



*Office of the Director of National Intelligence*

# ANNUAL STATISTICAL TRANSPARENCY REPORT

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

————— Calendar Year 2021 —————

Office of Civil Liberties, Privacy, and Transparency

April 2022

# Table of Contents

<b>Executive Summary</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<i>A. Background</i> .....	5
<i>B. Areas Covered in this Report</i> .....	5
<i>C. Statistical Fluctuations Over Time</i> .....	6
<i>D. Key Terms</i> .....	6
<b>FISA Probable Cause Authorities</b> .....	<b>10</b>
<i>A. FISA Titles I and III</i> .....	10
<i>B. FISA Title VII, Sections 703 and 704</i> .....	10
<i>C. Statistics</i> .....	11
<b>FISA Section 702</b> .....	<b>13</b>
<i>A. Section 702</i> .....	13
<i>B. Statistics—Orders and Targets</i> .....	16
<i>C. Statistics—U.S. Person Queries</i> .....	17
<i>D. Section 702 and FBI Investigations</i> .....	23
<i>E. NSA Dissemination of U.S. Person Information under FISA Section 702</i> .....	24
<b>IC Dissemination of U.S. Person Information</b> .....	<b>28</b>
<i>A. ICPG 107.1</i> .....	28
<i>B. Statistics</i> .....	28
<b>FISA Criminal Use and Notice Provisions</b> .....	<b>30</b>
<i>A. FISA Sections 106 and 305</i> .....	30
<i>B. Statistics</i> .....	30
<b>FISA Title IV—Use of Pen Register and Trap and Trace (PR/TT) Devices</b> .....	<b>32</b>
<i>A. FISA Pen Register/Trap and Trace Authority</i> .....	32
<i>B. Statistics</i> .....	32
<b>FISA Title V—Business Records</b> .....	<b>34</b>
<i>A. Business Records FISA</i> .....	34
<i>B. Statistics—Title V “Traditional” Business Records Statistics Orders, Targets &amp; Identifiers</i> .....	34
<b>National Security Letters (NSLs)</b> .....	<b>36</b>
<i>A. National Security Letters</i> .....	36
<i>B. Statistics—National Security Letters and Requests for Information</i> .....	36

# Table of Figures

*Figures 1: FISA “Probable Cause” Court Orders and Targets..... 11*

*Figures 2: FISA “Probable Cause” Targets Broken Down by U.S. Person Status..... 12*

*Figure 3: Section 702 Orders ..... 17*

*Figure 4: Section 702 Targets ..... 17*

*Figure 5: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Contents..... 18*

*Figure 6: U.S. Person Query Terms Used to Query Section 702 Contents by CIA, NCTC, and NSA ..... 18*

*Figure 7: How the IC counts U.S. Person Queries of Section 702 Noncontents..... 19*

*Figure 8: U.S. Person Queries of Noncontents of Section 702 by CIA and NSA ..... 19*

*Figure 9: FBI U.S. Person Queries ..... 21*

*Figure 10: FBI Review of Section 702 Query Results Requiring FISC Orders ..... 22*

*Figure 11: Accessing the Results of FBI U.S. Person Evidence of a Crime Only Section 702 Queries ..... 23*

*Figure 12: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition ..... 24*

*Figure 13: Section 702 Reports Containing USP Information Unmasked by NSA..... 26*

*Figure 14: Section 702 USP Identities Disseminated by NSA ..... 27*

*Figures 15: Requests for U.S. Person Identities and Decisions Regarding those Requests per ICPG 107. .... 29*

*Figures 16: Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Certain FISA Information ..... 31*

*Figure 17a: PR/TT Orders, Targets, and Unique Identifiers Collected ..... 33*

*Figure 17b: FISA PR/TT Targets - U.S. Persons and Non-U.S. Persons ..... 33*

*Figures 18: Title V Business Records Orders, Targets, and Unique Identifiers Collected ..... 35*

*Figures 19: NSLs Issued and Requests for Information..... 37*

## Executive Summary

The *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities* provides statistics and contextual information concerning how the Intelligence Community uses the *Foreign Intelligence Surveillance Act* and certain other national security authorities to accomplish its mission. The report also describes the circumstances under which such 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 Intelligence Community endeavors to enhance public understanding of intelligence activities by adding further context to other publicly released materials regarding the oversight framework.

This is the **ninth** such transparency report. The government is releasing this report consistent with Section 603(b) of the *Foreign Intelligence Surveillance Act of 1978, as amended* (codified in 50 U.S.C. § 1873(b)), and the Intelligence Community's [Principles of Intelligence Transparency](#).

Select Calendar Year (CY) 2021 Statistics Included in this Report:

Authority	CY2021 Number of Court Orders	CY2021 Number of Targets
FISA Titles I and III and Sections 703 and 704 "Probable Cause"	430	376
FISA Section 702	0	232,432 (Non-US persons only)
FISA Title IV "Pen Register and Trap and Trace"	10	6
FISA Title V – Section 501(b)(2)(B) "Business Records"	11	13

FISA Section 702 – Queries	CY2021
Estimated Number of U.S. Person Terms Used to Query Unminimized Section 702-Acquired Contents (excluding FBI)	8,790
Estimated Number of U.S. Person Queries of Unminimized Section 702-Acquired Noncontents (excluding FBI and NCTC)	3,958
Estimated Number of U.S. Person Queries of Unminimized Section 702-Acquired Contents and Noncontents (only FBI)	Fewer than 3,394,053
U.S. Person Queries of Unminimized Section 702-Acquired Contents by FBI in which Post Query Documented Justifications to Access Query Results Indicated an Evidence of a Crime Only Purpose for the Query	12

