PROCEDURES. The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, including specific restrictions regarding non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of each agency to obtain, produce, and disseminate foreign intelligence information. Each agency's Section 702 minimization procedures are adopted by the Attorney General, in consultation with

the DNI. The FISC reviews the sufficiency of each agency's minimization procedures as part of the certification application package. Such reviews include assessing the IC's compliance with past procedures. The 2020 minimization procedures for [CIA](#), [FBI](#), [NCTC](#), and [NSA](#) were released on *IC on the Record* in April 2021.

In addition to the protections afforded by the targeting procedures, as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization procedures. See [Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of FISA \(July 2, 2014\)](#) at 100. As with the targeting procedures, all identified compliance incidents are reported to the FISC, regardless of U.S. person status. Moreover, as noted previously, PPD-28 regulates the IC's retention and dissemination of personal information of non-U.S. persons collected pursuant to Section 702.

QUERYING PROCEDURES. The FISA Amendments Reauthorization Act of 2017 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 U.S. person term used for a query. Similar to the Section 702 targeting and minimization procedures, the querying procedures are required to be reviewed by the FISC as part of the certification package for consistency with the statute and the Fourth Amendment. Congress added other requirements in Section 702(f), which pertain to accessing certain results of queries conducted by FBI; those requirements will be discussed later in this report.

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 U.S. person or non-U.S. person. As explained in the April 2021-released [Joint Assessment of Section 702 Compliance](#), NSA personnel are required to obtain Office of General Counsel approval before any use of U.S. person identifiers as terms to query the content of Section 702 information. The 2020 querying procedures for [CIA](#), [FBI](#), [NCTC](#), and [NSA](#) were released on *IC on the Record* in April 2021.

COMPLIANCE. The IC's application of the targeting, minimization, and querying procedures is subject to robust internal agency oversight and to rigorous external oversight by DOJ, ODNI, Congress, and the FISC. Every identified incident of noncompliance, regardless of the U.S. person status of individuals affected by the incident, is reported to the FISC (through notices or in reports) and to Congress in semiannual reports. Depending on the nature of the incident, the FISC may order remedial actions, which could include deleting improperly collected information, recalling improperly disseminated information, and retraining IC employees. DOJ and ODNI also jointly submit semiannual reports to Congress that assess the IC's overall compliance efforts. [Past Joint Assessments of Section 702 Compliance](#) have been publicly released.

B. Statistics—Orders and Targets

COUNTING SECTION 702 ORDERS. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information. Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC's order. Because

the number of the government’s Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

ESTIMATING SECTION 702 TARGETS. The number of Section 702 targets, provided below, reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on information readily available to the IC.

Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Figure 3: Section 702 Orders

Section 702 of FISA	CY2018	CY2019	CY2020
Total number of orders issued	1	2*	1

See 50 U.S.C. § 1873(b)(2).

*This number includes (a) the FISC order dated September 4, 2019, which authorized the amended 2018 certifications and made public on October 8, 2019, and (b) a FISC order dated December 6, 2019, which authorized the 2019 certifications. The number does not include the FISC-R order, dated July 9, 2019, and made public on October 8, 2019, because the FISC-R order did not authorize any certifications.

Figure 4: Section 702 Targets (recall that only non-USPs are targeted)

Section 702 of FISA	CY2018	CY2019	CY2020
Estimated number of targets of such orders	164,770	204,968	202,723

See 50 U.S.C. § 1873(b)(2)(A).

C. Statistics—U.S. Person Queries

The USA FREEDOM Act requires reporting of the “number of search terms concerning a known United States person used to retrieve the unminimized contents [...]” – referred to as “query terms of content” – and “the number of queries concerning a known United States person of unminimized noncontents information [...].” See 50 U.S.C. §§ 1873(b)(2)(B) and (b)(2)(C), respectively.

Below are statistics for U.S. person queries of raw Section 702-acquired data. The U.S. person statistics are based on (a) U.S. person *query terms* used to query Section 702 *content* and (b) U.S. person *queries* conducted of Section 702 *noncontents* (i.e., metadata). It is important to understand that these two very different numbers cannot be com-

pared because they use *different counting methodologies* (query terms versus queries conducted) and *different data types* (content versus noncontents).

COUNTING U.S. PERSON QUERY TERMS USED TO QUERY SECTION 702 CONTENT.

The NSA counts the number of U.S. person identifiers it has approved to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier “johndoe@XYZprovider” to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used “johndoe@XYZprovider” to query its 702-acquired information. Not every query term approved, however, is ultimately used. CIA and NCTC count the number of unique U.S. person identifiers their personnel have actually used to

query within the agencies' respective repositories of unminimized Section 702-acquired information. Because of the variance in how these agencies count these query terms, the government

deems it likely that the number of query terms reported is slightly higher than the actual number of query terms used.

