THE

PRIVACY AND CIVIL LIBERTIES

OVERSIGHT BOARD

REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SEPTEMBER 28, 2023

[THIS PAGE INTENTIONALLY LEFT BLANK]

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

SEPTEMBER 28, 2023

Privacy and Civil Liberties Oversight Board

Sharon Bradford Franklin, Board Chair

Edward W. Felten, Board Member

Travis LeBlanc, Board Member

Beth A. Williams, Board Member

Richard E. DiZinno, Board Member

The Board acknowledges with gratitude the staff members who worked on this project, including Jerry Bjelopera, Pamela Brooke, Hannah Burgess, Geoff A. Cohen, Karen E. Dunkley, Jennifer Harp Fitzpatrick, Danette Fox, Danielle Kendrick, Mark M. Jaycox, Richard Morgan, Alexa Potter, Saleela Khanum Salahuddin, Lauren Sarkesian, and other current and former staff members.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

TABLE OF CONTENTS

Annexes:

EXECUTIVE SUMMARY

Part 1: Introduction to the PCLOB Report

The Privacy and Civil Liberties Oversight Board's July 2014 *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (hereinafter "2014 PCLOB Report") is a comprehensive public report that for the first time provided an unclassified description of the intricacies of this complex program. Since 2014, the Section 702 program has undergone a number of changes, including agency-imposed policy and programmatic updates, changes imposed by the Foreign Intelligence Surveillance Court (FISC), technological changes, and new statutory mandates. Given the scope of change since 2014, the Board believes an updated report will better inform public understanding of the program, particularly in the lead-up to the program's December 2023 expiration, or "sunset,"[1] before which Congress will determine whether to vote to reauthorize Section 702 without any changes, reauthorize with statutory amendment, or allow the authorization to expire.

PCLOB conducted a comprehensive study of the current Section 702 program, and this report presents PCLOB's findings in an unclassified format to the greatest extent possible, consistent with the protection of classified information and applicable law. It carries forward and updates factual and legal information from the 2014 PCLOB Report, and adds new discussions where substantial changes have been implemented, greater transparency is now possible, or new information has become available. New sets of recommendations and Board Member statements are also included. There is also a Classified Annex to this Report (Annex C) and to the Separate Statement of Board Members Beth A. Williams and Richard E. DiZinno (Annex D).

Part 2: Description and History

The Section 702 program traces its lineage to counterterrorism efforts following the attacks of September 11, 2001. Following the September 11th attacks, President George W. Bush issued a classified presidential authorization directing the National Security Agency (NSA) to collect certain foreign intelligence information by electronic surveillance in order to prevent acts of terrorism within the United States. In August 2007, Congress enacted and the President signed the Protect America Act of 2007,[2] a legislative forerunner to what is now Section 702 of the Foreign Intelligence Surveillance Act (FISA). In 2008, Congress enacted the FISA Amendments Act, which replaced the expired Protect America Act provisions with the new Section 702 of FISA.

Congress most recently voted to reauthorize Section 702 in January 2018. The reauthorization legislation made some changes to the statute, including: requiring agencies to develop and submit to the FISC specific procedures for querying U.S. person information;

[1] FISA Amendments Reauthorization Act of 2017, Pub. Law 115-118, § 201, 132 Stat. 3 (2018).

[2] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

requiring a FISC order before the Federal Bureau of Investigation (FBI) can view results of a limited category of queries of U.S. person information; and requiring FISC approval and congressional notification to conduct "abouts" collection, which NSA had voluntarily ceased (all described in more detail in this Report); as well as other changes intended to improve oversight and transparency of the program. Under the statute enacted in 2018, Section 702 is scheduled to expire on December 31, 2023, and its reauthorization process provides another opportunity for evaluation by Congress and the public of its purpose, procedures, and protections.

Section 702 statutorily authorizes the government to target non-U.S. persons, reasonably believed to be located outside the United States, in order to collect foreign intelligence information using the compelled assistance of U.S. electronic communications service providers (ECSPs).[3] The government may target only individuals who are expected to communicate, receive, or possess foreign intelligence information within given categories of intelligence previously authorized by the Attorney General and the Director of National Intelligence (DNI) and certified for collection by the FISC.

Although the government may use Section 702 only to target non-U.S. persons, communications of U.S. persons or information concerning them may be "incidentally" collected when a lawfully targeted non-U.S. person communicates with or talks about a U.S. person. Since the enactment of Section 702, the intelligence community has stated that it cannot provide metrics to identify the amount of incidentally collected U.S. person information under Section 702.

Under the statute, the Attorney General and the DNI make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted. While individual targets are not submitted to the FISC or any other judicial authority for review, Section 702 certifications must contain "targeting procedures" approved by the Attorney General that must be "reasonably designed" to ensure that any Section 702 acquisition is "limited to targeting [non-U.S.] persons reasonably believed to be located outside the United States" and to prevent the intentional acquisition of wholly domestic communications.[4] Section 702 requires that certifications also include "minimization procedures" that control the acquisition, retention, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.[5] Finally, certifications also include "querying procedures."[6] The government's annual Section 702 certification packages must be reviewed and approved by the FISC.[7] Once Section 702 acquisition has been authorized, the

[3] 50 U.S.C. § 1881a(a), (b)(3), (h)(2)(A)(vi).

[4] *Id.* § 1881a(d)(1), (h)(2)(A)(i), (h)(2)(B).

[5] *Id.* § 1881a(e)(1), (h)(2)(A)(ii), (h)(2)(B).

[6] *Id.* § 1881a(f)(1)(A).

[7] *Id.* § 1881a(d)(2), (e)(2), (j).

Attorney General and the DNI send written directives to ECSPs compelling the providers' assistance in the acquisition.[8]

There are currently three certifications under which foreign intelligence information may be obtained under Section 702. These certifications authorize the collection of foreign intelligence information about foreign governments and related entities; counterterrorism; and combatting proliferation.[9] Cybersecurity-related targets may fall under any of the three certifications.

Part 3: Operations and Oversight

Under Section 702, non-U.S. persons reasonably believed to be located outside the United States may be "targeted" through the "tasking" of "selectors." *Targets* are individuals, groups, or entities that are expected to receive, communicate, or possess foreign intelligence information within the scope of a specific Section 702 certification. *Selectors* may be communications facilities that are assessed to be used by the target, such as the target's email address or telephone number. The targeting procedures govern this acquisition process.

During calendar year 2022, approximately 246,073 non-U.S. persons located abroad were targeted under Section 702.[10] The number of Section 702 targets has nearly doubled over the last five years.

Once a selector has been approved for collection under the Section 702 targeting procedures, it is tasked (or sent to) an ECSP to begin acquisition. Collection under Section 702 includes messages that are sent or received by targets in communication with other persons.

Depending on the role and function of the provider and the type of information being acquired, the particular manner of acquisition differs. Generally, acquisition under Section 702 falls into one of several categories: upstream, telephony, and downstream. Additionally, in its April 21, 2022 Memorandum and Order, the FISC authorized NSA to use an additional "highly sensitive technique." Within each category, the details of acquisition procedures depend on differing mission requirements and the capabilities and operations of individual providers.

First, upstream collection occurs with the compelled assistance of U.S. communications providers that control, operate, or maintain the telecommunications "backbone" over which communications transit. Upstream collection occurs inside the United States and only at locations that are likely to carry traffic associated with tasked Section 702 selectors. Upstream collection is not routed to the Central Intelligence Agency (CIA), FBI, or the National Counterterrorism Center

[8] *Id.* § 1881a(i).

[9] Memorandum Opinion and Order, at 10, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) [hereinafter Apr. 21, 2022 FISC Opinion and Order].

[10] OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2022, at Figure 4 (2023) [hereinafter CY2022 ASTR].

(NCTC), and resides only in NSA systems, where it is subject to NSA's minimization procedures. Prior to 2017, upstream collection acquired not only communications to or from Section 702-tasked selectors, but also "abouts" communications (in which the tasked selector was neither the sender nor the recipient of the communication, but the selector was contained in the body of the communication). In 2017, NSA suspended the practice of "abouts" collection. In the 2018 Reauthorization Act, Congress codified that the government must first obtain approval from the FISC and inform Congress thirty days before restarting "abouts" collection.

Second, in its April 21 2022 Memorandum and Order, the FISC authorized NSA to use an additional "highly sensitive technique" pursuant to Section 702 "in a manner that is reasonably expected to result in no incidental collection of U.S. persons' communications."[11] The Board has reviewed classified information regarding this collection technique and discusses it in further detail in the Classified Annex to this report.

Third, Section 702 collection includes telephony. Selectors for telephony collection refer to unique signaling information used by network providers to identify the source or destination of a call, such as phone numbers. While implementation differs across ECSPs, for the majority of telephony collection, the ECSP identifies the calls to and from the tasked selectors and provides a copy of those communications to NSA. NSA can acquire the signaling information and content of the phone calls associated with those selectors.

Finally, Section 702 collection involves downstream collection, which was previously referred to as PRISM. To facilitate the acquisition of downstream collection, if requested by NSA, FBI may serve a 702 directive on an ECSP, for example an email provider, compelling the provider to collect and produce the communications of an identified selector—such as an email address. In such a case, the ECSP provides the government with communications using that selector until the government detasks that selector. Unlike upstream collection, which is captured as it transits the backbone, downstream collection is retrieved at the beginning or end of its journey, i.e., from a service provider. As of 2023, the vast majority of the Internet communications NSA acquired pursuant to Section 702 was obtained through downstream collection.

The government uses targeting procedures to effectuate the collection process and ensure compliance with the applicable provisions of FISA and the Constitution. While the targeting procedures are subject to judicial review by the FISC, individual targeting determinations are subject to agency compliance mechanisms and oversight review by DOJ and the Office of the Director of National Intelligence (ODNI). Only NSA and FBI are authorized to conduct acquisitions under Section 702 and, thus, are the only agencies that have targeting procedures.

[11] Off. of the Dir. of Nat'l Intel., *Release of Two FISC Decisions Authorizing Novel Intelligence Collection* (May 19, 2023), https://www.intel.gov/ic-on-the-record-database.

Other agencies nominating targets for collection under Section 702 must provide information to NSA and FBI regarding those targets.

To target under Section 702, both the nominating agency and the targeting agency must assess that all known users of the selector are non-U.S. persons reasonably believed to be located outside the United States. In addition, the targeting procedures require the analyst to reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information related to one of the certifications.

Section 702 requires that agencies adopt minimization procedures designed to reduce the privacy and civil liberties impact of the acquisition, retention, and dissemination of incidentally collected U.S. person information.[12] The minimization procedures adopted by each agency with access to unminimized Section 702 collection, both content and noncontent (including metadata), must be approved by the FISC.[13] Under Section 702, unminimized collection is the raw data received from providers that has not yet been determined to meet the standards for retention—i.e., that has not been determined to be (a) foreign intelligence information; (b) necessary to understand foreign intelligence information or to assess its importance; or (c) evidence of a crime. Four agencies

[12] 50 U.S.C. § 1801(h).

[13] *Id.* § 1805.

currently receive unminimized Section 702 collection, namely NSA, CIA, FBI, and, new since 2017, NCTC. The Section 702 minimization procedures include provisions designating when data may be retained, what data must be purged (i.e., destroyed or deleted) upon recognition, when data must be "aged off" agency systems (i.e., deleted at the end of its retention period) and what types of evaluated information may be retained indefinitely, subject to any other retention periods that may be specified by law.[14] Agency minimization procedures and practices impose additional restrictions on the use and dissemination of Section 702-acquired data and rules governing handling of attorney-client communications.

Agencies conduct queries to search through unminimized data that has already been lawfully collected and identify pertinent information. Hence, a query does not cause the government to obtain any new communications. Queries are thus similar to an Internet search, in this case searching Section 702 data repositories to identify and return records that include a match to the query terms used (e.g., an email address, phone number, name, or other terms relating to the subject of an analyst's investigation). Pursuant to the agencies' querying procedures, queries must be reasonably likely to retrieve foreign intelligence information or, in the case of FBI, may alternatively be reasonably likely to retrieve evidence of a crime. In order to satisfy this query standard, queries must:

- Be conducted for the purpose of retrieving foreign intelligence information or, in the case of FBI, alternatively evidence of a crime;
- Be reasonably tailored so that they retrieve the information sought and limit the retrieval of unnecessary or irrelevant information; and
- Be supported by a proper justification (the facts indicate that the information sought is reasonably likely to be contained in the agency's Section 702 collection).

While the government is restricted from targeting U.S. persons, agency procedures permit querying Section 702 collection using terms that identify one or more U.S. persons. The same query standard applies to both U.S. person queries and non-U.S. person queries. However, there are specific reporting and approval requirements for U.S. person queries.

This Report further describes exceptions and exemptions to the querying procedures, as well as additional information regarding the use of U.S. person queries, and each agency's implementation of the querying procedures. The report also describes FBI's use of "batch job queries," in which multiple query terms are run as part of a single query action, pursuant to the same justification. In June 2023, FBI began requiring attorney pre-query approval to conduct batch job queries of any size.

[14] *Id.* § 1801(h)(1).

In addition, Part 3 of this Report details agencies' internal compliance mechanisms as well as the Section 702 oversight conducted by various entities external to NSA, FBI, CIA, and NCTC, several of which were mandated by Congress when it first enacted Section 702 in 2008 and again when it reauthorized the program in 2018. DOJ, ODNI, and the FISC have the primary responsibility for overseeing the Intelligence Community's implementation of the program. The various agency Offices of the Inspector General, Government Accountability Office, and PCLOB have also played roles in oversight of surveillance conducted under Section 702. In addition, Congress conducts oversight of surveillance conducted under Section 702.

Finally, Part 3 of this Report outlines the various incidents of noncompliance with the rules governing Section 702 that have been identified in the course of internal agency compliance review, as well as oversight conducted by DOJ and ODNI. Those incidents of noncompliance have included individual errors, system issues, and instances where Intelligence Community personnel did not fully understand the requirements.

Part 4: Policy Analysis

The Board concludes that Section 702 remains highly valuable to protect national security, and that it creates serious privacy and civil liberties risks. To assess the overall impact of the Section 702 program, these privacy and civil liberties risks must be measured against the value that the Section 702 program provides. The Board believes that the privacy and civil liberties risks posed by Section 702 can be reduced while preserving the program's value in protecting Americans' national security.