# Introduction

Consistent with the *Foreign Intelligence Surveillance Act of 1978, as amended* (FISA) ([50 U.S.C. §§ 1801 et seq.](#)), specifically, Section 603(b) (codified at [50 U.S.C. § 1873\(b\)](#)) and the Intelligence Community's (IC) *Principles of Intelligence Transparency*, the government is releasing its **ninth Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities (hereafter the *Annual Statistical Transparency Report*) presenting statistics on how often the government uses certain national security authorities, including FISA. These statistics add further context to the rigorous and multi-layered oversight framework, including oversight conducted by independent judicial and legislative entities, which is designed to safeguard 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-U.S. persons are afforded privacy protections based on the different authorities discussed herein.**

This report goes beyond FISA's statutory reporting requirements, providing the public with detailed explanations as to how the IC uses its national security authorities and metrics that add context to current public discussions. This document should be read in conjunction with previously released national security-related materials, particularly those hyperlinked throughout, as well as the statistical report provided by the Director of the Administrative Office of the U.S. Courts (AOUSC), *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, [dni.gov](#), and the IC's transparency portal, [intel.gov](#). [ODNI's Guide to Posted Documents](#) offers a topical index of significant public releases.

## 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 the *Annual Statistical Transparency Report*. The 2014 report and subsequent annual reports are available [here](#).

In June 2015, Congress enacted the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015* (USA FREEDOM Act), amending FISA to formally require the government to publicly report 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\(b\)](#).

In January 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 the *Annual Statistical Transparency Report* provides statistics describing the use of a variety of national security authorities, the report predominantly concerns the government's use of FISA.



FISA 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 the collection and use of 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.

In addition to reporting statistics regarding the use of FISA authorities, this report also provides statistics regarding requests to unmask 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. 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 the impact of the COVID-19 pandemic likely influenced target behavior, which in turn affected some of the numbers reported this year.

### *D. Key Terms and Concepts*

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 have specifically defined meanings in the context of the IC's use of its collection authorities and 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 603(e)(4) of FISA, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization or querying 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 selector, such as a telephone number or email address, regarding which the government is seeking collection.

The IC also uses the term “target” as a verb. For example, Section 702 authorizes the targeting of (i) non-U.S. 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 to be applied to each individual targeting decision.

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; it facilitates 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, determines the overall priorities of the top-level NIPF issues.

Prior to targeting, 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) and not prohibited by other legal authorities (*e.g.*, PPD-28).

- **FOREIGN INTELLIGENCE INFORMATION.** Under FISA, “foreign intelligence information” is information that relates to (and if concerning a U.S. person, is necessary to) the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power; sabotage, international terrorism, or the intentional proliferation of weapons of mass destruction by a foreign power or agent of a foreign power; clandestine intelligence activities by an intelligence service or intelligence network of a foreign power or by an agent of a foreign power; or information that relates to (and if concerning a U.S. person, is necessary to) the national defense or the security of the United States or the conduct of the foreign affairs of the United States. 50 U.S.C. § 1801(e).
- **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.
- **UNMINIMIZED INFORMATION.** Unminimized information is lawfully collected information for which a determination has not been made as to whether it contains foreign intelligence information or whether it may be otherwise retained pursuant to the agency’s minimization procedures.
- **DISSEMINATION.** Dissemination refers to the sharing of foreign intelligence information or evidence of a crime.

- **FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC).**

The FISC was established in 1978 when Congress enacted FISA (*see* 50 U.S.C. §§ 1801-1885c). The FISC is composed of eleven federal district court judges who are designated by the Chief Justice of the United States. Pursuant to FISA, the FISC reviews applications submitted by the U.S. Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. The FISC also conducts oversight by assessing the government's use of FISA authorities. The FISC uses a variety of tools to conduct such assessments, including mandating that the government report information on every identified compliance incident, implementing specialized reporting requirements to monitor certain aspects of FISA activities, and convening hearings. Based upon its assessment, the FISC can terminate, modify, or limit the government's authority to use FISA and may also require the government to devise and report on remedial measures related to identified instances of noncompliance.

- **FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW (FISC-R).** Also established in 1978 when Congress enacted FISA, the FISC-R acts as court of review for the FISC. It consists of three federal district or circuit court judges who review decisions of the FISC. FISC-R decisions may be appealed to the U.S. Supreme Court.
- **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 collect foreign intelligence 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 or briefing orders requiring the government to take a particular action or provide the FISC with specific information. As in 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 collection 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 *does* count each such renewal as a separate order granting the requested FISA authority.

### At a Glance: Foreign Intelligence Surveillance Court (FISC)

- Established in 1978.
- Comprised of 11 federal district court judges.
- Authorizes and oversees the government's use of the FISA authorities – electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes.



- **MASKED U.S. PERSON INFORMATION.** An 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 privacy and civil liberties.
- **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 identifying 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.** FISC amici are technical experts (individuals or organizations) in the areas of privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical insight to a matter under consideration by the FISC or FISC-R. 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 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. 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.

### At a Glance: Masking

- Substitution of a U.S. person's identity with a generic phrase.
- This is done to protect the U.S. person's civil liberties and privacy while allowing IC elements to disseminate appropriate intelligence.
- Example: Reporting of Section 702-acquired information states that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person" – instead of the person's actual name.

# 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, 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 and 1823. Title I (electronic surveillance) and Title III (physical search) are 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) and 1823(a). 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 [intel.gov](https://www.intel.gov) (e.g., in postings in [September 2017](#), [July 2020](#), [August 2020](#), and [September 2020](#)).