Figure 5: How the IC counts U.S. Person Query Terms Used to Query Section 702 Content

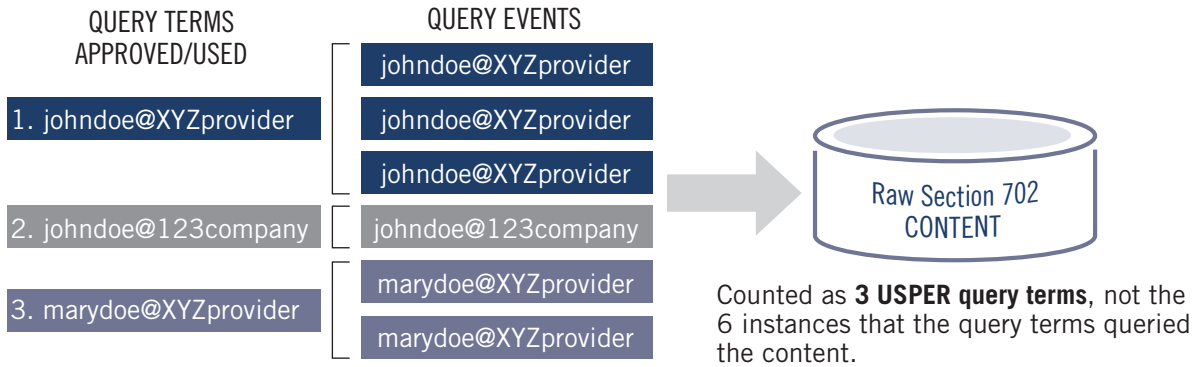


Figure 6: U.S. Person Query Terms Used to Query Section 702 Content

Section 702 of FISA	CY2018	CY2019	CY2020
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*, **	9,707	9,299	7,218

See 50 U.S.C. § 1873(b)(2)(B).

*Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

** The estimated number of content query terms for CY2018 and CY2019 were previously reported as 9,637 and 9,126 respectively, but have been updated to reflect instances where terms were mistakenly undercounted. For example, if a single query was conducted as "johndoe@xyz.provider OR johndoe@123company," that was sometimes erroneously counted as one term when it should have been counted as two terms. Queries, such as "johndoe@xyz.provider AND johndoe@123company," are counted as one term.

COUNTING QUERIES USING U.S. PERSON IDENTIFIERS OF NONCONTENTS COLLECTED UNDER SECTION 702. This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired

information. For example, if the U.S. person identifier telephone number "111-111-2222" was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

Figure 7: How the IC counts U.S. Person Queries of Section 702 Noncontents

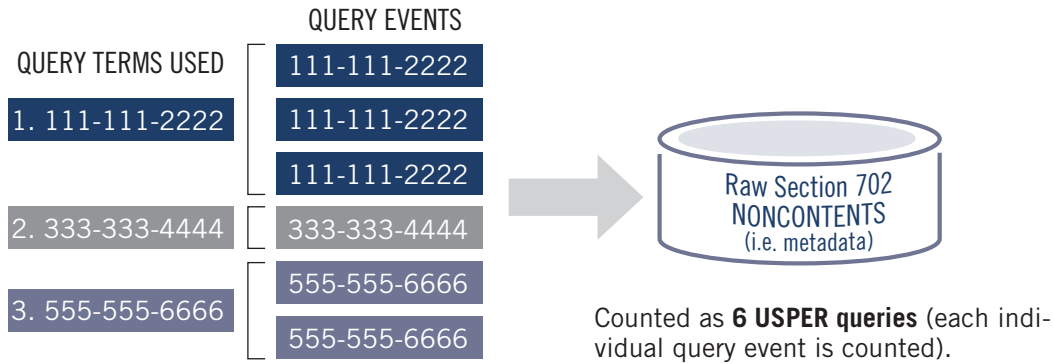


Figure 8: U.S. Person Queries of Noncontents of Section 702

Section 702 of FISA	CY2018	CY2019	CY2020
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*, **	14,307	16,545	9,051

See 50 U.S.C. § 1873(b)(2)(C).

*Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

** The estimated number of noncontents queries for CY2018 and CY2019 were previously reported as 14,374 and 16,692, respectively. These numbers have been adjusted because it was determined that these estimates inadvertently included some queries that were of both content and non-content.

FBI QUERIES NOT DESIGNED TO RETURN FOREIGN INTELLIGENCE INFORMATION. The FBI is the only intelligence agency with Section 702 querying procedures that allow for queries that are reasonably likely to retrieve evidence of a crime, in addition to queries designed to be reasonably likely to return foreign intelligence information. Recognizing that unrelated crimes can be discovered in the course of conducting FISA activities, since enactment Congress has required that FISA minimization procedures contain provisions addressing how to treat evidence of unrelated crimes acquired in the course of a foreign intelligence activity. See, e.g., *United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991) (permitting use of FISA collection in a state homicide case of recordings of the target committing a murder unrelated to the foreign intelligence purpose for the collection). There are also in-

stances for which the the activity in which the FBI is interested (e.g., international terrorism) is both relevant to foreign intelligence information and a criminal act. In recent years, both Congress and the FISC, however, have focused on instances in which FBI’s purpose at the time the query is solely to retrieve evidence of a crime (i.e., authorized queries that are “not designed to return foreign intelligence information”).

This report includes two statistics regarding such FBI queries. Since 2015, the government has been required by FISC orders to report certain queries conducted solely for the purpose of retrieving evidence of a crime. In addition, statutory provisions were added to FISA in 2018 that impose obligations related to certain queries conducted solely for the purpose of retrieving evidence of a crime.

The Court-ordered requirements have changed over time, largely as a result of the 2018 statutory additions, requiring the following detailed explanation to fully understand the reported figures.

On November 6, 2015, the FISC approved the 2015 certifications and, among other things, concluded that the FBI's querying provisions in its minimization procedures "strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government's national security interests, on the other." *Memorandum Opinion and Order* dated November 6, 2015, at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries "designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment." *Id.*

Nevertheless, the FISC ordered the government to report in writing, "each instance after December 4, 2015, in which FBI personnel *receive and review* Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." *Id.* at 44 and 78 (emphasis added). The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. Consistent with the IC's *Principles of Intelligence Transparency*, the DNI has declassified statistics regarding such queries, and the number of reports of such queries in CY2018 and CY2019 are reported below in the first row of Figure 9.