I. Value of Section 702 Program

The Board states that the United States is safer with the Section 702 program than without it. The Board assesses that the Section 702 program has been highly valuable in protecting the United States from a wide range of foreign threats, including terrorist attacks in the United States and abroad, cyber-attacks on U.S. critical infrastructure, and both conventional and cyber threats posed by the People's Republic of China, Russia, Iran, and the Democratic People's Republic of Korea. Information collected under Section 702 informs national decision-makers; provides insight into foreign adversaries' organizational goals, strategies, and objectives; and can identify the capabilities of hostile actors.

Section 702's value is based in part on the program's unique capabilities to collect intelligence. As the Board explained in 2014, Section 702 offers certain advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In some regions of the world communications infrastructure is limited, which impairs the government's ability to collect signals intelligence under other authorities; intelligence collection regarding these regions would be greatly impaired without the

Section 702 program. Section 702 also has national security advantages over traditional FISA collection under Title I of the statute due to its agility, stemming from the lower legal standards and lack of individualized review by the FISC.

From an operational standpoint, the Section 702 program enables the U.S. government to identify individual threat actors and their networks; find elusive targets; and obtain a uniquely refined and detailed view of their individual targets. Additionally, Section 702 capabilities provide information to facilitate other intelligence collection, while protecting sensitive sources and methods. Information obtained through FISA Section 702 collection has enabled the government to discern both the large scale strategies and small scale decision-making of terrorist organizations and other foreign adversaries.

Certain selected declassified examples of the program's value are included in the Report in accordance with the categories of threats to which they relate, including counterterrorism, strategic competition with major powers, defending against cyber-attacks, and slowing proliferation of weapons and theft of advanced technologies. Additional examples and further discussion are contained in the Classified Annex to this Report.

The Board also examined the value of upstream collection, U.S. person queries, and batch queries.

Upstream collection remains valuable for several reasons, including that it offers access to targets' communications where they use non-U.S. ECSPs.

With regard to U.S. person queries, they help personnel "connect the dots"—that is, uncover plots, identify bad actors, and recognize links between foreign intelligence targets and U.S. persons. The strongest examples of the value of U.S. person queries provided to the Board involve so-called "victim queries," or what the government now refers to as "defensive queries." In particular, the government has identified instances in which U.S. person queries provided a means to investigate whether hostile cyber actors have compromised individuals' or organizations' electronic communications and to enable the agency to focus its outreach to the potential victims.

"Batch queries"—queries through which FBI personnel search Section 702 information with hundreds or thousands of query terms at once—allow analysts to process larger sets of identifiers with greater speed when the terms in the batch share a common query justification. The batch query tool also enables analysts to detect connections among the query terms.

II. Privacy and Civil Liberties Implications

The Board finds that Section 702 poses significant privacy and civil liberties risks, most notably from U.S. person queries and batch queries. Significant privacy and civil liberties risks also include the scope of permissible targeting, NSA's new approach to upstream collection, a new sensitive collection technique that presented novel and significant legal issues approved by the

FISC in 2022, how data is initially ingested into government repositories, incidental collection, and inadvertent collection.

As an initial matter, the definition of "foreign intelligence information" that may be collected under FISA is very broad, though the government has not sought to use Section 702 to collect information extending to the outer bounds of the FISA definition of foreign intelligence information. The Board agrees that the purposes authorized under the three Section 702 certifications fit within the twelve legitimate objectives outlined in Executive Order 14086 (E.O. 14086) on Enhancing Safeguards for United States Signals Intelligence Activities, issued in October 2022, and these limitations should help ensure that the government will not conduct surveillance to the full scope of the FISA definition of foreign intelligence information.

The Board finds that the risk of overbroad government collection of communications under Section 702 and subsequent government use of that information is very real and can cause harm, at varying degrees. Section 702's targeting presents a number of privacy risks and harms by authorizing surveillance of a large number of targets, providing only programmatic review of a surveillance program, allowing extensive incidental collection, and causing inadvertent collection. The FISC reviews and approves targeting procedures to minimize the risks of improper surveillance, but there is no individualized judicial review of targeting decisions.

Surveillance of individuals in any form invariably risks intruding on privacy and civil liberties. In CY2022, the Section 702 program targeted approximately 246,073 non-U.S. persons located abroad,[15] which represents a 276 percent increase since CY2013. The surge in Section 702 targeting in recent years increases the privacy and civil liberties risks, both for actual targets and for those whose information has been incidentally or inadvertently collected.

Though the Board recognizes that Section 702 is not "bulk" collection, the program lacks individualized and particularized judicial review of targeting decisions, because only persons who lack recognized Fourth Amendment rights may be targeted under Section 702. This poses risks that targeting can be overbroad or unjustified. These risks are increasing as the target numbers and their associated selectors continue to grow. It is worth noting, however, that Section 702 limits targeting based on a number of factors to minimize the risks of improper surveillance and to ensure that intrusions upon privacy and civil liberties are taken into account.

The Board discusses that, in 2017, NSA suspended upstream "abouts" collection, which involved the collection of communications that were neither to nor from a selector, but instead contained the selector. Since then, NSA has changed its approach to upstream in an effort to ensure that only communications that are actually to or from a target are collected. These changes have substantially reduced the privacy risks stemming from upstream collection under Section 702. Nonetheless, the privacy risks from incidental and inadvertent collection remain, and upstream

[15] CY2022 ASTR, *supra*, at 18.

collection requires a more intrusive process than downstream collection to determine whether communications to be collected are those of a target. The process for identifying the communications to be collected in upstream involves screening a broader set of traffic transiting the internet backbone, which necessarily includes communications that are not to or from targets, and which will not be ingested into government databases.

While the Board is unaware of any government interest in, or plans to, restart "abouts" collection, the Board further discusses that "abouts" collection is a practice that raised significant privacy and civil liberties concerns. If NSA were to resume "abouts" collection, the unique privacy risks stemming from such collection could reappear.

The Board also notes that although the privacy risks in upstream have been substantially reduced following the suspension of "abouts" collection, the new approach to identifying communications to be acquired in upstream continues to raise privacy risks, which are further discussed in Annex C of this Report.

Additionally, Annex C of this Report includes analysis of the new highly sensitive collection technique which was discussed and approved by the FISC in its April 2022 certification decision. As discussed in the annex, this new collection method involves new privacy risks, although the government has taken steps to mitigate those risks.

The Board explains that although Section 702 targets can only be non-U.S. persons, through incidental collection the government acquires a substantial amount of U.S. persons' communications as well. While the term may make this collection sound insignificant, and we do not yet know the scope of incidental collection, it should not be understood as occurring infrequently or as an inconsequential part of the Section 702 program. Further, the scope of Section 702 collection as a whole is extensive. The Board adds that since there is currently no data or transparency identifying the magnitude of incidental collection of U.S. person information, rigorous and reproducible best estimates or even approximate figures would provide critical transparency in this space.

The Board points out that once collected, subject to certain restrictions, U.S. person information may be queried, analyzed, disseminated in intelligence reports, retained, and used as evidence against the U.S. person in criminal proceedings. Such collection can also be used to initiate targeted surveillance of the individual under alternate legal authorities, or it may be shared with domestic and foreign law enforcement and intelligence partners.

The Board assesses that U.S. person queries present some of the most serious privacy and civil liberties harms. Except in the very limited circumstances covered by Section 702(f)(2) for certain FBI queries, government personnel are not required by Section 702 to make any showing of suspicion that the U.S. person is engaged in any form of wrongdoing prior to using a query term associated with that specific U.S. person. Nor does Section 702 require analysts or agents to seek approval from any judicial authority or other independent entity outside their agency. Americans'

communications captured through surveillance can include discussions of political and religious views, personal financial information, mental and physical health information, and other sensitive data. Moreover, ordinary Americans may be in contact with Section 702 targets for business or personal reasons even if the Americans have no connection to, or reason to suspect, any wrongdoing by their foreign contacts and even when the government has no reason to believe the target has violated any U.S. law or engaged in any wrongdoing.

Although all U.S. person queries by the Intelligence Community present privacy and civil liberties risks, FBI's querying procedures and practices pose the most significant threats to Americans' privacy. The Board recognizes and welcomes the fact that FBI has recently implemented several reforms designed to improve compliance, but these changes have not been sufficient to protect privacy and civil liberties. FBI's querying practices pose greater threats to privacy because FBI, as the United States' domestic law enforcement agency, has the ability and the mission to investigate and prosecute Americans for crimes. Further, FBI routinely searches Section 702 data at the pre-assessment and assessment stages of FBI investigations. Although Section 702 queries must still meet the query standard, the low thresholds applicable at the pre-assessment stage increase the risk that an individual's private communications will be compiled despite the lack of any basis to suspect the individual of wrongdoing. In addition, searches conducted by FBI analysts related to social advocacy and non-violent civil protests also pose significant threats to civil liberties.

Batch queries present yet another privacy and civil liberties harm in the context of the Section 702 program. The rules allowing a single broad justification for hundreds or thousands of query terms can cause serious privacy harms. Without a specific and individualized assessment for each discriminant it is not possible to ensure that the query standard is actually being met and only searches reasonably believed to return evidence of a crime or foreign intelligence are performed.

The Board's policy analysis further analyzes privacy and civil liberties implications from: exceptions and exemptions to querying procedures; use, retention and dissemination practices; and training and auditing regimes. Finally, the Board discusses considerations regarding transparency and operations of the FISC, and particularly the role of FISC amici.

The Board concludes that although the Section 702 program presents serious risks to, and actual intrusions upon, the privacy and civil liberties of both Americans and non-Americans, the United States is safer with the Section 702 program than without it. The Board further finds that the most serious privacy and civil liberties risks result from U.S. person queries and batch queries, and the government has not demonstrated that such queries have nearly as significant value as the Section 702 program overall.

Ultimately, the Board believes that these privacy and civil liberties risks can be reduced while preserving the program's value in protecting Americans' security. The Board presents a series of recommendations outlining how Congress and the government can reduce these risks.

Part 5: Recommendations

- **Recommendation 1: Congress should codify the twelve legitimate objectives for signals intelligence collection under Executive Order 14086.**

  These provide important privacy and civil liberties protections for signals intelligence collection, including the Section 702 program, and intentionally narrow the grounds upon which the government can otherwise collect under Section 702. Such codification would provide the necessary clarity in conferring explicit jurisdiction to the FISC to ensure that E.O. 14086 is properly enforced across the judicial branch.

- **Recommendation 2: Congress should codify the prohibition against "abouts" collection by removing NSA's ability to restart it without congressional approval other than in certain exigent circumstances. Any restart of "abouts" collection should apply to only those particular forms of traffic related to the exigency.**

  The current statute allows the government to restart "abouts" collection following approval by the FISC and after providing thirty days' notice to Congress. Due to the significant risks to privacy and civil liberties generated by "abouts" collection, and because there is currently no identified mission need for such collection, the Board recommends that Congress amend the statute to remove the government's ability to restart "abouts" collection, except in certain exigent circumstances.

- **Recommendation 3: Congress should require FISC authorization of U.S. person query terms.**

  The most critical safeguard for Americans' privacy rights is to require individualized and particularized judicial review for all U.S. person query terms. Specifically, the Board recommends that Congress require FISC review and approval under the current standards of "reasonably likely to retrieve" foreign intelligence or "reasonably likely to retrieve" evidence of a crime, in order for the government to access the results of any query using U.S. person query terms.

  The Board recommends that Congress include two specific exceptions to the requirement for FISC approval of U.S. person query terms. First, the government has indicated that a substantial portion of its U.S. person queries, at least within FBI, have been related to identifying victims. Congress should provide a consent exception in which the government can access Section 702 communications associated with a U.S. person query with the actual consent of the U.S. person without having to obtain FISC approval. Second, Congress

should include a provision that makes an exception for exigent circumstances, modeled upon other exigent circumstances provisions in FISA.

- **Recommendation 4: Congress should codify any exemptions from and exceptions to the Section 702 querying procedures in order for such exemptions and exceptions to be implemented.**

- **Recommendation 5: Congress should require that NSA perform and publish an assessment of the feasibility and value of proposed methodologies for estimating the scope of incidental collection of U.S. person information, including the use of statistical and cryptographic techniques. Congress should establish lawful processes for private providers to assist the assessment as necessary.**

  The Board recommends that Congress require a pilot project at NSA to assess the viability of one or more of the available proposals and others that may be developed, and provide the necessary legal authorities to permit service providers to assist as needed.

- **Recommendation 6: Congress should codify a requirement that the government submit to the FISC a random sample of targeting decisions and supporting written justifications from NSA, FBI, and CIA for *post hoc* judicial review as part of the annual Section 702 recertification process. The sample size and methodology should be approved by the FISC.**

- **Recommendation 7: Congress should strengthen the role of the FISC amicus and improve transparency for FISC opinions.**

  First, the Board urges that Congress expand the types of matters in which the FISC and Foreign Intelligence Surveillance Court of Review (FISC-R) shall appoint amici to participate beyond those involving "novel and significant" issues to explicitly include the annual Section 702 certification process. Second, the Board recommends that Congress amend the FISA amicus provision to direct that amici should have full access to all the information related to matters in which they participate, providing them with the same information that is available to the government in these matters. In addition, the Board recommends that Congress amend the amicus provision to provide that whenever the FISC or FISC-R appoints an amicus curiae in a matter, that individual may consult with other amici designated on the FISC's approved list regarding any information relevant to the proceeding. Third, Congress should authorize amici to seek appellate review and petition for appeal of decisions by both the FISC and the FISC-R.

  With regard to the declassification reviews of FISC decisions, orders, or opinions involving a significant construction or interpretation of law, the Board recommends that Congress set a time limit for such reviews so that the declassification review and public release of each

such decision, order, or opinion must be completed no later than 180 days after the date on which the decision, order, or opinion was issued.