### 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.
- Individual courts orders are required; bulk collection is not permitted.

## B. FISA Title VII, Sections 703 and 704

Sections 703 and 704 of FISA Title VII similarly require an individualized 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 target a U.S. person who is reasonably believed to be located outside the United States in order to acquire foreign intelligence information if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data inside the United States, in a manner that otherwise requires an order under FISA. 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

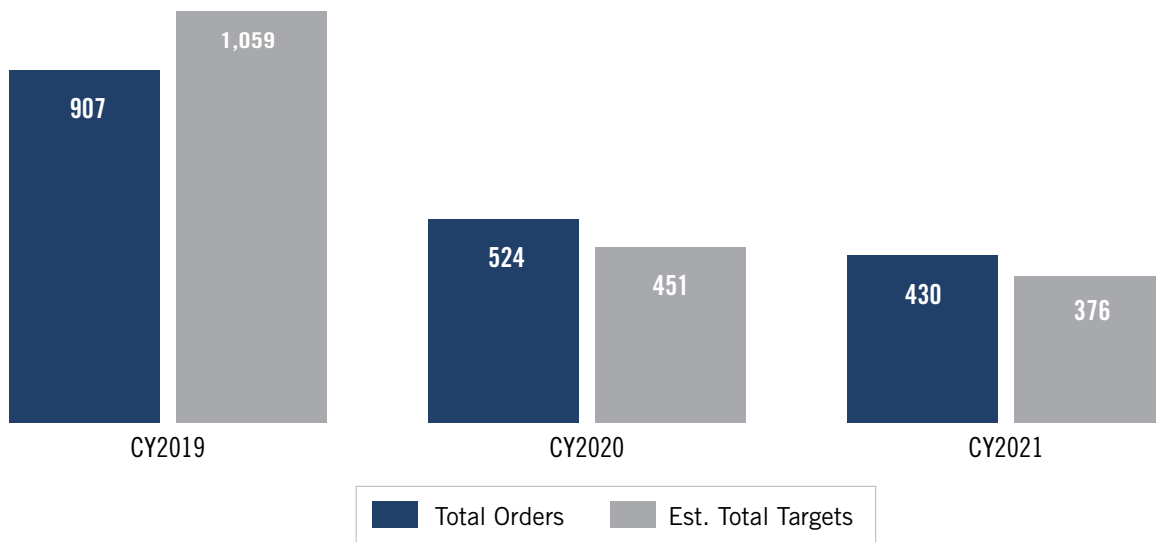
the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power. Additionally, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1881b(b) and 1881c(b).

**C. Statistics**

**HOW TARGETS ARE COUNTED.** If the IC received authorization to conduct electronic surveillance or physical search against the same target in four separate applications, the IC counts this as 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 counts this as four targets.

**HOW ORDERS ARE COUNTED.** The number of court orders is not dependent on the number of targets authorized in a single order, nor is it reduced if the court order concerns a target for whom a prior order has been obtained by the government. As such, four orders authorizing collection on a single target are counted as four orders. Alternatively, one order authorizing collection on four targets is counted as a single order.

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



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

**U.S. PERSON STATUS:** While Section 703 and Section 704 apply only to U.S. person targets, Titles I and III of FISA govern electronic surveillance and physical searches (as defined by FISA) within the United States of both U.S. persons and non-U.S. persons. The following figure breaks down the number and percentage of targets by U.S. person status.

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

Titles I and III and Sections 703 and 704—Targets	CY2019	CY2020	CY2021
Estimated number of targets who are <i>non</i> -U.S. persons <i>See</i> 50 U.S.C. § 1873(b)(1)(B).	892	349	<b>309</b>
Estimated number of targets who are U.S. persons <i>See</i> 50 U.S.C. § 1873(b)(1)(C).	167	102	<b>67</b>
Percentage of targets who are estimated to be U.S. persons	15.8%	22.6%	<b>17.8%</b>

## 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 requirements 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 an application package. This package contains a certification detailing the type of information to be collected along with targeting, minimization, and querying procedures. Individual targeting decisions are required; bulk collection is not permitted. Additional information on how the government uses Section 702 is posted on intel.gov's IC on the Record, including FISC orders and opinions approving the government's use of this authority, most recently in [April 2021](#).

**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 (for example, telephone numbers and email addresses) used by the target. 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 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.

### 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.
- Individual targeting decisions are required; bulk collection is not permitted.



signals intelligence activities continue to include appropriate safeguards for the personal information of all individuals, regardless of nationality or residency.

The National Security Agency (NSA) and Federal Bureau of Investigation (FBI) task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized Section 702 data – NSA, FBI, the Central Intelligence Agency (CIA), and the 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, the FISC considers every identified compliance incident reported by the government through notices and reports, other reports concerning 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 [March 2022](#), on [intel.gov](https://www.intel.gov), 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 the FISC remains aware of how the government is implementing 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, the FISC issues an order and opinion 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.

**CERTIFICATIONS.** Under Section 702, the Attorney General and DNI jointly execute certifications, good for one year from the date of approval, 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 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 noncompliance with the targeting procedures are reported to the FISC regardless of a target's citizenship or U.S. person status. Such reporting to the FISC includes 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.

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 a targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why they are seeking to target a person. 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 the selector is being tasked. The TAR is reviewed by the Department of Justice (DOJ) oversight team as part of its 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](#) last released on intel.gov's IC on the Record in March 2022. [NSA's 2020 targeting procedures and FBI's 2020 targeting procedures](#) were publicly released on intel.gov's 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. As noted above, 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 on 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](#) were released on intel.gov 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.