In the FISA Amendments Reauthorization Act of 2017, which was passed in January 2018, Congress imposed new requirements regarding accessing

the contents of communications retrieved pursuant to certain queries conducted by the FBI. Specifically, under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can access the contents of communications that were retrieved pursuant to a query using a U.S. person 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. Before the FISC may issue such an order based on a finding of probable cause, a federal officer must prepare a written application that includes the officer's justification for the belief that the query results would provide evidence of a crime, and the application must be approved by the Attorney General. The FBI must report annually the number of times it received an order pursuant to Section 702(f)(2)(A). *See* 50 U.S.C. § 1873(b)(2). These figures for CY2018, CY2019, and CY2020 are reported in the second row of Figure 9.

In light of the statutory change that focused on the use of U.S. person query terms instead of whether U.S. person information had been accessed, in December 2019, the FISC modified the trigger for the reporting requirement it first imposed in 2015. Instead of requiring that the FBI report instances in which FBI personnel "received and reviewed" Section 702-acquired information concerning a U.S. person in response to any query (whether or not the query terms concerned a United States person) not designed to return foreign intelligence information, the FISC modified its order to require that the FBI report to the Court when FBI personnel had "accessed" any unminimized Section 702 content (regardless of whether the content concerned a United States person) returned in response to "a query that used a U.S.-person query term and was not designed to find and extract foreign-intelligence information." *Memorandum Opinion and Order* dated December 6, 2019, at 71 - 73, 81 (released on *IC on the Record*

on September 4, 2020). Unlike the requirements of Section 702(f)(2)(A), the FISC's reporting requirement was intentionally broader, applying to any such query, regardless of whether the query was conducted in the course of a predicated criminal investigation. Consistent with the IC's *Principles of Intelligence Transparency*, the DNI has declassified the CY2020 number of reports of such queries, which is reported below in the first row of Figure 9.

While the FBI notified the Department of Justice of a reportable query that occurred in CY2020, previous FBI queries not designed to return foreign intelligence information typically were not initially identified by FBI, but were instead discovered during oversight reviews conducted by the Department of Justice. Reports of such queries derived from the Department of Justice's compliance notices to the FISC regarding such FBI queries are also included in the numbers reported in the first row of Figure 9. As the Court described on pages 69 - 71 of its December 2019 opinion, some of the incidents the Department of Justice identified and that are reported in reports of queries counted in Figure 9 resulted from instances when an FBI system automatically displayed 100 characters of text around the query term within the records identified as responsive to the query. The Department of Justice has reported to the Court identified instances of queries resulting in such automatic displays regardless of whether it could be determined that FBI per-

sonnel had actually reviewed the information. The FBI modified its systems to eliminate this automatically displayed information when FBI personnel query Section 702 information shortly before the FISC's December 2019 opinion.

Although the statutory requirement to obtain a court order pursuant to Section 702(f)(2) is narrower than the Court's requirements to report certain queries to the FISC, a Section 702(f)(2) order should have been obtained, because of this automatic displaying of text, prior to accessing content in nearly all of the queries described in the reports to the FISC enumerated in Figure 9. The FISC discussed this issue in both the December 2019 and November 2020 opinion. See [Memorandum Opinion and Order](#) dated December 6, 2019, at 69 - 73 (released on *IC on the Record* on September 4, 2020); [Memorandum Opinion and Order](#) dated November 18, 2020 at 42 - 44 (released on *IC on the Record* in April 2021). As detailed in the FISC's opinions, the FBI has taken steps, including widespread training and system modifications, to improve compliance with query requirements, to include identifying instances where a Section 702(f)(2) order is required. See November 2020 opinion at 44 - 50. These steps include modifying systems to create automated alerts to FBI attorneys to queries that potentially trigger the Court-ordered reporting requirement. FBI attorneys then follow up on any queries in an effort to ensure compliance with the applicable requirements.

Figure 9: FBI Review of 702 Query Results of Queries Not Designed to Return Foreign Intelligence Information

Section 702 of FISA	CY2018	CY2019	CY2020
As required by Court orders (described in detail above), reports to FISC of FBI personnel accessing specified Section 702-acquired content returned by specified queries not designed to find and extract foreign intelligence information	5*	91**	1
FISC orders obtained pursuant to Section 702(f)(2) to review the results of a query that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence	0	0	0

See FISC Memorandum Opinion and Order dated December 6, 2019 at 71 - 73, 81; 50 U.S.C. § 1873(b)(2).

* This figure was previously reported as six, but a review determined that the correct number of reports to the Court was five.

** This figure was previously reported as one; however, subsequent to the completion of the CY2019 *Annual Statistical Transparency Report*, the Department of Justice filed with the FISC additional reports of FBI personnel having reviewed, or potentially reviewed, the specified Section 702 acquired content that were identified in the course of the Department of Justice's oversight reviews. Most of these reports involved queries in which FBI systems automatically displayed information in response to queries, as discussed above and in the FISC's December 2019 opinion. With respect to 89 of the 91 reports cited above, in some instances, a single report to the Court involved multiple queries on the same day by the same user that returned and displayed Section 702 content. Queries on different days or by different users (including queries using the same terms) were counted as separate reports, even if the Department of Justice advised the Court of such queries in a single filing. In the case of the remaining two of the 91 reports, separate users ran multiple queries on multiple days, but the reports to the Court did not specify the dates on which queries that returned or displayed Section 702 information were run. Although the FBI modified its systems to remedy the automatic display issue in 2019, subsequent oversight reviews have identified additional reportable queries that occurred prior to the FBI's modifications of its systems.