- **Recommendation 8: NSA should conduct annual evaluations to ensure continual improvements and modern capabilities are applied to limit the amount of backbone traffic screened and acquired during upstream collection and to document those efforts as part of the annual certification process.**

- **Recommendation 9: FBI and CIA should strengthen their post-targeting review requirements for foreign intelligence targets and improve their systems to ensure that collection from targets remains appropriate and continues to generate valuable foreign intelligence.**

- **Recommendation 10: The Intelligence Community should establish protocols and update systems to accommodate and require tagging Section 702-acquired information that analysts determine contain U.S. person communicants.**

  The Board is not recommending that the Intelligence Community agencies conduct any extra investigation in order to apply this tag; rather the Board recommends that if they otherwise determine an individual is a U.S. person in the course of their regular duties, they apply this tag to avoid further duplication of effort.

- **Recommendation 11: The Intelligence Community should increase clarity and, where possible, parity regarding agencies' required treatment of Section 702-acquired attorney-client communications. In addition, FBI specifically should centralize tracking of criminal indictments and taint review teams to limit the number of attorney-client communication compliance incidents.**

- **Recommendation 12: FBI, in batch queries, should ensure that each query term that relates to a specific person may be used only if it individually meets the applicable query standard and approval process. Validating each U.S. person query term through implementation of Recommendation 3 would address the privacy risks to U.S. persons. In the case of query terms associated with non-U.S. persons, each term should meet standards developed following an assessment in accordance with E.O. 14086's requirement that signals intelligence activities be conducted only as is necessary and proportionate to a valid intelligence priority**.

- **Recommendation 13: The NSA, FBI, CIA, and NCTC querying procedures should be updated to require that personnel, prior to conducting a query in raw Section 702 information, perform due diligence to assess the U.S. person status of the query subject by searching in minimized FISA and non-FISA datasets**.

- **<u>Recommendation 14</u>: The Intelligence Community should improve its recordkeeping of certain types of queries of raw Section 702-acquired information, including sensitive queries of raw Section 702-acquired information and, in the case of FBI, evidence of a crime only queries. The number of these queries, along with the number of U.S. person queries, should be published annually in the Annual Statistical Transparency Report.**

- **<u>Recommendation 15</u>: FBI should strengthen its internal Section 702 compliance processes and supplement its internal auditing**.

  FBI would benefit from a well-staffed office at FBI Headquarters with specially trained individuals who can easily be contacted regarding Section 702 compliance-related questions, as well as at least one specially trained employee at every FBI field office.

- **<u>Recommendation 16</u>: DOJ should annually review each FBI field office's compliance with the Section 702 procedures**.

  The Board finds that additional DOJ reviews of FBI field offices, as well as at embassies, would help mitigate many of the current FBI compliance issues.

- **<u>Recommendation 17</u>: FBI should explore methods for the use of secure automated review and machine learning to supplement its manual internal auditing of Section 702 compliance.**

  The Board recommends that FBI better leverage its technological resources—including secure IT automation and machine learning—to more quickly and precisely identify, audit, and address Section 702 compliance issues. FBI should develop the capability quickly to understand trends and patterns in system usage. The Board assesses that there are opportunities for FBI to supplement its administrative safeguards with stronger technical safeguards.

- **<u>Recommendation 18</u>: NSA, FBI, CIA, and NCTC should submit to ODNI for annual review all internal and external training provided to personnel regarding the targeting, minimization, and querying procedures. DOJ should also make available securely online all external Section 702 training so that agency personnel can access this material on an as-needed basis. Additionally, Intelligence Community agencies should require supplemental retraining for personnel who have not accessed unminimized Section 702 data in the previous ninety days.**

- **<u>Recommendation 19</u>: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.**

The Board recommends that the government continue and build upon efforts taken in response to Recommendation 10 from the 2014 PCLOB Report, and develop and implement specific, replicable, and routine assessment methodologies that sufficiently capture and clearly articulate the value and efficacy of the Section 702 program. To the extent possible, the results of these assessments should be published to facilitate transparency and civil society discussions in this space.

Annex A: Separate Statement of Chair Sharon Bradford Franklin

Chair Sharon Bradford Franklin's separate statement explains that while she joins the Board's report in full, in her view, Recommendation 3 should be further strengthened. She recommends that Congress should require that before FBI may access the results of a U.S. person query conducted at least in part to seek evidence of a crime, the government must obtain approval by the FISC under a probable cause standard. She writes that this would ensure that such queries fully comply with the Fourth Amendment, and would be consistent with criminal law in other contexts. Specifically, she explains that a search through Section 702 communications data seeking information about a particular American constitutes a search under the Fourth Amendment, and current query standards are insufficient to meet constitutional requirements.

Chair Franklin also states that she agrees with the aspects of Recommendation 3 that are designed to reduce the burden on the government and the FISC, including limiting the requirement for FISC review to instances in which the U.S. person query has resulted in a hit in 702 data and government personnel want to access the results of the query. Further, she agrees with the exceptions for exigent circumstances and for searches conducted with actual consent. Congress could require a probable cause standard for FBI queries and still retain these aspects of Recommendation 3.

Chair Franklin further explains that providing individualized judicial review for U.S. person queries is critically important to ensure that this aspect of the Section 702 program is on a sound constitutional footing and protects Americans' right to privacy in their communications. She concludes that this reform should be an essential component of reauthorization of the program.

Annex B: Separate Statement of Board Members Beth A. Williams and Richard E. DiZinno

Board Members Beth A. Williams and Richard E. DiZinno wrote separately to state that they voted against this Report, and this Report therefore should not be attributed to them. The Board's voice in the ongoing policy discussions is significantly muted by the Majority's decision to produce and issue this Report, with its deeply flawed policy analysis and recommendations.

Members Williams and DiZinno emphasize two key points, about which there is no serious disagreement across the full Board: (1) the Section 702 program is both legal, and incredibly

valuable to the safety and security of the American people;[16] and (2) significant reforms are needed and should be welcomed. They underscore that the Section 702 program is so valuable that not one Member of this Board believes that Congress should allow it to lapse. And they reiterate that failure to reauthorize the program would cause grave damage to the security of our country, and quite likely, lead to the loss of American lives.

They explain how much of the Majority's analysis and many of its recommendations miss the mark, in ways both large and small. Specifically, they explain how the Report fails to differentiate in any meaningful way between areas where the government is largely succeeding in its efforts to protect privacy and civil liberties and areas where it is not. For example, with regard to targeting, the evidence clearly shows that what has most worried Americans for decades about government surveillance programs—the improper collection of U.S. person data—is ***not*** occurring under the Section 702 program.[17] But the Report nevertheless dwells on speculative "harms," untethered to operational realities or available evidence, and in some cases contrary to such evidence. The Report offers recommendations, some of which would do more to violate rather than protect the privacy of individuals.

They further explain that the Report undervalues key aspects of the program, especially U.S. person queries. They describe this value both in their unclassified Separate Statement and in the Classified Annex to their Statement (Annex D of this Report). They discuss how the Majority ignores substantial evidence of the value of these queries across the Intelligence Community, wrongly suggesting that only queries that lead to criminal prosecutions have value, and dismissing the significant foreign intelligence and defensive function of queries. Most significantly, Members Williams and DiZinno describe how the Report's Recommendation 3—unmoored from any legal justification—elevates form over function by placing heavy bureaucratic burdens on agency personnel and the FISC without evidence there would be much, if any, privacy and civil liberties improvement. Indeed, this recommendation would force additional, potentially invasive and unnecessary investigation of U.S. persons, and will make it substantially more difficult to detect and thwart hostile foreign action, including acts of terror, against the United States.

Members Williams and DiZinno provide their own analysis of the Section 702 program and offer a path forward, with stronger recommendations to address privacy and civil liberties concerns meaningfully, and in a manner that meets the Board's mission to balance privacy and civil liberties with the need to protect our national security.[18]

[16] Every court to have reached a decision on the program has found it to be constitutional and reasonable under the Fourth Amendment.

[17] The Board recognizes and reaffirms its 2014 conclusion that the Section 702 program is not bulk collection.

[18] *See* 42 U.S.C. § 2000(ee) ("The Board shall (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and

Their first set of recommendations focuses specifically on FBI, where the most widespread compliance violations have been reported over the last several years—particularly with regard to querying Section 702 information that has already been lawfully collected. They recommend cultural, structural, and procedural reform aimed at re-establishing public trust in FBI. They further describe additional, substantial reforms that they urge both Congress and FBI to implement. These include codifying and expanding protections to ensure that all U.S. person queries are limited and appropriate.

- **Recommendation 1: Reform the Structure and Culture of FBI.**

  FBI should reform its structure to better incorporate privacy and civil liberties into the fabric of its operations.

- **Recommendation 2: Codify Privacy and Civil Liberties Protections for Querying.**

  Congress should codify and expand protections to ensure that all queries of Section 702 information are limited and appropriate.

- **Recommendation 3: Improve FBI Compliance and Auditing.**

  FBI should improve its Section 702 compliance processes and auditing; DOJ should annually review FBI field offices.

Their second set of recommendations would guard against the potential weaponization and misuse of the program for political or other improper purpose. While many of the most egregious recent violations concerning the 2016 presidential transition did not involve Section 702, Members Williams and DiZinno recommend that additional safeguards be enacted to ensure appropriate oversight over the program. Specifically, Congress should have the opportunity to review sensitive queries, including those involving public officials, political candidates, members of the news media, and others involved in protected First Amendment activities, on a regular basis—not only when those queries are reported as compliance incidents. They explain that the best branch to safeguard against political misuse is a political branch accountable to the people—not a court with limited resources, appropriately focused only on legal issues, and operating largely out of the public eye. They recommend that more stringent policies should be adopted for requests to "unmask" U.S. persons. And Congress should enact a new criminal statute with significant penalties for those who leak protected Section 702 information concerning U.S. persons.

civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.").

- **Recommendation 4: Congressional Oversight of Sensitive Queries**.

  Congress should require that the Intelligence Community develop, or further refine, policies regarding sensitive queries in coordination with DOJ and ODNI. These policies should be submitted to the FISC for review and approval as part of the annual certification process, and included in the agency querying procedures. Congress should require that each agency report to Congress, at least once every six months, each of the sensitive query terms used during the previous six-month period.

- **Recommendation 5: Strengthen Procedures Concerning Unmasking.**

  The Intelligence Community should adopt new rules to protect against the unmasking of U.S. Persons for political purposes.

- **Recommendation 6: Enact Specific Penalties for Leakers of Section 702 Information.**

  Congress should enact a new criminal statute with significant penalties for those who leak protected Section 702 information concerning U.S. Persons.

Finally, they express concern that under the current statutory framework of Section 702, the government may already have in its possession—but be legally unable to access—information that foreigners entering the United States, or persons applying for U.S. government security clearances, present threats to national security. In their view, it is unacceptable that such information is lawfully collected, but rendered essentially unusable or severely limited. Vetting is a crucial national security function, and Congress should make clear that Section 702 may be utilized to support it.

- **Recommendation 7: Amend Section 702 to Permit the Government to Query Its Holdings for Limited Vetting Purposes.**

  Congress should amend Section 702 to permit vetting, in limited circumstances, to be an exception to the querying standard, with applicant consent.

Members Williams and DiZinno thus recommend stronger changes more focused on the concerns at hand. They note that every court to have reached a decision on the program has found it to be legal. And every Member of this Board has concluded the program is valuable. They offer their analysis and recommendations to help ensure that the program accords with the high standards for privacy and civil liberties protection consistent with the nation's values.

PART 1: INTRODUCTION TO THE PCLOB REPORT

I. Background

In 2008, Congress enacted the FISA Amendments Act (FAA), which, among other things, provided a statutory basis to continue aspects of the "President's Surveillance Program," also known under the code name STELLARWIND, a top secret authorization issued by President George W. Bush in the aftermath of the September 11, 2001 attacks.[1] The FAA also added Section 702 to the Foreign Intelligence Surveillance Act (FISA). Section 702 permits the Attorney General and the Director of National Intelligence (DNI) to jointly authorize surveillance conducted using the compelled assistance of U.S. electronic communications service providers (ECSPs) to target non-U.S. persons, reasonably believed to be located outside the United States, for the purpose of collecting foreign intelligence information.

In June 2013, press reporting discussed two classified National Security Agency (NSA) collection programs following the unauthorized disclosures of classified documents by Edward Snowden, a former contractor for NSA.[2] Under one such program, implemented under Section 702 of FISA, the government collects the contents of and metadata associated with electronic communications, such as email and telephone calls, of non-U.S. persons, reasonably believed to be located outside the United States, if such persons are expected to possess, receive, or communicate certain types of foreign intelligence information.

The next month, a bipartisan group of U.S. senators asked the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") to investigate the program and provide an unclassified report exploring, among other topics, the operations of the Foreign Intelligence Surveillance Court ("FISC" or "Court"), and President Obama asked the Board to "review where our counterterrorism efforts and our values come into tension."[3] In response to these requests, the Board launched a comprehensive study of the program, which included public hearings, as well as meetings with the Intelligence Community, Department of Justice (DOJ), White House, congressional committee

[1] U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, at 259-67 (2009), https://oig.justice.gov/reports/2016/PSP-01-08-16-vol-1.pdf.

[2] *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[3] Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference; Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), http://www.pclob.gov/SiteAssets/newsroom/Pelosi%20Letter%20to%20PCLOB.pdf; Letter from Senator Tom Udall et al. to the Priv. and C.L. Oversight Bd. (June 12, 2013), http://www.pclob.gov/SiteAssets/newsroom/6.12.13%20Senate%20letter%20to%20PCLOB.pdf.

staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

The Board's resulting July 2014 *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (hereinafter "2014 PCLOB Report") is a comprehensive public report that for the first time provided an unclassified description of the intricacies of this complex program.[4] In the Board's words, the report "examine[d] the collection of electronic communications under Section 702 and provide[d] analysis and recommendations regarding the program's implementation."[5]

PCLOB's 2015, 2016, and 2022 Recommendations Assessment Reports provided updates on the status of the Board's recommendations in the 2014 PCLOB Report on FISA Section 702, as well as other PCLOB Reports. As discussed in PCLOB's 2022 Recommendations Assessment Report, all ten of the recommendations included in the 2014 PCLOB Report were either implemented, implemented in part, or were being implemented by the Administration.[6]

Since 2014, the Section 702 program has undergone a number of changes, including agency-imposed policy and programmatic updates, FISC-imposed changes, technological changes, and new statutory mandates. Given the scope of change since 2014, the Board believes an updated report will better inform public understanding of the program, particularly in the lead-up to the program's December 2023 expiration, or "sunset,"[7] before which Congress will determine whether to vote to reauthorize Section 702 without any changes, reauthorize with statutory amendment, or allow the authorization to expire.