Query terms may be date-bound and may include alphanumeric strings (e.g., telephone numbers or email addresses) or terms (e.g., 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. The [2020 querying procedures](#) were released 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 on intel.gov.

## ***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 counts 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 requests that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing its report.

As noted in Figure 3, the FISC did not issue any Section 702 orders in 2021. Pursuant to its authority under 50 U.S.C. § 1881a(k)(2), the FISC chose to extend its review of the 2021 certification application package, an authority that may be exercised "as necessary for good cause in a manner consistent with national security." Pending FISC review of the certification application package, the 2020 certification

order remained in effect throughout the extension period. A similar extension occurred in 2016, which was detailed in previous *Annual Statistical Transparency Reports*.

**Figure 3: Section 702 Orders**

Section 702 of FISA	CY2019	CY2020	CY2021
Total number of orders issued <i>See 50 U.S.C. § 1873(b)(2)</i>	2	1	0

**ESTIMATING SECTION 702 TARGETS.** The number of Section 702 targets reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on the following methodology. 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 4: Section 702 Targets (recall that only non-USPs are targeted)**

Section 702 of FISA	CY2019	CY2020	CY2021
Estimated number of targets of such orders <i>See 50 U.S.C. § 1873(b)(2)(A)</i>	204,968	202,723	<b>232,432</b>

### C. Statistics—U.S. Person Queries

The USA FREEDOM Act requires the government to report 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 [...]” of Section 702-acquired communications and data. *See 50 U.S.C. §§ 1873(b)(2)(B) and (b)(2)(C)*, respectively. FISA exempts FBI queries of contents and noncontents from this statutory reporting requirement. *See 50 U.S.C. § 1873(d)(2)(A)*. Changes in FBI’s systems documenting the assessed U.S. person status associated with query terms, however, now permit FBI to identify the number of U.S. person queries conducted against unminimized Section 702-acquired information. For reasons discussed more fully below, these statistics are reported separately from NSA, CIA, and NCTC due to unique variations in FBI’s data, chief among them that FBI does not count the number of unique query terms, but instead counts the total number of queries, which could include duplicate queries of the same term. Consistent with the *Principles of Intelligence Transparency*, the DNI has declassified these FBI statistics and related information regarding the FBI’s use of queries.

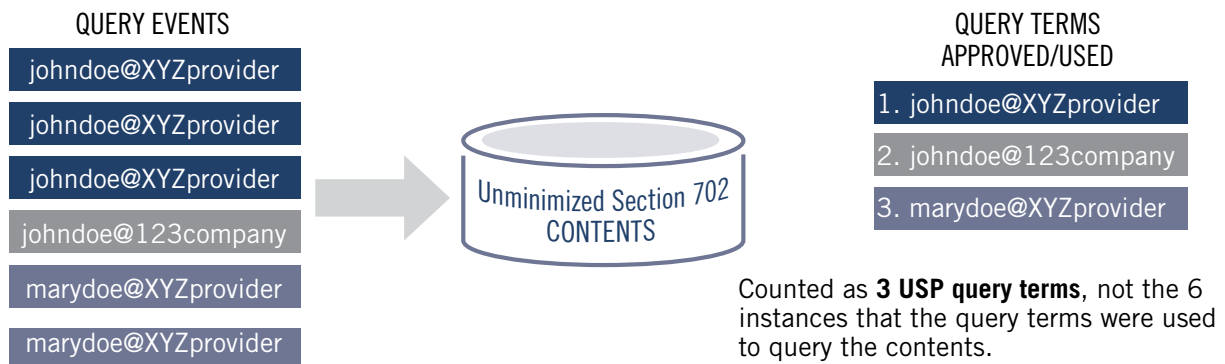
#### U.S. PERSON QUERIES BY NSA, CIA, AND NCTC.

**THE DIFFERENCE BETWEEN U.S. PERSON QUERIES OF CONTENTS AND NONCONTENTS.** Below are statistics for U.S. person queries of unminimized Section 702-acquired data. The U.S. person statistics are based on (a) U.S. person *query terms* used to query Section 702 *contents* 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 combined because they use *different counting methodologies* (query terms versus

queries conducted) and *different data types* (contents versus noncontents). Figures 5 and 7 illustrate the differences.

**COUNTING U.S. PERSON QUERY TERMS USED TO QUERY SECTION 702 CONTENTS.** NSA counts the number of U.S. person identifiers it has approved to query the contents of unminimized Section 702-acquired information. For example, if NSA approved U.S. person identifier “johndoe@XYZprovider” to query the contents of unminimized Section 702-acquired information, NSA would count it as one query term regardless of how many times NSA used “johndoe@XYZprovider” to query its unminimized Section 702-acquired information. Not every query term *approved*, however, is ultimately used. By contrast, 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 Contents**