D. Section 702 and FBI Investigations

With the enactment of the FISA Amendments Reauthorization Act of 2017, FISA now requires that the FBI report on the number of instances in which the FBI opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on Sec-

tion 702-acquired information. See 50 U.S.C. § 1873(b)(2)(D). This statistic provides transparency with regard to how often Section 702 collection is used for non-national security investigations conducted by the FBI. Figure 10 provides the required statistic.

Figure 10: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition

Section 702 of FISA	CY2018	CY2019	CY2020
The number of instances in which the FBI opened, under the Criminal Investigative Division or any successor division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under Section 702	0	0	0

See 50 U.S.C. § 1873(b)(2)(D).

E. NSA Dissemination of U.S. Person Information under FISA Section 702

BACKGROUND ON NSA DISSEMINATING U.S. PERSON INFORMATION UNDER SECTION 702. Consistent with prior transparency reports, and in continued compliance with a recommendation made in the PCLOB's *Section 702 Report*, this report provides additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information.

Prior to the PCLOB issuing its *Section 702 Report*, NSA's Director of the Civil Liberties, Privacy, and Transparency Office published "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*," on April 16, 2014, (hereinafter "[NSA DCLPO Report](#)"), in which it explained NSA's dissemination processes. NSA DCLPO Report at 7-8. NSA "only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information." NSA DCLPO Report at 7.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. [NSA's minimization procedures](#) (most recently released in April 2021) permit the NSA to disseminate U.S. person information if the information is necessary to understand the foreign intelligence. By policy, generally, the NSA masks the information that could identify the U.S. person. NSA's minimization procedures define U.S. person identifying information as "(1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person [...]." See NSA's Minimization Procedures 3(f).

The minimization procedures also permit NSA to disseminate U.S. person identities only if doing so meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S.

person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person information was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. For example, a Section 702 target may communicate information about a U.S. person that the target intends to victimize in some way; NSA may need to disseminate the identity of affected U.S. persons to appropriate authorities so that they can take appropriate protective, preventive, or investigative action.

Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person identity and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. See [NSA's Minimization Procedures](#). For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person "Bad Guy" communicated with U.S. person "John Doe" (i.e., the actual name of the U.S. person), the report would mask "John Doe's" name, and would state that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person." Other examples of masked U.S. person identities would be "a named U.S. entity," "a U.S. person email address," or "a U.S. IP address."

In the instances where NSA's report contains masked U.S. person information, recipients of the report may submit a request to NSA for the U.S. person identifying information. The requested identity information is released (i.e., unmasked) only if the requesting recipient has a "need to know" the identity of the U.S. person and if the dissemination of the U.S. person's identity would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance); additional approval by a designated NSA official is also required.

In certain other instances, however, NSA makes a determination that it is appropriate to include in the original report the U.S. person's identity (i.e., openly naming the U.S. person). When NSA includes U.S. person information in the original report, NSA is required to apply the same minimization and "need to know" standards discussed above.

As part of their regular oversight reviews, DOJ and ODNI review disseminations that contain information of or concerning U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were consistent with the minimization procedures.

Additional information describing how the IC protects U.S. person information obtained pursuant to FISA is provided in reports by the civil liberties and privacy officers for the ODNI (including NCTC), NSA, FBI, and CIA. The reports collectively documented the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations. See [ODNI Report on Protecting U.S. Person Identities in Disseminations under FISA](#) and [annexes containing agency specific reports](#).

STATISTICS REGARDING NSA'S DISSEMINATION OF U.S. PERSON INFORMATION ACQUIRED FROM SECTION 702. Below are statistics and charts to further explain how NSA disseminates U.S. person information incidentally acquired from Section 702 in classified intelligence reports. NSA may:

- i. Openly name (i.e., originally reveal) the U.S. person identity in the report;
- ii. Initially mask (i.e., not reveal) the U.S. person identity in the report; or,
- iii. In the instances where the U.S. person identity was initially masked, upon a specific request, later reveal and unmask the U.S. person identity but only to the requestor.

Consistent with the [CY2019 Annual Statistical Transparency Report](#), this year's report presents the number of reports (in Figure 11) separate from the statistics relating to the U.S. person identities later disseminated (in Figure 12).

NSA applies its minimization procedures in preparing its classified intelligence reports, and then disseminates the reports to authorized recipients with a need to know the information in order to perform their official duties. A limited number of NSA's intelligence reports from Section 702 collection contain references to U.S. person identities (whether masked or openly named).

The first row of Figure 11 provides "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." See 50 U.S.C. § 1881a(m)(3)(A)(i). NSA's counting methodology is to include any disseminated intelligence report that contains a reference to one or more U.S. person identities, whether masked or openly named, even if the report includes information from sources other than Section 702 collection. NSA does not maintain records that allow it to readily determine, in the case of an intelligence report that includes information from several sources, from which source a reference to a U.S. person identity was derived. Accordingly, the references to U.S. person identities may have resulted from Section 702-authorized collection or from other authorized signals intelligence activity conducted by NSA. This counting methodology was used in the previous report and is used in NSA's FISA Section 702(m)(3) report.

Note that a single report could contain multiple U.S. person identities, masked or openly named. For example, a single report could include a large number of U.S. identities that a foreign intelligence target is seeking to victimize; each of those identities would be counted.

As noted above, a U.S. person is "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), 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 [50 U.S.C. § 1801(a)(1), (2), or (3)].” See 50 U.S.C. § 1801(i). Thus the numbers below include U.S. person identities not only of U.S. persons who are individuals, but also of U.S. persons that are corporations or unincorporated associations.