PCLOB conducted a comprehensive study of the current Section 702 program, and this report presents PCLOB's findings in an unclassified format to the greatest extent possible, consistent with the protection of classified information and applicable law. It carries forward and updates factual and legal information from the 2014 PCLOB Report, and adds new discussions where substantial changes have been implemented, greater transparency is now possible, or new information has become available. New sets of recommendations and member statements are also included.

With this updated review, the Board concludes that Section 702 remains highly valuable to protect national security, and also that it creates serious privacy and civil liberties risks. Section 702 is valuable in supporting U.S. government efforts to counter foreign threats from actors outside the United States, such as terrorism, weapons proliferation, and cyber threats. At the same

[4] PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) [hereinafter 2014 PCLOB Report].

[5] *Id.* at 2.

[6] PRIV. AND C.L. OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT, at 2-3 (2022).

[7] FISA Amendments Reauthorization Act of 2017, Pub. Law 115-118, § 201, 132 Stat. 3 (2018).

time, the risk of overbroad government collection of communications under Section 702 and subsequent government use of that information is very real and can cause harm, at varying degrees. The most serious privacy and civil liberties risks result from current practices for U.S. person queries and batch queries, and these threats are most urgent for the government to address. Ultimately, the Board believes that the privacy and civil liberties risks presented by the Section 702 program can be reduced while preserving the program's value in protecting Americans' security, and the Board provides a series of recommendations to achieve this goal.

II. Investigative Methodology

In order to gain a meaningful understanding of the Section 702 program[8] as it stands at present and assess the evolution of changes since 2014, the Board received multiple briefings from the agencies involved in implementing the program, including technical, policy, and procedural updates. The Board appreciates the time and resources devoted to this engagement, which has thoroughly enhanced the Board's understanding of the program and allowed for full consideration of the practical implications of the Board's recommendations.

The Board has also engaged with Congress and the White House, and has held a public forum and requested public comment to gain a thorough understanding of the various equities and positions held by the public and civil society.

The Board has reviewed a number of classified and unclassified reports and FISC opinions documenting programmatic and compliance challenges, new operational and reporting mandates, and discussions of novel or significant interpretations of the law. In preparation for the release of this report, and in order to enhance public understanding and inform the public and congressional debate, the Board has worked with the Intelligence Community to seek maximum appropriate declassification of information contained in this report. The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process.

III. Report Organization

Following this introduction, Part 2 contains a factual narrative that explains the development of the Section 702 program, a discussion of what Section 702 encompasses and how it is unique from other FISA authorities, the statutory structure of Section 702 including updates since 2014, and significant FISC opinions that have shaped programmatic operations. Part 3 contains details on the Section 702 acquisition process, the procedures governing the Section 702 program, and internal and external oversight mechanisms used to ensure compliance with the various procedures, FISC opinions, and statutory mandates. Part 4 examines the policy implications of the program, including an assessment of the value of the Section 702 program.

[8] The Board also incorporated its Oversight Project concerning FBI Section 702 Queries into this report.

Part 5 outlines and explains the Board's recommendations for reforms to Section 702. Individual member statements are included in annexes. The Board also has developed a Classified Annex (Annex C), which includes further details on a number of topics outlined in the unclassified report.

PART 2: DESCRIPTION AND HISTORY

I. Genesis of the Section 702 Program

The Section 702 program traces its lineage to counterterrorism efforts following the attacks of September 11, 2001. On that day, 19 terrorists hijacked four aircraft and crashed three of them into the Twin Towers of the World Trade Center in New York City and the Pentagon outside Washington, D.C. The fourth plane crashed into a field in Shanksville, Pennsylvania, after passengers fought with the terrorists for control of the cockpit. The World Trade Center towers subsequently collapsed. Later investigation found that U.S. authorities knew that two of the terrorists had entered the United States.[9] However, concerns about the permissibility of sharing information between intelligence personnel and law enforcement agents hampered the search for these terrorists in the weeks before the attacks.[10]

Killed in the September 11th attacks were all the passengers on the four aircraft, thousands of civilians in the Twin Towers and surrounding area, hundreds of emergency responders attempting to rescue them, and dozens of military personnel and others in the Pentagon. As the 9/11 Commission stated, "On September 11, the nation suffered the largest loss of life—2,973—on its soil as a result of hostile attack in its history."[11] The federal government quickly began to develop a plan for the "elimination of terrorism as a threat to our way of life" that would "integrate diplomacy, financial measures, intelligence, and military actions into an overarching strategy."[12]

In October 2001, based upon a finding that an extraordinary emergency existed because of the September 11th attacks, President George W. Bush issued a classified presidential authorization directing NSA to collect certain foreign intelligence information by electronic surveillance in order to prevent acts of terrorism within the United States. Among other activities, President Bush authorized NSA to collect the contents of certain international communications, a program that was later referred to as the Terrorist Surveillance Program (TSP). Under this authorization,

[9] *See* THOMAS H. KEAN & HAMILTON H. LEE, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS ON THE UNITED STATES, at 266-77 (2004) [hereinafter 9/11 Commission Report]; U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS, at 223-362 (2004) [hereinafter DOJ OIG Report on 9-11].

[10] Originally intended only to apply to sharing of information between FBI agents involved in intelligence gathering and federal prosecutors, the restrictions on information sharing—a combination of internal DOJ policies, decisions by the Foreign Intelligence Surveillance Court, self-imposed limits by the National Security Agency, and over-cautiousness by analysts and agents—ended up creating what was colloquially referred to as "the wall" between intelligence investigations and criminal investigations. *See* 9/11 Commission Report, *supra*, at 78; DOJ OIG Report on 9-11, *supra*, at 21.

[11] 9/11 Commission Report, *supra*, at 311.

[12] *Id.* at 331.

electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.[13]

President Bush renewed the authorization for NSA's activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist, justifying such ongoing surveillance without judicial oversight. Key members of Congress and the presiding judge of the FISC were briefed on the existence of the program. According to a 2009 report by the inspectors general of DOJ and several defense and intelligence agencies, over time, "the program became less a temporary response to the September 11th terrorist attacks and more a permanent surveillance tool."[14]

In December 2005, the *New York Times* published articles revealing the TSP, i.e., the portion of the President's Surveillance Program that involved intercepting the contents of international communications.[15] In response to these revelations, President Bush confirmed the existence of the TSP,[16] and DOJ issued a "white paper" outlining the legal argument that the President could authorize these interceptions without obtaining a warrant or court order.[17] Notwithstanding this legal argument, the government decided to seek authorization under FISA to conduct the content collection that had been occurring under the TSP.[18] In January 2007, the FISC issued an order authorizing the government to conduct certain electronic surveillance of telephone and Internet communications carried over listed communication facilities where, among other things, the *government* made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States.[19]

---

[13] *See* Off. of the Dir. of Nat'l Intel., *DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001*, IC ON THE RECORD (Dec. 21, 2013), http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the [hereinafter Dec. 21 DNI Announcement].

[14] *See* U.S. DEP'T OF DEF., OFF. OF THE INSPECTOR GEN., ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, at 31 (2009), https://irp.fas.org/eprint/psp.pdf.

[15] DOJ OIG Report on 9-11, *supra*.

[16] *See, e.g.*, President's Radio Address (Dec. 17, 2005), http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html.

[17] Letter from Att'y Gen. Gonzalez to the S. Majority Leader, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006).

[18] *See* Dec. 21 DNI Announcement, *supra*.

[19] Declassified Certification of Attorney General Michael B. Mukasey, at 37, *In re National Security Agency Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008) [hereinafter 2008 Mukasey Decl.].

The FISC's order, referred to as the "Foreign Telephone and Email Order," in effect replaced the President's authorization of the TSP, and the President made no further reauthorizations of the TSP.[20] When the government sought to renew the January 2007 Foreign Telephone and Email Order, however, a different judge on the FISC approved the program, but on a different legal theory that required changes in the collection program.[21] Specifically, in May 2007, the FISC approved a modified version of the Foreign Telephone and Email Order in which the *court*, as opposed to the *government*, made probable cause determinations regarding the particular foreign telephone numbers and email addresses that were to be used to conduct surveillance under this program.[22] Although the modified Foreign Telephone and Email Order permitted the government to add newly discovered telephone numbers and email addresses without an individual court order in advance,[23] the government assessed that the restriction of the order, particularly after the May 2007 modifications, was creating an "intelligence gap."[24]

Separate from, but contemporaneous with, the Foreign Telephone and Email Orders, a second collection effort was being undertaken. Specifically, the government used Titles I and III of the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located abroad who were suspected of engaging in terrorism and who used U.S.-based ECSPs. The government stated that it and the FISC expended "considerable resources" to obtain court orders based upon a probable cause showing that these overseas individuals met the legal standard for electronic surveillance under FISA,[25] i.e., that the targets were international terrorist groups and that they used the specific communications facilities (such as email addresses) regarding which the government was seeking to conduct electronic surveillance.[26] The persons targeted by these efforts were located outside the United States, and the communications being sought were frequently with others who were also located outside the United States.[27] Drafting applications that demonstrated satisfaction of

[20] *Id.*

[21] *Id.* at 38 n.20.

[22] *Id.* at 38.

[23] *Id.*

[24] *See* S. Rep. No. 110-209, at 5 (2007) (stating that "the DNI informed Congress that the decision . . . had led to degraded capabilities"); Eric Lichtblau et al., *Reported Drop in Surveillance Spurred a Law*, N.Y. TIMES (Aug. 11, 2007) (reporting on Administration interactions with Congress that led to the enactment of the Protect America Act, including reported existence of an "intelligence gap").

[25] *The Need to Bring the Foreign Intelligence Surveillance Act into the Modern Era: Hearing Before the S. Select Comm. on Intel.*, 110th Cong. 6-7 (2007) (statement of Kenneth L. Wainstein, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just.) [hereinafter May 2007 Wainstein Statement].

[26] 50 U.S.C. § 1805(a)(2).

[27] May 2007 Wainstein Statement, *supra*, at 7.

this probable cause standard, the government asserted, slowed, and in some cases prevented, the acquisition of foreign intelligence information.[28]

In light of the perceived growing inefficiencies of obtaining FISC approval to target persons located outside the United States, in the spring of 2007 the government proposed a modification to FISA.[29] Reports by the DNI to Congress that implementation of the FISC's May 2007 modification to the Foreign Telephone and Email Order had resulted in "degraded" acquisition of communications, combined with reports of a "heightened terrorist threat environment," accelerated Congress's consideration of these proposals.[30] In August 2007, Congress enacted and the President signed the Protect America Act of 2007,[31] a legislative forerunner to what is now Section 702 of FISA. The Protect America Act was a temporary measure that was set to expire 180 days after its enactment.[32]

The government transitioned the collection of communications that had been occurring under the Foreign Telephone and Email Orders (previously the TSP) and some portion of the collection targeting persons located outside the United States that had been occurring under individual FISA orders to directives issued under the Protect America Act.[33] The Protect America Act expired in February 2008,[34] but existing Protect America Act certifications and directives remained in effect until they expired.[35]

Shortly after passage of the Protect America Act, efforts began to replace it with a permanent statute. Federal officials testified numerous times before various congressional committees in support of modernizing and streamlining FISA. In testimony before the Senate Judiciary Committee, the Assistant Attorney General for National Security stated: "Prior to the passage of the Protect America Act of 2007 (PAA) in August, the difficulties we faced with FISA's outdated provisions—i.e., the extension of FISA's requirements to surveillance targeting foreign intelligence targets overseas—substantially impeded the Intelligence Community's ability to

[28] *See, e.g., id.*

[29] *See* S. Rep. No. 110-209, at 2, 5 (2007) (noting the Administration's submission of proposed modifications in April 2007); *see generally* May 2007 Wainstein Statement, *supra*, at 7; *The Need to Bring the Foreign Intelligence Surveillance Act into the Modern Era: Hearing Before the S. Select Comm. on Intel.*, 110th Cong. (2007) (statement of J. Michael McConnell, Dir. of Nat'l Intel.).

[30] *See* S. Rep. No. 110-209, at 5 (2007).

[31] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

[32] Protect America Act § 6(c).

[33] 2008 Mukasey Decl., *supra*, at 13 n.22.

[34] *See* Protect America Act—Extension, Pub. L. No. 110-182, 122 Stat. 605 (2008) (extending Protect America Act for two weeks).

[35] Protect America Act § 6.

collect effectively the foreign intelligence information necessary to protect the Nation."[36] The government argued that the constraints on the use of FISA that necessitated the PAA could not be met only by increasing resources; rather, FISA had to be amended to eliminate those constraints.[37] Finally, the Administration argued that the Intelligence Community should "not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States."[38]

In response to the Administration's request, the Senate Select Committee on Intelligence (SSCI) approved a bill in the fall of 2007 that formed the basis for what eventually became the FISA Amendments Act (FAA) of 2008. In its report on the bill, the SSCI stated that the legislation would make permanent the PAA's provisions authorizing "targeting of foreign terrorists and other foreign intelligence targets reasonably believed to be located outside the United States" without individualized FISC orders, "but the bill also significantly increases protections of the civil liberties of U.S. persons located inside and outside the United States."[39] Among these protections were a prohibition on reverse targeting of persons located in the United States under Section 702,[40] and the requirement to obtain a FISC order prior to targeting U.S. persons located overseas (now Sections 703 and 704 of FISA).[41] It included new requirements to report on the use of the authorities to Congress,[42] review of the TSP program by Inspectors General of the relevant agencies,[43] and disclosure to Congress of important rulings by the FISC.[44] The bill also reaffirmed that provisions of Title 18 and FISA were "the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted" unless explicitly amended by Congress.[45] The bill passed Congress with significant bipartisan

[36] *FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 1 (2007) (statement of Kenneth L. Wainstein, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just.).

[37] *See Administration Views of FISA Authorities: Hearing Before the H. Permanent Select Comm. on Intel*., 110th Cong. 16, 24 (2007) (statement of Kenneth L. Wainstein, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just.).

[38] *Id.* at 20.