**Figure 6: U.S. Person Query Terms Used to Query Section 702 Contents by CIA, NCTC, and NSA**

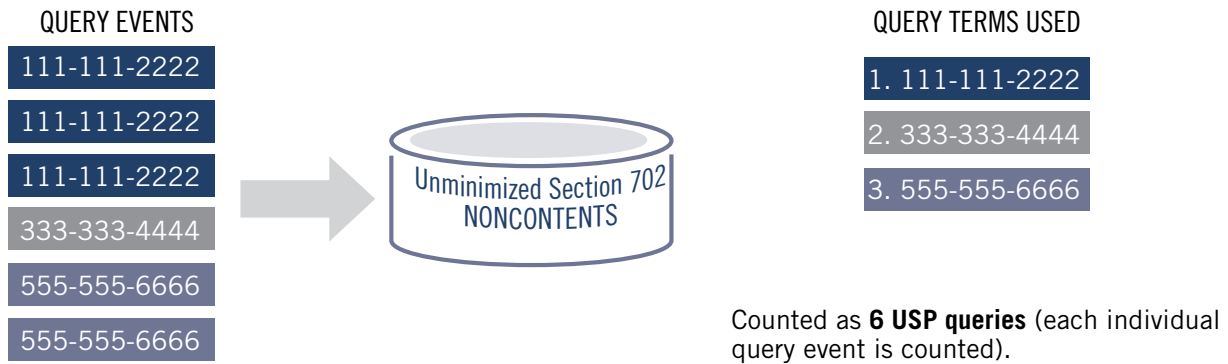
Section 702 of FISA	CY2019	CY2020	CY2021
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information) <i>See 50 U.S.C. § 1873(b)(2)(B).</i>	9,299	7,218	<b>8,790</b>

NCTC queries both contents and noncontents together and has included all of its U.S. person query data in Figure 6.

**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 was 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 unminimized 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 by CIA and NSA**

Section 702 of FISA	CY2019	CY2020	CY2021
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) <i>See 50 U.S.C. § 1873(b)(2)(C).</i>	16,545	9,051	<b>3,958</b>

As noted above, NCTC runs all queries against both contents and noncontents and has, therefore, included all of its U.S. person query data in Figure 6. As such, Figure 8 does not include NCTC data.

**U.S. PERSON QUERIES CONDUCTED BY THE FBI.**

For the first time, the *Annual Statistical Transparency Report* now includes the number of queries using U.S. person identifiers run by FBI against unminimized Section 702 collection. Understanding that U.S. person queries represent an activity that is particularly relevant to the FISC’s compliance assessments, in its November 18, 2020 Opinion and Order, the FISC expanded quarterly reporting requirements to include “the number of U.S. person queries run by the FBI against Section 702-acquired information.” FBI system changes now allow for the capture of the information requested by the FISC.

FBI U.S. person queries are being reported separately from NSA, CIA, and NCTC. There are several factors that differentiate FBI from the other agencies.

- **DIFFERENT STANDARD DUE TO DUAL LAW ENFORCEMENT AND INTELLIGENCE MISSIONS.** FBI’s standard for conducting queries of unminimized Section 702-acquired information is fundamentally different from that of the other agencies. Where NSA, CIA, and NCTC are authorized to query Section 702-acquired contents and noncontents for foreign intelligence information, FBI is authorized to conduct queries that are both reasonably likely to return foreign intelligence information and, as discussed in greater depth in the following subsection, queries that are reasonably likely to return evidence of a crime. FBI queries for evidence of a crime have been permitted pursuant to the FISC-approved FBI Section 702 minimization procedures, and now querying procedures, since 2009. *See* October 2018 FBI

Minimization Procedures; *see also* Memorandum Opinion issued on April 7, 2009, at 14-17. This broader query authority is a result of FBI's dual law enforcement and intelligence mission. "Such queries are permitted in part to ensure that the FBI does not fail to identify the foreign-intelligence significance of information in its possession." *See* FISC Memorandum Opinion and Order issued on November 6, 2015, at 42.

- **DIFFERENT FREQUENCY DUE TO DOMESTIC-FOCUSED MISSION.** While FBI receives Section 702 collection for only a small percentage of the total Section 702 targets (approximately 4.4% in March 2022), the frequency with which FBI uses U.S. person query terms is greater than other agencies. The difference in frequency is largely attributable to FBI's domestic-focused mission versus the other agencies' foreign-focused missions. FBI queries are often initiated through tips and leads relating to domestic matters, provided by the public and domestic partners, meaning they are more likely to involve U.S. persons.
- **DIFFERENT COUNTING METHODOLOGIES.** FBI does not currently have the capability to identify the number of unique U.S. person query terms, only the total number of queries, which may include duplicate queries. Unlike NSA, CIA, and NCTC, if FBI runs the same query term five times against Section 702-acquired content, this is counted as five queries, not one query term. In addition, unlike NSA and CIA but comparable to NCTC, FBI queries are run against content and noncontent.
- **DIFFERENT TIMING OF REPORTING DUE TO FISC ORDER.** Certain statistical information regarding FBI queries is tracked and reported quarterly from December 1 to November 30 and, therefore, does not align with the calendar year reporting done for other agencies concerning their query numbers.

For these reasons, FBI U.S. person query data is being reported separately.

Figure 9 provides statistics pertaining to the number of U.S. person queries of contents and noncontents that the FBI conducts to retrieve foreign intelligence information and/or evidence of a crime from unminimized Section 702-acquired collection. Because investigative activities can vary widely from year to year, the statistics are not necessarily representative of the number of such queries conducted in prior years or indicative of future investigative needs. Particular to calendar year 2021, there were two factors that contributed to significant fluctuations throughout the year. In the first half of the year, there were a number of large batch queries related to attempts to compromise U.S. critical infrastructure by foreign cyber actors. These queries, which included approximately 1.9 million query terms related to potential victims—including U.S. persons—accounted for the vast majority of the increase in U.S. person queries conducted by FBI over the prior year. A batch query is when FBI runs multiple query terms at the same time using a common justification for all of the query terms. Each of the query terms in a batch query is counted as a separate query. These particular large batch queries were reviewed by the Department of Justice and found to be compliant with the FBI's Section 702 querying procedures. Separately, in June and August, FBI made several changes to systems that store unminimized Section 702-acquired information designed to ensure compliance with FBI's Section 702 querying procedures. Specifically, FBI added an additional approval process for batch queries involving 100 or more query terms. FBI also modified two important systems that allow FBI to query across multiple datasets to require FBI personnel to affirmatively "opt-in" to querying unminimized FISA Section 702-acquired information. Following these changes, the average monthly number of FBI U.S. person queries run against unminimized Section 702-acquired collection decreased. All of the factors that coincided in 2021 provide examples of how the number of U.S. person queries may fluctuate in future years based upon both investigative needs and/or changes in policy and system design.