The second row of Figure 11 provides the *number of reports* containing U.S. person identities *where*

the U.S. person identity was masked in the report. The third row provides the *number of reports* containing U.S. person identities *where the U.S. person identity was openly included* in the report.

Figure 12 provides statistics relating to the numbers of U.S. person identities originally masked in those reports counted in Figure 11 but which NSA later provided to authorized requestors (i.e., unmasked). This statistic is the number required to be reported to Congress pursuant to 50 U.S.C. § 1881(m)(3)(A)(ii), which requires “an accounting of the number of United States-person identities subsequently disseminated by [NSA] in response to requests for identities that were not referred to by name or title in the original reporting.”

Figure 11: Section 702 Reports Containing USP Information Disseminated by NSA

Section 702 Reports Containing U.S. Person Information Disseminated by NSA	CY2018	CY2019	CY2020
REPORTS – Total number of NSA disseminated §702 reports containing USP identities regardless of whether the identity was openly included or masked	4,495	4,297	3,627
REPORTS – Total number of NSA disseminated §702 reports containing USP identities where the USP identity was masked	3,442	3,196	2,648
REPORTS – Total number of NSA disseminated §702 reports containing USP identities where the USP identity was openly included	1,379	1,562	1,351

Rows 2 and 3 will not total row 1 because one report may contain both masked and openly included identities.

Figure 12: Section 702 USP Identities Unmasked by NSA

Section 702 - U.S. Person Information Unmasked by NSA	CY2018	CY2019	CY2020
The number of U.S. person identities that NSA unmasked in response to a specific request from another agency	16,721	10,012	9,354

IC Dissemination of U.S. Person Information

A. ICPG 107.1

Intelligence Community Policy Guidance (ICPG) 107.1, Requests for Identities of U.S. Persons in Disseminated Intelligence Reports, requires all IC elements to have procedures to respond to requests for the identities of U.S. persons whose identities were originally masked in a disseminated intelligence report. ICPG 107.1 applies to information regardless of the legal authority under which the information was collected including, but not limited to, FISA Section 702.

ICPG 107.1 does not change the standard for when a U.S. person's identity may be unmasked. Each IC element must follow the applicable legal authorities when determining if the element is permitted to unmask the identity of a U.S. person. [Each IC element must also have its own procedures](#) to implement ICPG 107.1, which were posted on *IC on the Record*.

B. Statistics

ICPG 107.1 also requires the DNI to report, on an annual basis, certain statistics to track requests made pursuant to ICPG 107.1. As of

ICPG 107.1

- Procedures to respond to requests for U.S. person information that was masked in disseminated intelligence reporting and to report the number of those requests.
- Applies to all 18 IC elements.
- Applies regardless of the legal authority under which the information was collected.
- Does not change the standard for when a U.S. person identity may be unmasked.

January 1, 2019, all IC elements began tracking the applicable requests, including whether those requests were approved or denied, pursuant to the requirements of ICPG 107.1 § E.2. Accordingly, Figure 13 provides these numbers for CY2019 and CY2020.

To explain how the IC counted applicable requests, definitions are provided below.

Figure 13: Requests for U.S. Person Identities and Decisions Regarding those Requests per ICPG 107.1

ICPG 107.1 § E.2. Reporting by the Intelligence Community		
Total requests received and disposition	CY2019	CY2020
Total Number of Requests Received by all IC elements this calendar year	7,724	6,933
Of the requests received, the IC Approved	6,845	6,193
Of the requests received, the IC Denied in Full	349	279
Of the requests received, the IC processed as Withdrawn in Full	270	216
Of the requests received, the IC has Pending Decisions	260	245

- **REQUESTS RECEIVED** are requests to identify U.S. persons whose identities were initially masked in disseminated intelligence reports. A single request may include one or more identities or involve one or more disseminated intelligence reports, but is still counted as one request. Duplicate requests, where the same requesting entity makes a request identical to what it had already requested, are not counted. If a subsequent request changes in any manner – with respect to the identities requested, the disseminated intelligence reports, or the intended recipients of the identities – the second request would be counted as a new request received.
- **APPROVED** are requests approved in part or in their entirety. Requests that were approved in part, regardless of whether they were also denied in part or withdrawn in part, are included in this number. Approvals that occurred in January following the reported calendar year for requests that were initially received in the preceding year are included in this number. For example, if an approval was made in January 2021 for a request that was received in December 2020, that approval was counted in the CY2020 number.
- **DENIED IN FULL** are requests denied in their entirety. This includes denials that occurred in January following the reported calendar year for requests that were initially received in preceding year (akin to approvals).
- **WITHDRAWN IN FULL** are requests that are withdrawn or cancelled by the requesting entity in their entirety. This includes withdrawals that occurred in January following the reported calendar year for requests that were initially received in preceding year (akin to approvals).
- **PENDING DECISIONS** are requests where there is no final decision made because (a) the receiving IC element has not reviewed or decided on the request or (b) the receiving IC element asked the requesting entity for additional information to process the request and is waiting for such information.

FISA Criminal Use and Notice Provisions

A. FISA Sections 106 and 305

FISA Section 106 requires advance authorization from the Attorney General before any information acquired through Title I electronic surveillance may be used in a criminal proceeding. This authorization from the Attorney General is defined to include authorization by the Acting Attorney General, Deputy Attorney General, or, upon designation by the Attorney General, the Assistant Attorney General for National Security. Section 106 also requires that if a government entity intends to introduce information obtained or derived from electronic surveillance into evidence in any trial, hearing, or other proceeding, against an “aggrieved person,” as defined by FISA, it must notify the aggrieved person and the court. The aggrieved person is then entitled to seek suppression of the information. FISA Section 706 requires that any information acquired pursuant to Section 702 be treated as electronic surveillance under Section 106 for purposes of the use, notice, and suppression requirements.