[39] S. Rep. No. 110-209, at 6.

[40] *Id.* at 6, 14-15. Namely, targeting a person outside the United States as a pretext, when the real intention is to acquire the communications of someone inside the United States.

[41] *Id.* at 6, 15.

[42] *Id.* at 6, 17.

[43] *Id.* at 17.

[44] *Id.*

[45] *Id.*

support,[46] and President Bush signed the FISA Amendments Act into law in July 2008.[47] The FISA Amendments Act replaced the expired Protect America Act provisions with the new Section 702 of FISA, which was set to expire on December 31, 2012. The authorities and limitations of Section 702 are discussed in detail in this Report. In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which require judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information.[48]

Congress reauthorized the expiring FISA provisions without changes in December 2012 with significant bipartisan support.[49] The only change to the statute approved by Congress was to extend Section 702's expiration date to December 31, 2017.

Less than six months after this 2012 reauthorization, the press began reporting on classified documents regarding U.S. surveillance programs, including surveillance under Section 702, leaked without authorization by Edward Snowden, a former NSA contractor.[50] As noted in the Introduction to this Report, it was this action that led to the PCLOB's 2014 comprehensive study and report on the program implemented under Section 702 of FISA, as well as a separate study and report of a program implemented under Section 215 of the USA PATRIOT Act.

According to the DNI, the Snowden disclosures caused "profound damage" to U.S. national security.[51] At the same time, the disclosures led to greater public and congressional attention to U.S. surveillance activities, as reflected in enactment of the USA FREEDOM Act in 2015 and in the debate over reauthorization of Section 702 that took place in 2017. Legislators considered, among other things, the "querying," or searching, of the intelligence collected under Section 702 for information about U.S. persons, and so-called "abouts" collection, which involved NSA's acquisition of communications that contained a reference to a tasked selector, such as an email address or other identifier, but were not necessarily to or from that tasked selector.[52] Congress voted to reauthorize Section 702, again with significant bipartisan support, and the final

[46] The Senate passed the bill by a vote of 68-29 and the House of Representatives by a vote of 293-129.

[47] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L. No. 110-261, 122 Stat. 2436 (2008).

[48] 50 U.S.C. §§ 1881b-c.

[49] The Senate passed the reauthorization by a vote of 73-24 and the House of Representatives by a vote of 301-118.

[50] *See NSA collecting phone records of millions of Verizon customers daily*, *supra*.

[51] *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Select Comm. on Intel.*, 113th Cong. 2 (2014) (statement of James R. Clapper, Dir. of Nat'l Intel.) ("[W]e've lost critical foreign intelligence collection sources, including some shared with us by valued partners. . . . We are beginning to see changes in the communications behavior of adversaries . . . particularly terrorists. . . .").

[52] *See, e.g.*, USA Liberty Act of 2017, H.R. 3989, 115th Cong. (2017).

bill was signed by the President on January 19, 2018.[53] The reauthorization legislation made some changes to the statute, including: requiring agencies to develop and submit to the FISC specific procedures for querying U.S. person information;[54] requiring a FISC order before the Federal Bureau of Investigations (FBI) can view results of a limited category of queries of U.S. person information;[55] and requiring FISC approval and congressional notification to conduct "abouts" collection,[56] which NSA had voluntarily ceased (all described in more detail below);[57] as well as other changes intended to improve oversight and transparency of the program.[58]

Under the statute enacted in 2018, Section 702 is scheduled to expire on December 31, 2023, and its reauthorization process provides another opportunity for evaluation by Congress and the public of its purpose, procedures, and protections.[59]

II. Differentiating Section 702 from other FISA Authorities

Section 702 statutorily authorizes the government to target non-U.S. persons, reasonably believed to be located outside the United States, in order to collect foreign intelligence information using the compelled assistance of U.S. ECSPs.[60] The government may target only individuals who are expected to communicate, receive, or possess foreign intelligence information within given categories of intelligence previously authorized by the Attorney General and the DNI and certified for collection by the FISC.[61] By contrast, Titles I and III of FISA authorize the targeting of different individuals, including U.S. persons, using additional collection methods, and in the case of Titles I and III, require higher burdens of proof.

Titles I and III, frequently referred to as "traditional FISA," authorize electronic surveillance and physical search occurring inside the United States. These authorities require a heightened burden of proof: that is, a showing of probable cause that the target of the surveillance is a foreign power or an agent of the foreign power.[62] Unlike Section 702, which may only be

[53] FISA Amendments Reauthorization Act of 2017.

[54] *Id.* § 101.

[55] 50 U.S.C. § 1881a(f)(2).

[56] FISA Amendments Reauthorization Act of 2017 § 103.

[57] Press Release, Nat'l Sec. Agency, *NSA Stops Certain Section 702 "Upstream" Activities* (Apr. 28, 2017), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618699/nsa-stops-certain-section-702-upstream-activities/.

[58] FISA Amendments Reauthorization Act of 2017.

[59] *Id.* § 201.

[60] 50 U.S.C. § 1881a(a), (b)(3), (h)(2)(A)(vi).

[61] OFF. OF THE DIR. OF NAT'L INTEL, SECTION 702: TARGETING UNDER FISA SECTION 702 (2023), https://www.odni.gov/files/FISA_Section_702/Targeting _Under_Section_702_FISA.pdf [hereinafter Section 702: Targeting Under FISA Section 702]. However, a U.S. person could not be a target under Section 702.

used to target non-U.S. persons located abroad, Titles I and III may be used to target U.S. persons and individuals located in the United States based on individualized court orders.[63]

Title IV of FISA authorizes the installation and use of Pen Register and Trap and Trace (PR/TT) devices when the information requested is (a) foreign intelligence information not concerning a U.S. person; or (b) relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities.[64] PR/TT devices are used to capture metadata associated with, but not the content of, communications. PR/TT collection is conducted domestically and may target both individuals located in the United States and U.S. persons. While Section 702 collection may include metadata, it may not target individuals located in the United States or U.S. persons.

Title V of FISA authorizes the government to obtain FISC orders compelling the production of business records with the assistance of certain companies.[65] Title V, as amended by Section 215 of the USA PATRIOT Act, previously authorized the compelled production of "any tangible thing," and following enactment of the USA FREEDOM Act in 2015, this included specific authorization for the production of call detail records.[66] However, Section 215 lapsed after expiration of the March 15, 2020 sunset date, and since then the authority under Title V has generally reverted to its original scope, which restricts the types of businesses that may be compelled to participate and the scope of what constitutes a business record.[67] The only types of businesses currently covered under this portion of FISA are common carriers (i.e., transportation companies), public accommodation facilities, storage facilities, and vehicle rental facilities located in the United States.[68] In order to obtain an order under Title V, the government must present specific and articulable facts giving reason to believe that the records pertain to a foreign power or an agent of a foreign power, but there is no requirement that the foreign power or agent of a foreign power be located outside the United States or be a non-U.S. person.[69]

Under Title VII, but separate and distinct from Section 702, are Sections 703, 704, and 705. These sections allow for the targeting of U.S. persons located outside the United States, and all require a probable cause showing that the target is a foreign power or agent of a foreign power

[62] 50 U.S.C. §§ 1802(a)(1), 1822(a)(1).

[63] *Id.* §§ 1806(a), 1825(a)-(b).

[64] *Id.* § 1842(a)(1).

[65] *Id.* § 1862(a).

[66] *See* 2014 and 2020 PCLOB reports relating to Section 215 of FISA.

[67] 50 U.S.C. § 1862(a).

[68] *Id.*

[69] *Id.* § 1862(b)(2)(B).

or, for Sections 703 and 704 only, officers or employees of a foreign power. Section 703, pursuant to an order issued by the FISC, allows for the targeting inside the United States of U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[70] Subject to certain exceptions, Section 704 requires the government to obtain a FISC order to target a U.S. person located outside the United States in circumstances when the government would have been required to obtain a probable cause warrant to conduct collection against that person domestically.[71] Section 705 permits the Attorney General to approve similar collection against a U.S. person who is already the subject of a FISC order obtained pursuant to Section 104 or 304 of FISA.[72] Again, these provisions are separate and distinct from Section 702, because Section 702 may not be used to target U.S. persons.

As noted above, Section 702 authorizes the government to target individuals for purposes of collecting foreign intelligence information. However, unlike traditional FISA, it does not require that a target be a "foreign power" or "agent of a foreign power," terms that are defined in the FISA statute and, for the latter, generally requires targets outside the United States to be acting on behalf of a foreign power for clandestine intelligence or engaging in specific categories of activity such as international terrorism.[73] The Intelligence Community uses Section 702 to surveil various categories of foreign intelligence targets who may fall outside of the FISA definition of an agent of a foreign power, such as international cyber actors who attack non-U.S. victims. Persons who are close contacts of terrorists or weapons proliferators and are in communication with them may also be targeted under Section 702, though they likewise may not be covered by the definition of "agent of a foreign power" under the FISA definition.

III. Statutory Structure of Section 702 and 2018 Reauthorization

A. Statutory Structure: Authorities, Limitations, and Reporting

Section 702 permits the Attorney General and the DNI jointly to authorize the (a) targeting of non-U.S. persons, (b) who are reasonably believed to be located outside the United States, (c) with the compelled assistance of ECSPs, (d) to acquire foreign intelligence information.[74]

On January 19, 2018, Congress enacted the FISA Amendments Reauthorization Act of 2017 reauthorizing Section 702 through 2023.[75] The legislation established the statutory structure for operation of the program today. In addition to reauthorizing Section 702, it imposed limitations

[70] *Id.* § 1881b(a).

[71] *Id.* § 1881c(a).

[72] *Id.* § 1881d.

[73] *Id.* § 1801(b).

[74] *Id.* § 1881a(a), (b)(3), (h)(2)(A)(vi).

[75] FISA Amendments Reauthorization Act of 2017 § 201.

on the government's authority to use Section 702 and included some additional privacy and civil liberties safeguards under FISA and other U.S. intelligence laws.[76] The following discussion describes Section 702's statutory framework with particular emphasis on significant areas that were altered by the legislation.

B. Statutory Definitions and Limitations on Government's Authority

As noted above, there are four key aspects of the Section 702 authorization, each defined and limited by statute.

First, Section 702 authorizes the *targeting of non-U.S. persons*.[77] While FISA does not define *targeting*, it is generally understood to constitute the use of collection authority on a specified individual or group.[78] The definition of "person" includes not only natural persons, but also groups, entities, associations, corporations, or foreign powers.[79] The definition of "person" is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a "person," but an entire foreign country and all its citizens cannot be a "person" targeted under Section 702.[80] In addition, the persons who may be targeted under Section 702 cannot intentionally include United States persons.[81] "United States persons" or "U.S. persons" are U.S. citizens, U.S. lawful permanent residents (green card holders), groups substantially composed of U.S. citizens or lawful permanent residents, and virtually all U.S. corporations.[82] As is discussed in detail below, NSA targets persons by tasking "selectors," such as email addresses and telephone numbers. NSA must make determinations (regarding location, U.S. person status, and foreign intelligence purpose) about the users associated with each selector on an individualized basis. It cannot simply assert that it is targeting a particular terrorist group. According to their respective targeting procedures, NSA and FBI each must make independent determinations, for each potential

[76] *Id.* §§ 108-109.

[77] 50 U.S.C. § 1881a(a).

[78] Section 702: Targeting Under FISA Section 702, *supra*.

[79] 50 U.S.C. §§ 1801(m), 1881(a). The term "foreign power" is a defined term in FISA; it includes international terrorist groups, foreign governments, and entities not substantially composed of U.S. persons that are engaged in the proliferation of weapons of mass destruction.

[80] *See* Priv. and C.L. Oversight Bd., *Transcript of Hearing on Government Surveillance Programs*, at 71 (Mar. 19, 2014), https://documents.pclob.gov/prod/Documents/EventsAndPress/d974abd8-af20-4c8c-8a61-13f4b71ee1ac/20140319-Transcript.pdf [hereinafter PCLOB March 2014 Hearing Transcript] (statement of Rajesh De, Gen. Couns., Nat'l Sec. Agency).

[81] 50 U.S.C. § 1881a(b)(3).

[82] *Id.* § 1801(i) (providing that corporations or associations that would otherwise be U.S. persons are not U.S. persons if they are a foreign power as defined in 50 U.S.C. § 1801(a)(1)-(3)).

target, regarding the target's U.S. person status, using supporting facts and data, and must rebut facts giving rise to any indication that a target is a U.S. person prior to targeting.[83]

Second, under Section 702, the non-U.S. person target must also be *reasonably believed to be located outside the United States*.[84] A "reasonable belief" is not defined in FISA, but Section 702 does require that targeting procedures (described in further detail below) be adopted to ensure that Section 702 acquisition is limited to targets reasonably believed to be located outside the United States. The targeting of persons believed to be located in the United States is not permitted by Section 702, whether the persons in question are U.S. persons or not.[85] According to NSA's FISC-approved targeting procedures, this determination of "foreignness," encompassing both a target's non-U.S. person status and location outside the United States, is a reasonable determination based on the totality of the circumstances available at the time of targeting.

Third, under Section 702, targeting of non-U.S. persons reasonably believed to be located outside the United States occurs with the *compelled assistance of electronic communication service providers*.[86] FISA defines ECSPs to include telecommunications carriers, providers of electronic communication services,[87] providers of remote computing services,[88] or any other communication service provider who has access to wire or electronic communications.[89] The Attorney General and the DNI compel assistance through the issuance of written directives to these providers.[90] Given the nature of the Internet, communications generated and delivered through

[83] NAT'L SEC. AGENCY, EXHIBIT A, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 1-4 (2022) [hereinafter 2021 NSA Targeting Procedures]; FED. BUREAU OF INVESTIGATION, EXHIBIT C, PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 1-2 (2021) [hereinafter 2021 FBI Targeting Procedures].

[84] 50 U.S.C. § 1881a(a).

[85] *Id.* § 1881a(d)(1)(a).

[86] *Id.* § 1881a(i)(1).

[87] *Id.* § 1881(b)(4)(B). Electronic communications include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12).

[88] 50 U.S.C. § 1881(b)(4)(C). Remote computing services provide the public "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[89] 50 U.S.C. § 1881(b)(4).