The number of FBI queries does not reflect the number of U.S. persons associated with these queries. For example, a single U.S. person might be associated with 10 unique query terms including name, social security number, passport number, phone number, multiple email addresses, etc. These 10 identifiers could be run 10 different times throughout the reporting period, resulting in 100 queries associated with a single individual. Query terms may also be associated with a U.S. company rather than a specific U.S. person.

Finally, certain steps FBI has taken to ensure U.S. person protections apply to all U.S. person queries result in an over counting of U.S. person queries. More specifically, FBI has the capability to run queries in which a single query action might include hundreds or thousands of query terms. FBI counts such query actions as hundreds or thousands of queries, not one query. However, if even one query term in such a query action is associated with a U.S. person, every term in the query action carries the U.S. person label. This means that if one term in a 100 term query action is associated with a U.S. person, the query action will be counted as 100 U.S. person queries, even if some of the query terms are not associated with a U.S. person. This system design ensures that all potential U.S. person query terms are captured, but results in an over counting of the number of U.S. person queries actually conducted by the FBI. For this reason, the total number of FBI U.S. person queries is referred to as “fewer than” the total number of queries labeled as U.S. person queries.

**Figure 9: FBI U.S. Person Queries**

Section 702 of FISA	December 2019 – November 2020	December 2020 – November 2021
Estimated number of U.S. Person queries of unminimized Section 702-acquired contents and noncontents for foreign intelligence information and/or evidence of a crime	<b>Fewer than 1,324,057</b>	<b>Fewer than 3,394,053</b>

**FBI U.S. PERSON QUERIES NOT DESIGNED TO RETURN FOREIGN INTELLIGENCE INFORMATION.**

As noted above, 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 that are reasonably likely to return foreign intelligence information. Recognizing that unrelated crimes can be discovered in the course of conducting FISA activities, Congress required that FISA minimization procedures contain provisions addressing how to treat evidence of unrelated crimes acquired in the course of a foreign intelligence activity. 50 U.S.C. § 1801(h)(3); *see, e.g., United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991) (permitting use in a state homicide case of FISA collection recordings of the target committing a murder unrelated to the foreign intelligence purpose for the collection). There are also instances for which the activity in which 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 have focused particular attention on instances in which FBI’s purpose at the time of the query is solely to retrieve evidence of a crime (*i.e.*, authorized queries that are “not designed to return foreign intelligence information”). There are two specific requirements related to these queries: (1) a statutory requirement for FBI to obtain a court order to review the results of evidence of a crime only queries related to a predicated criminal investigation and (2) a FISC quarterly reporting requirement to provide the number of U.S. person evidence of a crime only queries

whether or not they are associated with a predicated criminal investigation. Both are explained below with corresponding statistics.

**STATUTORY REQUIREMENT FOR THE FBI TO OBTAIN A FISC ORDER.** In the *FISA Amendments Reauthorization Act of 2017*, which was passed in January 2018, Congress required FBI to obtain an order from the FISC, also known as a Section 702(f)(2) order, before accessing the contents of Section 702-acquired communications when:

- (1) the communications were retrieved using a U.S. person query term;
- (2) the query was not designed to find and extract foreign intelligence information; and
- (3) the query was performed in connection with a predicated criminal investigation that does not relate to national security.

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 FISC issues an order approving access to the contents of the relevant communications “if the Court finds probable cause to believe that such contents would provide” evidence of a crime, contraband, fruits of a crime, items illegally possessed by a third party, or property designed for use, intended for use, or used in committing a crime. 50 U.S.C. § 1881a(f)(2)(D).

Figure 10 reports the number of these Section 702(f)(2) orders, obtained between December 1, 2020 and November 30, 2021, in order to align with current reporting periods required by the FISC and Congress for quarterly and semiannual reporting. New to this year’s report, Figure 10 also provides the number of instances in which compliance reviews identified that FBI accessed the contents of communications under circumstances requiring a Section 702(f)(2) order but did not obtain one. Such incidents of noncompliance are reported to the FISC as they are discovered. Compliance with the Section 702(f)(2) requirement continues to be a focus of DOJ’s and FBI’s training programs.

**Figure 10: FBI Review of Section 702 Query Results Requiring FISC Orders**

Section 702 of FISA	December 2020 - November 2021
<b>FISC ORDERS OBTAINED PURSUANT TO SECTION 702(F)(2)</b> to review the results of a query that 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 <i>See 50 U.S.C. § 1873(b)(2).</i>	0
<b>IDENTIFIED INSTANCES IN WHICH A FISC ORDER WAS REQUIRED PURSUANT TO SECTION 702(F)(2) BUT NOT OBTAINED PRIOR TO REVIEWING THE RESULTS OF A QUERY</b> that 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	4

**FBI FISC REPORTING REQUIREMENT.** Since 2015, prior to Congress’s passage of the Section 702(f)(2) court order requirement, the FISC has required separate FBI reporting relating to evidence of a crime queries. These reporting requirements have changed over time, but have generally been broader than the Section 702(f)(2) requirement to obtain a court order.