FISA Section 305 provides comparable requirements for use of information acquired through Title III physical search (i.e., advance authorization, notice, and opportunity to suppress) in a legal proceeding.

B. Statistics

The FISA Amendments Reauthorization Act of

FISA Sections 106 and 305 Criminal Use and Notice Provisions

- Commonly referred to as the “criminal use provision.”
- Section 106 applies to information acquired from Title I electronic surveillance and Section 702; Section 305 applies to information acquired from Title III physical search.
- Attorney General advance authorization is required before such information may be used in a criminal proceeding; if such information is used or intended to be used against an aggrieved person, that person must be given notice of the information and have a chance to suppress the information.
- The FISA Amendments Reauthorization Act of 2017 codified that statistics must be provided to the public as they pertain to Section 106 and Section 305, as well as Section 702 acquired information.

2017 codified a requirement that certain statistics concerning criminal proceedings must be provided to the public pertaining to Sections 106 and 305, including Section 702-acquired information.

Figure 14: Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Certain FISA Information

FISA Sections 106 and 305	CY2018	CY2019	CY2020
The number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to Section 106 (including with respect to Section 702-acquired information) or Section 305 of the government’s intent to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or Section 702 acquisition	14	7	9

See 50 U.S.C. § 1873(b)(4).

FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices

A. FISA Pen Register/Trap and Trace Authority

Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to capture dialing, routing, addressing or signaling (DRAS) information. Title IV does not authorize the use of PR/TT devices to collect the contents of communications. For example, a PR/TT could be used to acquire the phone numbers, dates, and lengths of calls that were set to or received by a specified phone number, but not the content of the calls. The government may submit an application to the FISC for an order approving the use of a PR/TT device for (i) “any investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1842(a). If the FISC finds that the government’s application meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device. FISC orders and opinions authorizing the government’s use of PR/TT devices may be found on *IC on the Record* (for example in a [September 27, 2017 posting](#)) and on [Intel.Gov’s Intel Vault](#) page.

B. Statistics

COUNTING ORDERS. Similar to how orders were counted for Titles I and III and Sections 703 and

FISA Title IV

- Commonly referred to as the “PR/TT” provision.
- Bulk collection is prohibited.
- Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.
- Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.

704, this report only counts the orders granting authority to conduct intelligence collection -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

ESTIMATING THE NUMBER OF TARGETS. The government’s methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not four.

Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

House Report on the USA FREEDOM Act states that “[t]he phrase ‘unique identifiers used to communicate information collected pursuant to such orders’ means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders - not just the number of target email addresses or phone numbers.” *H.R. Rep. No. 114-109*, pt. I, at 26 (with certain exceptions noted).

ESTIMATING THE NUMBER OF UNIQUE IDENTIFIERS. This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and email addresses) that were in contact with the targeted identifiers. Specifically, the

Figure 15a: PR/TT Orders, Targets, and Unique Identifiers Collected

Title IV of FISA	CY2018	CY2019	CY2020
Total number of orders	34	22	15
Estimated number of targets of such orders	29	21	8
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*, **	132,690	96,995	53,824

See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

*Pursuant to 50 U.S.C. §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include email addresses or telephone numbers.

**This number is generated from the FBI's systems that hold unminimized PR/TT collection. For every docket that resulted in the acquisition of PR/TT data, the collection was uploaded into these systems.

Figure 15b: PR/TT Orders and Targets

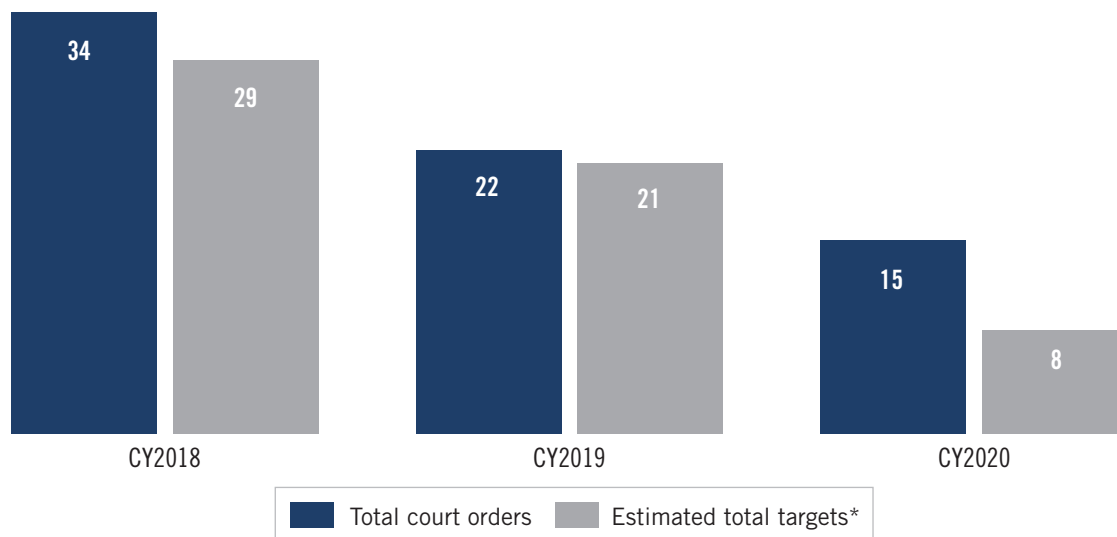


Figure 16: FISA PR/TT Targets – U.S. Persons and Non-U.S. Persons

PR/TT Targets	CY2018	CY2019	CY2020
Estimated number of targets who are non-U.S. persons	15	8	5
Estimated number of targets who are U.S. persons	14	13	3
Estimated percentage of targets who are U.S. persons	48.3%	61.9%	37.5%

See 50 U.S.C. §§1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii) for rows one and two, respectively.