[90] *Id.* § 1881a(i)(1).

communication services offered directly to individuals by one entity may be acquired as they cross the network of another provider without the knowledge of the consumer-facing provider.[91]

Fourth, the targeting of non-U.S. persons reasonably believed to be located outside the United States must be conducted *to acquire foreign intelligence information*. Non-U.S. persons located abroad may be targeted under Section 702 only if the government has reason to believe that those persons possess, are expected to receive, or are likely to communicate foreign intelligence information.[92] As defined by FISA, foreign intelligence information is information that relates to the ability of the United States to protect against actual or potential attack by a foreign power, sabotage, international terrorism, the proliferation of weapons of mass destruction by a foreign power, or clandestine intelligence activities by a foreign power.[93] It also includes information with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States or the conduct of the foreign affairs of the United States.[94] In drafting the annual certifications, the Attorney General and the DNI specify the categories of foreign intelligence information the government is seeking to acquire. Such categories are informed by the National Intelligence Priorities Framework, which establishes the President's national security priorities, allocating resources and adjusting mission focus accordingly.[95]

Although the government may use Section 702 only to target non-U.S. persons, communications of U.S. persons or information concerning them may be "incidentally" collected when a lawfully targeted non-U.S. person communicates with or talks about a U.S. person.

Although the government may use Section 702 only to target non-U.S. persons, communications of U.S. persons or information concerning them may be "incidentally" collected when a lawfully targeted non-U.S. person communicates with or talks about a U.S. person.[96] Since

[91] 2014 PCLOB Report, *supra*, at 22.

[92] Section 702: Targeting Under FISA Section 702, *supra*.

[93] 50 U.S.C. § 1801(e)(1).

[94] *Id.* § 1801(e)(2).

[95] OFF. OF THE DIR. OF NAT'L INTEL., INTELLIGENCE COMMUNITY DIRECTIVE 204, NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK (2021).

[96] OFF. OF THE DIR. OF NAT'L INTEL., SECTION 702: INCIDENTAL COLLECTION IN A TARGETED INTELLIGENCE COLLECTION PROGRAM (2023), https://www.odni.gov/files/FISA_Section_702/Incidental_Collection_Section_702_FISA.pdf. In this fact sheet, the IC has defined incidental as the collection of communications between a Section 702 target and non-targets. The term has also been used to refer to the collection of information concerning U.S. persons. For example, then-General Counsel of ODNI Bob Litt elaborated on the definition in a 2015 Brookings speech where he noted: "Rather, the concerns about this statute, at least within the United States, have to do with the fact that even when we are targeting non-U.S. persons we are inevitably going to collect the communications of U.S. persons, either because U.S. persons are talking to the foreign targets, or, in in some limited circumstances, because we cannot technically

the enactment of Section 702, the intelligence community has stated that it cannot provide metrics to identify the amount of incidentally collected U.S. person information under Section 702.[97]

There are currently three certifications under which foreign intelligence information may be obtained. These certifications authorize the collection of foreign intelligence information about foreign governments and related entities; counterterrorism; and combatting proliferation.[98] Cybersecurity-related targets may fall under any of the three certifications.[99]

In addition to defining the scope of the Section 702 authorization, Congress specified limitations on the government's authority to engage in Section 702 targeting. As previously mentioned, the government may not intentionally target U.S. persons or persons "known at the time of the acquisition to be located in the United States."[100] The government is also prohibited from engaging in "reverse targeting," i.e., intentionally targeting a non-U.S. person located abroad, when the "purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States."[101] In other words, the ban on reverse targeting prohibits the government from targeting a non-U.S. person outside the United States when the real interest is to target a person in the United States. Under Section 702, the government also "may not intentionally acquire communications as to which the sender and all of the intended recipients are known at the time of the acquisition to be located in the United States."[102] Finally, Section 702 contains a

separate the communications we are looking for from others. This is called "incidental" collection because we aren't targeting the U.S. persons."

[97] In the 2014 PCLOB Report, the Board recommended that NSA "implement measures to provide insight about the extent to which…NSA acquires and utilizes the communications involving U.S. persons and people located in the United States." *See* 2014 PCLOB Report, *supra*, at 146. NSA has explained that it is often difficult or impossible to determine from a communication the nationality of its participants, and that the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired without conducting an individualized analysis of each unknown communicant. This could include reviewing the content of communications to or from that communicant that NSA otherwise would have no legitimate foreign intelligence purpose to examine and thus never would review. In 2016, NSA stated that it would endeavor to develop metrics that could provide an estimate of the extent of U.S. person information collected incidentally under Section 702. However, in June 2017, the then-Director of National Intelligence testified to Congress that it would be infeasible for the intelligence community to provide such an estimate. Since that time, NSA has continued to assert that it would be infeasible to provide further metrics about the volume of incidental collection of U.S. person information that would be accurate and meaningful. *See Open Hearing on FISA Legislation: Hearing Before the S. Select Comm. on Intel.*, 115th Cong. 84 (2017) (statement of Daniel R. Coats, Dir. of Nat'l Intel.).

[98] Memorandum Opinion and Order, at 10, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) [hereinafter Apr. 21, 2022 FISC Opinion and Order].

[99] Nat'l Sec. Agency, Text for training for course OVSC1203 which concerns FISA 702 for training that is operational as of September 16, 2022, at 7 (Sept. 19, 2022).

[100] 50 U.S.C. § 1881a(b)(1).

[101] *Id.* § 1881a(b)(2).

[102] *Id.* § 1881a(b)(4).

limitation that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment.[103]

C. Changes to Section 702 Pursuant to the FISA Amendments Reauthorization Act

In its 2018 reauthorization of Section 702, Congress required the Attorney General and the DNI to adopt separate querying procedures consistent with the Fourth Amendment to govern certain "queries" (searches) of Section 702-acquired data with terms and identifiers.[104] Prior to 2018, the rules covering queries of Section 702-acquired information were contained in each agency's minimization procedures and those rules were less detailed. As described in more detail below, minimization procedures govern the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting U.S. persons.[105] As implemented by each respective agency, querying procedures generally contain a definition of "query," the procedural standard for when queries are authorized, and exceptions.[106] While the query standard under the querying procedures applicable to the agencies is agnostic as to whether the query uses U.S. person or non-U.S. person identifiers, certain requirements for reporting, review, and approval are specific to U.S. persons. Congress also required that the querying procedures "include a technical procedure whereby a record is kept of each United States person query term used for a query."[107] Pursuant to statute, these procedures must be reviewed annually by the FISC to ensure they satisfy both of these requirements.[108]

---

[103] *Id.* § 1881a(b)(6).

[104] *Id.* § 1881a(f)(1)(A). As amended by the 2018 reauthorization, Section 702 defines a query as "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through" Section 702 acquisitions. *Id.* § 1881a(f)(3)(B). However, agency rules governing queries of Section 702-acquired information apply to all queries, regardless of the U.S. person status of the subject.

[105] *Id.* §§ 1801(h), 1881a(c)(1)(a), 1821(4).

[106] *See, e.g.*, FED. BUREAU OF INVESTIGATION, EXHIBIT I, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 FBI Querying Procedures]; NAT'L SEC. AGENCY, EXHIBIT H, QUERYING PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 NSA Querying Procedures]; CENT. INTEL. AGENCY, EXHIBIT J, QUERYING PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021); NAT'L COUNTERTERRORISM CTR., QUERYING PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021).

[107] 50 U.S.C. § 1881a(f)(1)(B).

[108] *Id.* § 1881a(f)(1)(C).

Furthermore, Congress imposed heightened requirements on FBI to access the results of certain queries.[109] As amended by the 2018 reauthorization, Section 702 requires that FBI must obtain a FISC order, sometimes referred to as a Section 702(f)(2) order, to review the contents retrieved by a U.S. person query that was not designed to find and extract foreign intelligence information and that was conducted in connection with a predicated criminal investigation not related to national security.[110]

To put this new requirement into context, FBI is authorized to employ particular investigative methods depending on the stage of the inquiry, namely (a) prior to opening an assessment, (b) during an assessment, and (c) during an investigation.[111] Each of these is established by the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and outlined in FBI's Domestic Investigations and Operations Guide (DIOG).[112]

Prior to opening an assessment, FBI personnel can initially process a complaint, observation, or information.[113] During this phase, FBI employees are authorized to engage in certain investigative methods that include: viewing public information; viewing records or other information already in the possession of FBI and DOJ; viewing online services and resources; and conducting voluntary clarifying interviews of the complainant or the person who initially furnished the information.[114] When engaged in these "pre-assessment" activities, FBI employees must have a reason that is tied to an authorized FBI criminal or national security purpose.[115]

When FBI initially receives information regarding a potential threat to national security or a federal crime, FBI may open an assessment so long as it has an authorized purpose and clearly defined objective, such as to detect, obtain information about, or prevent or protect against federal

[109] *Id.* § 1881a(f)(2). This requirement is also codified in Section 702(f)(2) of FISA.

[110] *See* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, at 6-1 (2021) [hereinafter FBI DIOG]. This is in contrast to (a) activities authorized prior to opening an assessment, where the personnel must have a reason that is tied to an authorized FBI criminal or national security purpose; or (b) activities conducted pursuant to an FBI assessment, which require an authorized purpose and clearly defined objectives, but may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence. *Id.* at 5-1.

[111] U.S. DEP'T OF JUST., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS, at 19-24 (2008), https://www.justice.gov/archive/opa/docs/guidelines.pdf [hereinafter The Attorney General's Guidelines for Domestic FBI Operations].

[112] The DIOG provides detailed guidance to officers on a broad range of issues and is intended to standardize investigative practices. FBI DIOG, *supra*, at 1-1; *id.* at 5-11.

[113] FBI DIOG, *supra*, at 5-2.

[114] *Id.* at 5-2-5-3.

[115] *Id.* at 5-1. An example of a pre-assessment activity includes checking records in internal FBI databases or searching Internet databases related to preliminary unverified information through an incoming phone or internet "tip."

crimes or threats to national security.[116] The AGG-DOM do not require any particular factual predication to open an assessment.[117] There are five types of assessments, including those seeking information proactively or in response to investigative leads relating to activities constituting violations of federal criminal law or threats to national security; identifying, obtaining, or utilizing information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities; and seeking information to identify potential human sources.[118] As part of FBI's "pre-assessment" and assessment activities, FBI personnel may conduct queries of Section 702-acquired information provided the queries meet the standards required by FBI's Section 702 querying procedures.[119]

Depending on the information obtained during the assessment, FBI personnel will either close the assessment or open a predicated investigation. Supervisors must approve a predicated investigation.[120] Predicated investigations concerning federal crimes or threats to national security are either preliminary investigations or full investigations.[121] Preliminary investigations may be opened on the basis of any credible "allegation or information" indicating the existence of possible criminal activity or threats to national security, such as if a confidential human source with no established history alleged that an "individual is a member of a terrorist group," or if an analyst, while conducting an assessment, discovers on a blog a threat to a specific person.[122] The acceptable purposes for conducting preliminary investigations include "determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking

[116] *Id.* at 5-2, 5-8. Examples provided in the DIOG when an assessment can be conducted include when there is reason to collect information or facts to determine whether there is a criminal or national security threat and there is a rational and articulable relationship between the stated authorized purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other.

[117] *Id.* at 5-1. The DIOG further specifies that "[a]lthough 'no particular factual predication' is required, the basis of an assessment cannot be arbitrary or groundless speculation, nor can an assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject." The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 17.

[118] FBI DIOG, *supra*, at 5-8.

[119] *See* 2014 PCLOB Report, *supra*, at 137. In 2014, the Board's Recommendation 2 urged FBI to update their minimization procedures to more clearly reflect this actual practice, and FBI implemented this recommendation. However, FBI does not log the number of U.S. person query terms conducted at the assessment and pre-assessment stages and thus, the Board is unable to indicate the exact numbers of searches occurring at this stage. In a response by FBI to the Board's request for further information on the numbers, FBI noted that it "does not have statistics on how many . . . queries were conducted at the assessment stage versus the predicated investigation stage" and that it "does not have the ability at this time to track the number of unique query terms." Fed. Bureau of Investigation, Responses to May 4, 2022 Written Questions Submitted by PCLOB to FBI, at 15 (Sept. 9, 2022); Fed. Bureau of Investigation, Attachment B – Counting U.S. Person Queries, at 2.

[120] FBI DIOG, *supra*, at 6-4; The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 20.

[121] FBI DIOG, *supra*, at 6-1; The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 21.

[122] FBI DIOG, *supra*, at 6-1, 6-3; The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 21.

place; identifying, locating, and apprehending the perpetrators; obtaining evidence needed for prosecution; or identifying threats to the national security."[123] All lawful methods may be used in a preliminary investigation, except for mail opening, physical search requiring a search warrant or a FISA order, electronic surveillance requiring a "judicial order or warrant (Title III of FISA), or Title VII FISA requests."[124]

A full investigation may be opened if there is an "articulable factual basis" that reasonably indicates that criminal activity or a national security threat existed, exists, or may exist in the future.[125] The AGG-DOM and the DIOG authorize a full investigation to be opened in order to detect, obtain information about, or prevent or protect against federal crimes or threats to national security or to collect foreign intelligence information.[126] An example would be corroborated information from an intelligence agency stating that an individual is a member of a terrorist group; or if an analyst discovers on a blog a threat to a specific home builder and additional information connecting the blogger to a known terrorist group is uncovered.[127]

As noted, the new Section 702(f)(2) requirement applies only at the predicated investigation stage and applies only if the query is "not designed to find and extract foreign intelligence information" (that is, its purpose is to retrieve solely evidence of a crime unrelated to national security).[128] To obtain an order under Section 702(f)(2) to access the contents of communications returned by such a query, FBI must demonstrate probable cause to believe the information will provide evidence of criminal activity, contraband, fruits of a crime, or other items illegally possessed by a third party, or property designed for use, intended for use, or used in committing a crime.[129] Further, information found in the results of such a query may not be used as evidence in a criminal proceeding unless such a FISC order was obtained prior to reviewing the query results or the proceeding affects, involves, or is related to national security or specified serious crimes.[130] However, an order is not required if FBI determines that "there is reasonable

[123] FBI DIOG, *supra,* at 6-1; The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 21.