Currently, and as of November 2020, the FISC requires that the government include, in its quarterly reports, the number of U.S. person queries run by FBI against Section 702-acquired information

in which the post-query documented justifications to access the results of said queries indicated an evidence of a crime only purpose. Memorandum Opinion and Order dated November 18, 2020 at 63. This includes, but is broader than the Section 702(f)(2) requirement noted above as the evidence of a crime queries that must be reported to the FISC also include queries that are not linked to a predicated criminal investigation (for example, evidence of a crime only queries conducted when FBI is assessing, but has not yet opened, a predicated criminal investigation).

In other words, the statistic in Figure 11 includes all evidence of a crime only U.S. person queries in which responsive results were found and reviewed by FBI personnel, whether or not a Section 702(f)(2) order was required.

As was the case with the preceding charts for FBI's U.S. Person queries, the number of such queries reported includes queries conducted between December 2020 and November 2021, not calendar year 2021. As previously explained, this is due to the nature of the quarterly reporting periods required by the FISC. The comparable calendar year 2020 number is also provided for reference.

**Figure 11: Accessing the Results of FBI U.S. Person Evidence of a Crime Only Section 702 Queries**

Section 702 of FISA	CY2020	December 2020 – November 2021
Number of U.S. person queries in which post-query documented justifications to access query results indicated an evidence of a crime only purpose for the query	1	12

DOJ continues to assess the nature of these queries. Queries previously included in this category for quarterly reporting purposes may subsequently be determined to have been conducted for a foreign intelligence purpose. Additionally, queries identified as having a foreign intelligence purpose might subsequently be determined to have been conducted solely to retrieve evidence of a crime. Corrections made prior to February 28, 2022 are reflected in the numbers included in Figures 10 and 11.

While both the Figure 10 and Figure 11 statistics might appear small compared to those reported in Figure 9, there are two primary reasons why the comparatively low numbers in Figures 10 and 11 are an expected result. First, Section 702 collection targets non-U.S. persons located overseas. For U.S. person information to be found in Section 702 collection, the non-U.S. person target must either be conversing with or talking about a U.S. person. Second, a significant purpose of Section 702 collection must be to obtain foreign intelligence information. Any evidence of a crime unrelated to national security is generally secondary and ancillary to this purpose and is, therefore, less prevalent in the collection. Both of these factors support the conclusion noted by the FISC in its November 6, 2015 Memorandum Opinion and Order, at 44, that “FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from Section 702-acquired data.” See also, Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (PCLOB’s Section 702 Report) at 59-60; *id.* at 162 (Separate Statement of Board Members Brand and Cook). This does not mean U.S. person queries unrelated to national security are never fruitful or are less valuable. The FISC also noted that “unexpected connections may arise only rarely, but when they do arise, the foreign intelligence value of the information obtained could be substantial.” *Id.* at 42.



### D. Section 702 and FBI Investigations

Pursuant to the *FISA Amendments Reauthorization Act of 2017*, FISA requires that the FBI report 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 Section 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 12 provides the required statistic.

**Figure 12: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition**

Section 702 of FISA	CY2019	CY2020	CY2021
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 <i>See 50 U.S.C. § 1873(b)(2)(D).</i>	0	0	0

### 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 PCLOB issuing its *Section 702 Report*, NSA's Civil Liberties, Privacy, and Transparency Office published "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*," on April 16, 2014, (hereinafter "*NSA CLPT Report*"), in which it explained NSA's dissemination processes. *NSA CLPT 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 CLPT 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 NSA to disseminate U.S. person information if, for example, the information is necessary to understand the foreign intelligence. By policy, however, NSA generally 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 Section 3(f).

The minimization procedures 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. company," "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 ODNI (including NCTC), NSA, FBI, and CIA. The reports collectively document 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 to further illustrate NSA's dissemination practices for U.S. person information incidentally acquired from Section 702 collection in classified intelligence reports. NSA may:

- Openly name (*i.e.*, originally reveal) the U.S. person identity in the report;
- Initially mask (*i.e.*, not reveal) the U.S. person identity in the report; or
- In 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.

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 (masked or openly named).

As noted previously in the Key Terms and Concepts section 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 in Figure 13 below include identities of U.S. persons who are individuals as well as U.S. persons that are corporations or unincorporated associations.

The first row of Figure 13 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 includes 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.

The second row of Figure 13 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. Rows 2 and 3 will not total row 1 because one report may contain both masked and openly included identities.

**Figure 13: Section 702 Reports Containing USP Information Unmasked by NSA**

Section 702 Reports Containing U.S. Person Information Disseminated by NSA	CY2019	CY2020	CY2021
Total number of NSA disseminated §702 reports containing USP identities <i>regardless of whether the identity was openly included or masked</i>	4,297	3,627	<b>4,300</b>
Total number of NSA disseminated §702 reports containing USP identities <i>where the USP identity was masked</i>	3,196	2,648	<b>3,291</b>
Total number of NSA disseminated §702 reports containing USP identities <i>where the USP identity was openly included</i>	1,562	1,351	<b>1,426</b>

Figure 14 provides statistics relating to the number of U.S. person identities that were originally masked in those reports counted in Figure 13 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. § 1881a(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.”

Note that a single intelligence 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. person identities that a foreign intelligence target is seeking to victimize; each of those identities would be counted in Figure 14.