FISA Title V – Business Records

A. Business Records FISA

Title V of FISA, commonly referred to as the “Business Records” provision of FISA, authorizes the government to submit an application for an order requiring the production of certain records. Title V was added to FISA in 1998 and subsequently expanded in 2001 by the USA PATRIOT Act. The legal regime for Title V is particularly complicated at this time because on March 15, 2020, the expanded USA PATRIOT Act version of Title V expired for some investigations but not others, such that there are now in effect two applicable legal regimes for the acquisition of records.

With respect to the acquisition of records in an investigation initiated prior to March 15, 2020, or that is investigating offenses that began or occurred before March 15, 2020, the expanded USA PATRIOT Act version of Title V remains available. That means that the government may apply to the FISC for an order to obtain “any tangible thing” that is relevant to (i) “an investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” Such business record requests for tangible things may include books, records (e.g., electronic communications transactional records), papers, documents, and other items. Bulk acquisition of records is prohibited and a business record order must identify a “specific selection term” to narrow the scope of the collection.

For investigations initiated on or after March 15, 2020, or that are not investigating offenses that began or occurred before March 15, 2020, the

USA PATRIOT Act version of Title V is no longer available, meaning that the pre-USA PATRIOT Act version applies. For such investigations, instead of being able to apply for an order to obtain “any tangible thing,” the government may only seek to obtain records from (1) common carriers (e.g., an airline or a bus company, not a telecommunications company); (2) public accommodation facilities (e.g., hotels); (3) physical storage facilities; and (4) vehicle rental facilities. Instead of relevance to the investigation, the government must also provide specific and articulable facts giving reason to believe that the person to whom the records pertain is either a foreign power or an agent of a foreign power.

In addition, a separate authority to acquire a certain type of record, call detail records (CDRs), under a different mechanism also expired in March 2020. As previously discussed in last year’s Annual Statistical Transparency Report, in August 2019, NSA suspended use of the CDR authority and deleted previously acquired call detail records. Thus, given the NSA’s suspense of its Title V authority and obtaining CDRs in 2019 as well as the expiration of the underlying authority in March 2020, there are no statistics to report for calendar year 2020 pertaining to CDRs. **More specifically, in calendar year 2020, there were no court orders authorizing use of the CDR authority, previously codified at 50 U.S.C. § 1861(b)(2)(C), no call detail records acquired pursuant to this authority, and no queries of previously acquired CDR holdings because these records were deleted in 2019.**

B. Statistics – Title V Business Records Statistics Orders, Targets & Identifiers

As discussed above, aspects of the business records authority expired on March 15, 2020. The

following statistics regard business records orders obtained both before and after the partial expiration of the business records authority.

ESTIMATING THE NUMBER OF UNIQUE IDENTIFIERS. This is an estimate of the number of (1) targeted identifiers used to communicate information (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. The number of identifiers used by targets to communicate can vary significantly from year to year, which in turn will impact the number of non-targeted identifiers in contact with the targeted identifiers. The government also may obtain under Title V other types of tangible things from entities other than communication service providers. For example, the FBI could obtain, under this authority and if pertaining to an investigation initiated prior to March 15, 2020, a hard copy of a purchase receipt or surveillance video from a retail store. The purchase receipt or surveillance video could contain a unique identifier such as a telephone number, which would not be counted. Nevertheless, such tangible things would not include many, if any, unique identifiers used to communicate information and,

therefore, the figures reported constitute a good faith estimate.

EXPLAINING HOW THE GOVERNMENT COUNTS BUSINESS RECORDS STATISTICS. As an example of the government’s methodology, assume that in a given calendar year, the government submitted a BR request targeting “John Doe” with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records. Provider X returned 10 nontargeted email addresses that were in contact with the target; provider Y returned 10 nontargeted email addresses that were in contact with the target; and provider Z returned 10 nontargeted email addresses that were in contact with the target. Based on this scenario, the government would report the following statistics: A) one order by the FISC for the production of tangible things, B) one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

Figure 17a: Title V Business Records Orders, Targets, and Unique Identifiers Collected

Business Records – Section 501(b)(2)(B)	CY2018	CY2019	CY2020
Total number of business records orders issued pursuant to applications under Section 501(b)(2)(B)	56	61	28*
Estimated number of targets of such orders	60	53	25
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	214,860	66,719**	7,654

See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).

* As discussed above, for CY2020 this number reflects the number of business records orders (and associated unique identifiers collected) under Section 501(b)(2)(b) and the number of business records orders authorized pursuant to Section 502 for investigations initiated on or after March 15, 2020.

** The CY2019 number for unique identifiers has been corrected to reflect some unique identifiers that were mistakenly not reported last year. Last year’s report reported 57,382 unique identifiers. However, the FBI subsequently identified a production that had not been uploaded to an FBI database. As a result, the number of unique identifiers (9,337) in that production were not reported in last year’s number of unique identifiers. The updated CY2019 number now includes these additional unique identifiers. Last year’s numbers regarding the total number of business record orders and estimated number of targets of such orders remain the same. As a result of the omission, FBI has instituted a new process to identify and account for any productions that may not have been uploaded into an FBI system. FBI applied this new process prior to reporting its CY2020 numbers to ODNI. In addition, when the FBI identified the production that was not included in last year’s report, it determined that the recipient of the FISC order produced approximately 8,982 additional unique identifiers that were not subject to the order. Because those unique identifiers were not subject to the FISC’s order, the government has purged those records from its systems and the overproduced data is no longer available for review or dissemination. As a result, although the estimated number of unique identifiers for 2019 includes the overproduction and is reported as 66,719, the actual number of unique identifiers remaining in the FBI’s systems does not include the 8,982 overproduced unique identifiers.