**Figure 14: Section 702 USP Identities Disseminated by NSA**

Section 702 - U.S. Person Information Unmasked by NSA	CY2019	CY2020	CY2021
Number of U.S. person identities that NSA unmasked in response to a specific request from another agency	10,012	9,354	<b>13,036</b>

# 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 § E.1 requires that each element's procedures contain certain documentation and approval requirements.

Furthermore, ICPG 107.1 § E.1.f requires additional documentation and approvals if a request is made "during a period beginning on the date of a general election for President and ending on the date on which such President is inaugurated" (*i.e.*, a presidential election period) to unmask members of the President-elect's or Vice President-elect's transition teams. The end of CY2020 and the beginning of CY2021 covered such a period and, thus, elements were required to follow these additional requirements.

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 are available for review in the IC on the Record database at intel.gov.

## 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 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 15 provides these numbers for CY2019, CY2020, and CY2021.

### 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.
- Establishes certain documentation and approval requirements for applicable unmasking 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.



**Figure 15: 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	CY2021
Total Number of <b>Requests Received</b> by all IC elements this calendar year	7,724	6,933	<b>10,744</b>
Of the requests received, the IC <b>Approved</b>	6,845	6,193	<b>9,874</b>
Of the requests received, the IC <b>Denied in Full</b>	349	279	<b>381</b>
Of the requests received, the IC processed as <b>Withdrawn in Full</b>	270	216	<b>217</b>
Of the requests received, the IC has <b>Pending Decisions</b>	260	245	<b>328</b>

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

- **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 a prior request, 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 2022 for a request that was received in December 2021, that approval was counted in the CY2021 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 the 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 2017* codified a requirement that certain statistics concerning criminal proceedings must be provided to the public pertaining to notice provided pursuant to Sections 106 and 305, including with respect to the use of Section 702-acquired information.

### 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.

**Figure 16: Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Certain FISA Information**

FISA Sections 106 and 305	CY2019	CY2020	CY2021
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 <i>See 50 U.S.C. § 1873(b)(4).</i>	7	9	5

# 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 device could be used to acquire the phone numbers, dates, and lengths of calls that were sent 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 [intel.gov’s](#) IC on the Record (for example in a [September 27, 2017](#) posting).

### 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 a 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.

## B. Statistics

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

**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 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).

Pursuant to 50 U.S.C. § 1873(d)(2)(B), the estimated number of unique identifiers used to communicate information (see row 3 in Figure 17a) 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 17a: PR/TT Orders, Targets, and Unique Identifiers Collected**

Title IV of FISA	CY2019	CY2020	CY2021
Total number of orders <i>See 50 U.S.C. §§ 1873(b)(3)</i>	22	15	<b>10</b>
Estimated number of targets of such orders <i>See 50 U.S.C. §§ 1873(b)(3)(A)</i>	21	8	<b>6</b>
Estimated number of unique identifiers used to communicate information collected pursuant to such orders <i>See 50 U.S.C. §§(b)(3)(B).</i>	96,995	53,824	<b>53,989</b>

The U.S. person status of targets is reflected in the following figure:

**Figure 17b: FISA PR/TT Targets – U.S. Persons and Non-U.S. Persons**

PR/TT Targets	CY2019	CY2020	CY2021
Estimated number of targets who are non-U.S. persons <i>See 50 U.S.C. §§1873(b)(3)(A)(i)</i>	8	5	<b>1</b>
Estimated number of targets who are U.S. persons <i>See 50 U.S.C. §§1873(b)(3)(A)(ii)</i>	13	3	<b>5</b>
Estimated percentage of targets who are U.S. persons	61.9%	37.5%	<b>83.3%</b>



# FISA Title V – Business Records

## A. Business Records FISA

Title V of FISA, commonly referred to as the “Business Records” provision, 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 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 USA PATRIOT Act version of Title V remains available. That means 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 the calendar year 2019 *Annual Statistical Transparency Report*, in August 2019, NSA suspended use of the CDR authority and deleted previously acquired call detail records. Thus, the suspension of NSA’s acquisition of CDRs in 2019 in conjunction with the expiration of the underlying authority in March 2020 result in there being no statistics to report for calendar year 2021 pertaining to CDRs.

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

**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 below constitute a good faith estimate of the number of unique identifiers acquired by the FBI under these authorities.

**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 business records 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) assuming there is no overlap among the 10 non-targeted email addresses returned by the three providers, 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

For CY2020 and CY2021, the number in row one 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.

**Figure 18: Title V Business Records Orders, Targets, and Unique Identifiers Collected**

Business Records – Section 501(b)(2)(B) and Section 502	CY2019	CY2020	CY2021
Total number of business records orders issued pursuant to applications under Section 501(b)(2)(B) or Section 502 <i>See 50 U.S.C. §§ 1873(b)(5)</i>	61	28	11
Estimated number of targets of such orders <i>See 50 U.S.C. §§ 1873(b)(5)(A)</i>	53	25	13
Estimated number of unique identifiers used to communicate information collected pursuant to such orders <i>See 50 U.S.C. §§ 1873(b)(5)(B).</i>	66,719	7,654	23,157

# National Security Letters (NSLs)

## A. National Security Letters

In addition to statistics relating to FISA authorities, the government also reports information on FBI's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs, which are administrative subpoenas, to compel the production of certain records (as specified below) only if the information being sought is relevant to a pending national security investigation. The FBI issues NSLs 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 2022 the Department of Justice released its [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 2021. 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 differ.

**NSL REQUESTS VERSUS NSL TARGETS.** The government reports the annual number of requests, rather than NSL targets, 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

### 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.

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.

**Figure 19: NSLs Issued and Requests for Information**