Figure 17b: Title V Business Records Orders and Targets

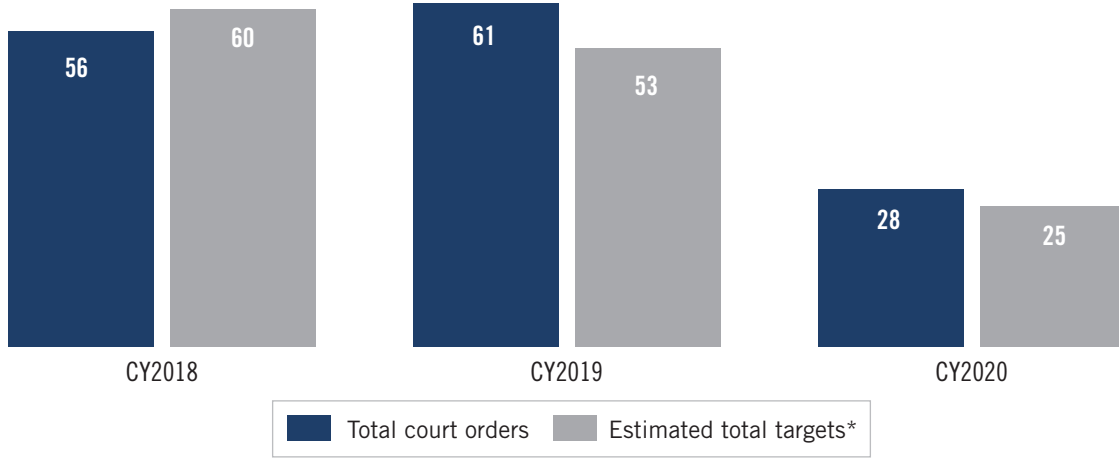
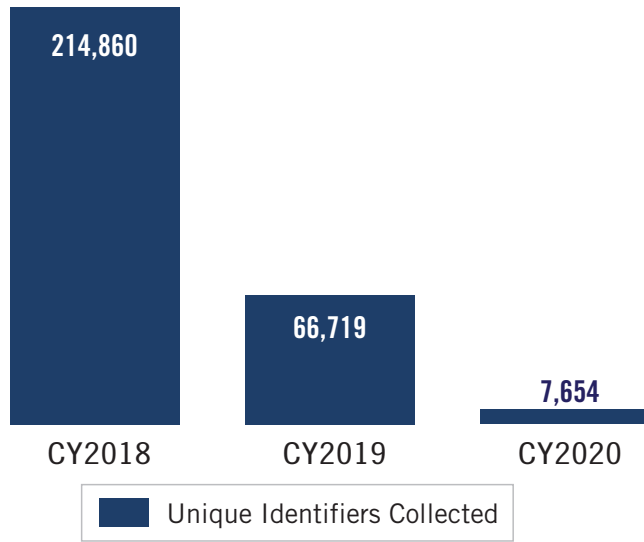


Figure 17c: Title V Business Records Unique Identifiers Collected



National Security Letters (NSLs)

A. National Security Letters

In addition to statistics relating to FISA authorities, the government also reports information on its use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

- ▶ 1) Telephone subscriber information, toll records, and other electronic communication transactional records, *see* 18 U.S.C. § 2709;
- ▶ 2) Consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), *see* 15 U.S.C. § 1681u;
- ▶ 3) Full credit reports, *see* 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
- ▶ 4) Financial records, *see* 12 U.S.C. § 3414.

B. Statistics – National Security Letters and Requests for Information

COUNTING NSLS. Today, the government is reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple ROIs, each is considered a “request” and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three email addresses for the provider to return records, this would count as one NSL issued and three ROIs.

THE DEPARTMENT OF JUSTICE’S REPORT ON NSLS. In April 2021, the Department of Justice released its

National Security Letters

- Not authorized by FISA but by other statutes.
- Bulk collection is prohibited, however, by the USA FREEDOM Act.
- FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.

Annual Foreign Intelligence Surveillance Act Report to Congress. That report, which is available online, provides the *number of requests* made for certain information concerning different U.S. persons pursuant to NSL authorities during calendar year 2020. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

WHY THE GOVERNMENT REPORTS THE NUMBER OF NSL REQUESTS INSTEAD OF THE NUMBER OF NSL TARGETS.

The government reports the annual number of requests for multiple reasons. First, the FBI’s systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider

may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of an account. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

Additionally, the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a),(b), 15 U.S.C. § 1681v, and 18 U.S.C.

§ 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple email accounts, landline telephone numbers, and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

As is the case with other statistics in this report, statistics often fluctuate from year to year for a variety of reasons. The IC is committed to sharing statistical data and engaging the public about how the IC uses its national security authorities and for what purposes.

Figure 18a: Table of NSLs Issued and Requests for Information

National Security Letters	CY2018	CY2019	CY2020
Total number of NSLs issued	10,235	13,850	9,682
Number of ROI	38,872	63,466	24,225

See 50 U.S.C. § 1873(b)(6).

Figure 18b: Chart of NSLs Issued and Requests for Information