[124] FBI DIOG, *supra*, at 6-8. This means that methods such as National Security Letters, FISA Orders for business records, online databases and resources, and other investigative methods are authorized to be used in preliminary investigations.

[125] *Id.* at 7-1; The Attorney General's Guidelines for Domestic FBI Operations, *supra,* at 22.

[126] FBI DIOG, *supra*, at 7-1; The Attorney General's Guidelines for Domestic FBI Operations, *supra*, at 22.

[127] FBI DIOG, *supra*, at 7-3.

[128] 50 U.S.C. § 1881a(f)(2)(A), (F).

[129] *Id.* § 1881a(f)(2)(C).

[130] *Id.* § 1881a(j)(3)(D)(i).

belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm."[131]

Congress also imposed changes affecting NSA's upstream collection. As noted in the 2014 PCLOB Report, NSA previously used a form of collection that targeted communications that were not necessarily either to or from a tasked selector, but contained a tasked selector in the communication.[132] This type of collection was referred to as "abouts" collection. It was criticized because there are increased privacy risks associated with collecting communications that are neither "to" nor "from" a target. In addition, NSA stated it could not be reasonably sure that wholly domestic communications—i.e., communications in which the sender and all intended recipients are persons located in the United States—were excluded from collection. Because of these concerns that the acquisition of "abouts" communications could include the collection of wholly domestic communications, NSA minimization procedures prohibited the use of U.S. person identifiers in querying data acquired through upstream collection.

In October 2016, the government informed the FISC of "significant non-compliance with the NSA's minimization procedures." These non-compliance events involved the use of U.S. person identifiers in queries into data collected using upstream collection,[133] which, as described above, were prohibited by NSA's minimization procedures. The FISC noted at the time that "in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented."[134]

After a period of months in which NSA attempted to identify the factors leading to the non-compliance, NSA chose instead to cease "abouts" collection.

NSA publicly explained at the time that it was suspending "abouts" collection due to technical and legal issues with targeting that led to compliance violations (i.e., avoiding domestic communications).[135] NSA examined its use of Section 702 "in consideration of mission needs, technological constraints, and U.S. person privacy interests."[136] Based on this review, NSA decided to cease collecting "abouts" in upstream collection. NSA assessed that this "would allow

[131] *Id.* § 1881a(f)(2)(E).

[132] 2014 PCLOB Report, *supra*, at 37.

[133] Memorandum Opinion and Order, at 34, *In re DNI/AG 702(g) Certification 2016-A, In re DNI/AG 702(g) Certification 2016-B, In re DNI/AG 702(g) Certification 2016-C* (FISA Ct. Apr. 26, 2017), https://dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[134] *Id.* at 20.

[135] *NSA Stops Certain Section 702 "Upstream" Activities*, *supra*.

[136] Nat'l Sec. Agency, NSA Responses to PCLOB Requests Numbered 2, 3, 4, 7, and 17 (dated August 31, 2022), at 2 (Nov. 10, 2022).

NSA to continue the collection activities that preserved the most valuable foreign intelligence information obtained via upstream collection activities while terminating prior aspects of upstream collection that NSA assessed were most likely to result in the acquisition of non-pertinent communications concerning non-consenting U.S. persons."[137]

Congress in 2018 prohibited upstream "abouts" collection, but left open the possibility of resuming this collection technique.[138] As amended by the 2018 reauthorization, should the Attorney General and DNI decide to resume intentional acquisition of "abouts" collection, absent an emergency situation (which has not occurred up to this point), the government must obtain approval from the FISC and inform Congress.[139] The written notice to Congress, which must be provided 30 days prior to commencing such collection, must include the FISC decision, order, or opinion approving the program and "a summary of the protections in place to detect any material breach."[140] Furthermore, Congress directed the FISC to consider appointing an *amicus curiae* to advocate for individual privacy and civil liberties interests during its review of any such proposed collection.[141] Finally, upon notification to Congress, Congress may hold hearings and review the proposed collection.[142]

Congress also bolstered transparency requirements. The government must report annually a good faith estimate of the number of (a) Section 702 targets, (b) non-U.S. persons targeted pursuant to certain FISC orders, and (c) criminal proceedings in which the government provides notice to a person of its intent to disclose information acquired or derived from FISA acquisition.[143] Further, as recommended in the 2014 PCLOB Report, the statute now requires publication of the FISC-approved Section 702 minimization procedures after a classification review and application of necessary redactions.[144]

D. Section 702 Certifications

As explained above, under Title I and III of FISA, the government must apply for authorization from the FISC in order to conduct electronic surveillance or physical search of a

[137] *Id.*

[138] FISA Amendments Reauthorization Act of 2017 § 103(b)(2)(A).

[139] *Id.* § 103(b)(2), (b)(4).

[140] *Id.* § 103(b)(3).

[141] *Id.* § 103(b)(6).

[142] *Id.* § 103(b)(2)(B).

[143] *Id.* §§ 102, 104, 107.

[144] *Id.* § 104.

specific target located within the United States.[145] This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance or physical search;[146] facts justifying a probable cause finding that this target is a foreign power or an agent of a foreign power and uses (or is about to use) the communication facilities or places at which the electronic surveillance or physical search is being directed;[147] minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance or physical search; and a certification regarding the foreign intelligence information sought.[148] If the FISC judge who reviews the government's application determines that it meets the required elements—including that there is probable cause to believe that the specified target is a foreign power or an agent of a foreign power and that the minimization procedures meet the statutory requirements—the FISC will issue an order authorizing the requested electronic surveillance.[149] The interests of U.S. persons and persons located in the United States implicated by traditional FISA authorities weigh in favor of these more rigorous restrictions.

Section 702, which permits targeting of non-U.S. persons located outside the country, differs from the traditional FISA framework both in the standards it applies and in the lack of individualized and particularized determinations by the FISC. Under the statute, the Attorney General and the DNI make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.[150] There is also no requirement that the government demonstrate probable cause to believe that a Section 702

Section 702, which permits targeting of non-U.S. persons located outside the country, differs from the traditional FISA framework both in the standards it applies and in the lack of individualized and particularized determinations by the FISC.

[145] 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. *Id.* § 1805(e).

[146] *Id.* § 1804(a)(2).

[147] *But see* 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders "in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown.").

[148] *Id.* §§ 1804(a), 1805(a).

[149] *Id.* § 1805(a), (c)-(d).

[150] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 97 (noting that Section 702 provides an alternative means of authorizing electronic surveillance without relying upon individualized applications); 50 U.S.C. § 1881a(a); NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 2 (2014), https://media.defense.gov/2021/Aug/18/2002833876/-1/-1/0/NSA_REPORT_ON_SECTION_702_PROGRAM.PDF (noting that Section 702 certifications do not require "individualized determination" by the FISC).

target is a foreign power or agent of a foreign power, as is required under traditional FISA.[151] Instead of identifying particular individuals to be targeted under Section 702, annual certifications identify the categories of foreign intelligence information regarding which the Attorney General and the DNI authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad.[152] The categories of information being sought must meet the definition of foreign intelligence information described above.

While individual targets are not submitted to the FISC or any other judicial authority for review, Section 702 certifications must contain "targeting procedures" approved by the Attorney General that must be "reasonably designed" to ensure that any Section 702 acquisition is "limited to targeting [non-U.S.] persons reasonably believed to be located outside the United States" and to prevent the intentional acquisition of wholly domestic communications.[153] The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to communicate or receive) the types of foreign intelligence information authorized by a certification.[154] The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. The Attorney General and the DNI must also attest that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program.[155]

Under these certifications, as noted above, the government is authorized to collect the contents of and metadata associated with electronic communications, such as email and telephone calls of non-U.S. persons, reasonably believed to be located outside the United States.

As also noted above, although only non-U.S. persons may be intentionally targeted, communications of U.S. persons or information about them may be acquired through "incidental collection" if a lawfully targeted non-U.S. person located abroad communicates with or refers to a U.S. person.[156] Section 702, therefore, requires that certifications also include "minimization

[151] *Compare* 50 U.S.C. § 1805(a), (c)-(d) *with* 50 U.S.C. § 1881.

[152] *See id.* § 1881a(h)(2)(A)(v) (requiring the Attorney General and the DNI to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information).

[153] *Id.* § 1881a(d)(1), (h)(2)(A)(i), (h)(2)(B).

[154] *See, e.g.*, 2021 NSA Targeting Procedures, *supra*; 2021 FBI Targeting Procedures, *supra*.

[155] 50 U.S.C. § 1881a(f), (g), (h)(2)(A)(iii). Most critically, the Attorney General's Acquisition Guidelines explain how the government implements the statutory prohibition against reverse targeting.

[156] In the 2014 PCLOB Hearing, in contrast to the "incidental collection" definition described above, then-General Counsel of NSA defined inadvertent collection as "collection not authorized by law." PCLOB March 2014 Hearing Transcript, *supra*, at 102. U.S. person information may also be acquired inadvertently due to an error in targeting or because new information comes to light indicating that the target should be considered a U.S. person. This is referred to as "inadvertent collection" and is distinct from incidental collection, and must generally be destroyed.

procedures" that control the acquisition, retention, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.[157] Minimization procedures are specific procedures reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and restrict the dissemination, of non-publicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[158] Minimization procedures are defined in FISA and must comply with specific statutory requirements. As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances surrounding its acquisition.

Finally, certifications also include "querying procedures."[159] In order to parse through Section 702 collection, analysts often use identifiers for specific individuals, key words, and limiting syntax to retrieve information from all or a portion of the agency's Section 702 collection. Analysts are permitted to search or "query" Section 702 collection if the query is conducted for an authorized purpose, is reasonably designed to retrieve the information sought while limiting the retrieval of other information, and is properly justified.[160] The querying procedures, described in more detail below, define what types of search-related activities the procedures apply to, establish the circumstances under which Section 702 collection may be queried, and exceptions to the query standard. Internal agency policies also specify special types of queries that require heightened review or approval.

E. FISC Review

The government's annual Section 702 certification packages are reviewed by the FISC.[161] In addition to the required procedures, the Section 702 certification packages include affidavits of national security officials[162] that further describe the government's basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorizations and limits.[163] The government may submit additional information explaining how the procedures

[157] 50 U.S.C. § 1881a(e)(1), (h)(2)(A)(ii), (h)(2)(B).

[158] *Id.* § 1801(h)(1).

[159] *Id.* § 1881a(f)(1)(A).

[160] 2021 NSA Querying Procedures, *supra*, at 3-6; 2021 FBI Querying Procedures, *supra*, at 3-7.

[161] 50 U.S.C. § 1881a(d)(2), (e)(2), (j). The Attorney General's Acquisition Guidelines, however, are not subject to FISC approval but must be submitted to the FISC as part of the annual review. *Id.* § 1881a(g)(2)(C). Section 702 does have a provision permitting the Attorney General and the DNI to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. *Id.* 1881a(c)(2).

[162] *Id.* § 1881a.

[163] *See* U.S. DEP'T OF JUST., SEMIANNUAL REPORT OF THE ATTORNEY GENERAL CONCERNING ACQUISITIONS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, at 4-5 (Mar. 2023).

will be applied and describing the operation of the program, through court filings or hearings before the FISC.[164]

By statute, the FISC's review of the Section 702 certifications is limited, as the FISC itself recognized in one instance shortly after the FAA was passed.[165] Unlike traditional FISA applications, when it reviews Section 702 certifications, the FISC does not review targeting decisions for particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding the information to be acquired, the FISC does not see or approve the specific persons targeted or communications facilities tasked for acquisition. Instead of requiring judicial review of these elements, Section 702 calls upon the FISC to decide whether the procedures are reasonably designed to ensure compliance with the guidelines, the statute, and the Fourth Amendment.[166]

In other respects, however, the FISC's role in the Section 702 program is more extensive. Pursuant to statute, if the FISC determines that a Section 702 certification or related documents are insufficient on constitutional or statutory grounds, the FISC cannot itself modify the documents, but will issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification.[167] About a month before filing final versions of certifications and procedures, the government files draft documents with the FISC. FISC staff and advisors review these submissions, obtain feedback from the judge who will consider the certifications, and engage with the government identifying possible deficiencies and necessary clarifications, communicating how the judge would likely rule if the certification package were presented in its draft form. When FISC staff and the government reach a point at which they believe the judge will support a certification application with or without caveats or the government wishes to argue particular issues before the Court, the final language of the certification package is presented to the Court.

1. *Review Process*

Upon receipt of the final documents, the FISC must generally appoint an *amicus curiae* to review any novel or significant interpretations of law.[168] The Court may also appoint *amici* "in

[164] *See, e.g.,* Memorandum Opinion, at 5-9, 15-16, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *2-5 (FISA Ct. Oct. 3, 2011) (describing 2011 government filings with, and testimony before, the FISC and describing representations made to the FISC in prior Section 702 certifications).

[165] Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

[166] 50 U.S.C. § 1881a(j)(2)(B).

[167] *Id.* § 1881a(j)(3)(B).

[168] *Id.* § 1803(i)(2)(A). Congress created the *amicus* role in 2015 under the USA FREEDOM Act. The role is similar to the Special Advocate role proposed by the Board in its 2014 *Report on the Telephone Records Program*

any instance as such court deems appropriate," and this may include instances in which amici may provide technical expertise to the Court.[169] FISC rules also permit individuals and organizations, upon motion, to file a brief.[170] Such engagement enables the FISC to hear argument from independent experts in addition to the government. *Amici* are individuals employed outside the government with expertise in "privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise" to the proceeding and who hold security clearances that enable them to access classified information relevant to the issues before the court.[171] *Amici* are tasked with presenting legal arguments that advance the protection of privacy and civil liberties or lend expertise and further the Court's understanding of intelligence collection, communications technology, or other relevant areas.[172]

In evaluating the sufficiency of a certification package, the FISC not only reviews the language within the submitted documents, but also the government's representations concerning implementation of the various procedures, and the government's compliance record.[173] For example, in 2018 the FISC approved the certifications in part, but also denied them in part.[174] The ruling was not based on the language of the procedures, but on the representations of the government concerning how it proposed to meet its statutory requirements. The Court held that FBI's implementation of its minimization procedures and querying procedures was inconsistent with Section 702 and the Fourth Amendment.[175] Section 702 requires that the querying procedures "include a technical procedure whereby a record is kept of each [U.S.] person query term used for a query."[176] The government asserted that, due to technical limitations in its systems, FBI could not differentiate between non-U.S. person query terms and U.S. person query terms and therefore its approach was "intend[ed] to satisfy the record-keeping requirement by keeping a record of all queries."[177] The FISC held that the law was unambiguous in its directive to keep records of U.S.

Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court.

[169] *Id.* § 1803(i)(2)(B).

[170] U.S. FOREIGN INTEL. SURVEILLANCE CT., RULES OF PROCEDURE, at 2, 15 (2010) [hereinafter FISC Rules of Procedure].

[171] 50 U.S.C. § 1803(i)(3)(A).

[172] *Id.* § 1803(i)(4). A current list of approved *amici* may be found on the FISC's website, available at https://www.fisc.uscourts.gov.

[173] *See, e.g.*, Memorandum Opinion and Order, at 68, 72-79, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Oct. 18, 2018) [hereinafter 2018 Cert FISC Opinion and Order].

[174] *Id.* at 134-35.

[175] *Id.* at 133.

[176] 50 U.S.C. § 1881a.

[177] 2018 Cert FISC Opinion and Order, *supra*, at 52.

person queries as such and that FBI's approach did not satisfy the statutory mandate.[178] Pursuant to this holding, which was affirmed by the Foreign Intelligence Surveillance Court of Review (FISC-R), FBI altered its querying procedures, implemented a temporary process to manually record all U.S. person queries, and ultimately altered its systems to capture this information from FBI users electronically.[179]

In other instances, the FISC has imposed requirements based on the government's compliance record. For example, since at least 2018, the FISC has expressed concern over FBI's query compliance record.[180] Compliance incidents are reported through Rule 13(b) notices and in quarterly reports to the FISC.[181] For a number of years, these incidents have overwhelmingly involved FBI query compliance incidents.[182] In September 2021, the FISC issued an order mandating that FBI revise its minimization procedures for Titles I, III, and business records, which govern queries into other FISA datasets, and its Section 702 querying procedures to ensure consistent standards are established and applied for all FISA datasets.[183] Additionally, by

[178] *Id.* at 61-62.

[179] Memorandum Opinion and Order, at 61-65, *In re DNI/AG 702(h) Certification and its Predecessor Certifications*, Docket No. 702(j)-19-01 and predecessor dockets, *In re DNI/AG 702(h) Certification 2019-B and its Predecessor Certifications*, Docket No. 702(j)-19-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2019-C and its Predecessor Certifications*, Docket No. 702(j)-19-03 and predecessor dockets (FISA Ct. Dec. 6, 2019).

[180] *See* 2018 Cert FISC Opinion and Order, *supra*, at 68-97.

[181] 50 U.S.C. § 1881a(m)(1); FISC Rules of Procedure, *supra*, at 5. As described later in this report, under the FISC Rules of Procedure, all compliance incidents must be reported to the FISC without undue delay in a Rule 13(b) notice and/or in a quarterly report.

[182] *See* U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 DECEMBER 2020 – 31 MAY 2021, at 54-62 (Aug. 2022) [hereinafter 26th Joint Assessment]; U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 JUNE 2020 – 30 NOVEMBER 2020, at 54-62 (Apr. 2022); U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 DECEMBER 2019 – 31 MAY 2020, at 55-64 (Dec. 2021); U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 JUNE 2019 – 30 NOVEMBER 2019 (Sept. 2021), at 56-63; U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 DECEMBER 2018 – 31 MAY 2019 (Aug. 2021), at 58-64.

[183] Order in Response to Querying Violations, at 13-14, *In re DNI/AG 702(h) Certifications 2020-A, 2020-B, 2020-C, and Predecessor Certifications*, Docket Nos. 702(j)-20-01, 702(j)-20-02, 702(j)-20-03, and predecessor dockets,

November 1, 2021, the government was required to submit a description of steps FBI was taking to ensure the querying standard is applied properly, an explanation of the government's interpretation of certain language in the context of requirements under Section 702(f)(2), and an assessment of whether FBI's systems and practices comply with procedural and statutory provisions.[184] In response to oversight findings, subsequent DOJ policy directives, and a September 2021 FISC order, FBI took a number of actions to enhance compliance, including reconfiguring its systems, collaborating with DOJ's National Security Division and the Office of the Director of National Intelligence (ODNI) to develop new guidance and training, implementing internal review and certain approval requirements, and altering policies.[185]

2. *FISC Review of Querying Procedures*

The FISC also has used its authority to impose reporting requirements in the context of reviewing FBI's querying procedures.[186] In 2015, the standard codified in FBI's minimization procedures was "[t]o the extent reasonably feasible . . . [FBI personnel] must design . . . queries to find and extract foreign intelligence information or evidence of a crime," contrasted with today's query standard, which requires that queries be "reasonably likely to retrieve foreign intelligence information . . . or evidence of a crime."[187] This language was interpreted differently by FBI than the querying standard documented in the current querying procedures. In 2015, DOJ represented during a hearing before the FISC that queries must be "reasonably likely" to return foreign intelligence information or evidence of a crime, but did not adopt that language in its procedures until 2018.

While the FISC stated in 2015 that a proper query should be reasonably designed to return foreign intelligence information or evidence of a crime, it also acknowledged that following the attacks on September 11, 2001, one of the main criticisms was a failure to identify and distribute information that could have been used to disrupt the plot.[188] In order to guard against such a failure in the future, the government advised the FISC that FBI had a practice of allowing FBI personnel to conduct federated searches of all datasets, including FISA datasets, whether or not such

In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under FISA, Docket No. 08-1833, *In re FBI Standard Minimization Procedures for Tangible Things Obtained Pursuant to Title V of FISA*, Docket No. BR 13-49 (FISA Ct. Sept. 2, 2021).

[184] *Id.* at 14.

[185] 26th Joint Assessment, *supra*, at 60-62.

[186] *See, e.g.*, 2018 Cert FISC Opinion and Order, *supra*, at 96-97.

[187] 2021 FBI Querying Procedures, *supra*, at 3-4.

[188] Memorandum Opinion and Order, at 42, *In re DNI/AG 702(g) Certification 2015-A and Predecessor Certifications*, Docket No. 702(i)-15-01 and predecessor dockets, *In re DNI/AG 702(g) Certification 2015-B and Predecessor Certifications*, Docket No. 702(i)-15-02 and predecessor dockets, *In re DNI/AG 702(g) Certification 2015-C and Predecessor Certifications*, Docket No. 702(i)-15-03 and predecessor dockets (FISA Ct. Nov. 6, 2015).

personnel were specifically trained or approved to handle such information, so long as personnel who were not specifically trained and approved could not access such information.[189] FBI personnel conducting those queries would be notified if there was a positive hit in Section 702-aquired data and, if so, the user could refer the results to personnel who were appropriately trained and approved to handle FISA-acquired information.[190] Such individuals were tasked with determining whether the information retrieved reasonably appeared to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime.[191] The individuals who conducted the original query were only allowed to review the results if the results were determined to meet one of the standards described above.[192] FBI's 2017 Section 702 minimization procedures (which governed the conduct of queries prior to the implementation of the requirement to maintain separate querying procedures in the 2018 Reauthorization Act) specified that the term "query" did not include situations in which a user does not receive raw FISA-acquired information in response to a query because the user has not been granted access to the raw FISA-acquired information. A similar provision appears in FBI's Section 702 querying procedures today. But by 2018, the Court's position on FBI's practices had changed.

In the 2018 certification process, FBI disclosed to the Court that in fiscal year 2017, it ran approximately 3.1 million queries (U.S. person and non-U.S. person queries combined) into unminimized FISA-acquired information in one system alone.[193] This was concerning to the Court because, unlike other agencies with access to unminimized FISA collection, FBI maintains a domestic-focused mission and is more likely to conduct U.S. person queries.[194] In addition, the 2018 Certifications, including the querying procedures, did not reflect the query standard that the

[189] *Id.*

[190] *Id.*

[191] *Id.* at 8, 12 n. 4 (referencing FBI Minimization Procedures).

[192] *Id.* at 43.

[193] 2018 Cert FISC Opinion and Order, *supra*, at 65. In the Annual Statistical Transparency Report for calendar year 2021, FBI reported that it ran 3.4 million U.S. person queries of Section 702-acquired information in all its systems. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2021, at 21 (2022). This figure was subsequently revised downwards to approximately 2.97 million in accordance with FBI's updated counting methodology developed for the CY2022 Annual Statistical Transparency Report. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2022, at 24 (2023). These numbers represent the number of queries conducted, but do not represent the number of individual U.S. persons who are the subject of those queries.

[194] 2018 Cert FISC Opinion and Order, *supra*, at 66.

government had stated to the Court orally: each query must be reasonably likely to retrieve foreign intelligence information or evidence of a crime.[195]

The FISC appointed an amicus to review the 2018 FBI querying procedures. In a hearing with the amicus and the government, the FISC asked DOJ to clarify what the querying standard meant.[196] DOJ described the querying standard as requiring that the query have a proper (a) purpose; (b) design; and (c) justification, as further described in Part 3 of this Report.[197] DOJ asserted that the query standard had been the same since 2008 even though the language in the procedures had changed.[198] In its subsequent opinion on the 2018 FBI querying procedures, the FISC repeated this three-pronged approach to the querying standard, appearing to agree with DOJ that the standard had not changed.[199] On examination of DOJ's reports of compliance incidents involving FBI queries of FISA-acquired datasets, including the identification of tens of thousands of queries that did not meet the query standard, the Court found that FBI's implementation of its querying rules did not satisfy the querying standard and "were not consistent with the requirements of the Fourth Amendment."[200]

The 2018 ruling triggered a shift in FBI operations. FBI has since altered systems and enhanced training and internal oversight, as described in Part 3 of this Report, and the three-pronged approach to the querying standard was expressly incorporated in the 2021 querying

[195] *Id.*

[196] Transcript of Proceedings Held Before the Honorable James E. Boasberg, U.S. Foreign Intel. Surveillance Ct., at 10, *In re DNI/AG 702(h) Certification 2018-A and Predecessor Certifications, In re DNI/AG 702(h) Certification 2018-B and Predecessor Certifications, In re DNI/AG 702(h) Certification 2018-C and Predecessor Certifications* (FISA Ct. July 13, 2018).

[197] *Id.* at 11-12.

[198] U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., AUDIT OF THE ROLES AND RESPONSIBILITIES OF THE FEDERAL BUREAU OF INVESTIGATION'S OFFICE OF THE GENERAL COUNSEL IN NATIONAL SECURITY MATTERS, at 23 (2022), https://oig.justice.gov/sites/default/files/reports/22-116.pdf. This three-pronged approach was first articulated in June 2018 FBI-DOJ querying guidance. Fed. Bureau of Investigation, DOJ/FBI Guidance for Queries of Raw FISA-acquired Information, at 1-2 (June 18, 2018).

[199] 2018 Cert FISC Opinion and Order, *supra*, at 67. The three-pronged approach to the querying standard was formally incorporated in the 2021 querying procedures. 2021 FBI Querying Procedures, *supra*, at 3-4. This led FBI to question why queries that had not been identified as compliance incidents a year ago, were now being reported as such. FBI asserted that DOJ, and likely the Court, had changed their interpretation of the standard. The FISC and DOJ disagreed, and continue to disagree, with this assertion.

[200] 2018 Cert FISC Opinion and Order, *supra*, at 92.

procedures.[201] Further, DOJ has evolved its FBI field office querying review program over time in response to FBI's query compliance challenges.[202]

With continued focus on FBI queries, and, in particular, U.S. person queries and evidence of a crime queries, the FISC expanded the list of quarterly reporting requirements. As of April 2022, the FISC requires the government to "report each instance in which FBI personnel accessed unminimized Section 702-acquired contents information that the user identified as a query ONLY for evidence of crime,"[203] and "(i) the number of U.S. person queries run by the FBI against Section 702-acquired information; (ii) the number of such queries identified by the user as evidence-of-crime-only queries; (iii) the number of instances in which users of [the FBI system] stated that they had received approval from an FBI attorney to perform a 'batch job' that includes 100 or more queries; and (iv) the number of instances in which users … did not receive prior approval from an FBI attorney for such a 'batch job' due to emergency circumstances."[204] These metrics allow the FISC to monitor and order new requirements for areas it has identified as important from both a privacy and civil liberties perspective and a compliance perspective.

3. *FISC Review of Compliance Incidents*

As discussed further below, the government has an obligation to report compliance incidents to the FISC, and the FISC reviews these incidents. For example, since 2019, the FISC has been tracking issues surrounding the failure of the recipients of intelligence reports to delete reports that have been recalled based on issues with the acquisition of Section 702 collection upon which the reports relied or the handling of Section 702 collection in the reports.[205] That is, when a FISA compliance incident is identified and an agency is required to purge collection, the agency must send recall notices to any recipients of any reports that contain information resulting from that purged collection. According to an ODNI policy on interagency recall, in those instances, a specific "FISA-compliance recall" identifier must accompany all recall notices to notify recipients that the report must be removed with steps taken to prevent its further use or disclosure.[206] A

[201] 26th Joint Assessment, *supra*, at 60-62.

[202] *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 11 (2023) (Joint Statement for the Record of Chris Fonzone, Gen. Couns., Off. of the Dir. of Nat'l Intel., et al.).

[203] A similar requirement had been in place since 2015, but was modified in 2019. Because of how FBI systems are structured, only U.S. person queries where FBI personnel elect to view the results of that query are "identified" as being an evidence of a crime only queries. In other words, non-U.S. person queries and queries where FBI personnel do not elect to access the results of that query do not lead to the system prompts that would ask whether they were evidence of a crime only queries. The government confirmed that reading of the order with the FISC.

[204] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 123-24.

[205] *Id.* at 73.

[206] *Id.; see* OFF. OF THE DIR. OF NAT'L INTEL., INTELLIGENCE COMMUNITY POLICY MEMORANDUM 200 (01) (2020).

FISA-compliance recall notice might be necessitated by a report's failure to properly mask a U.S. person identity that was not necessary to understand the foreign intelligence or failure to properly mark a disseminated report as containing FISA-derived information.

The FISC continued oversight of this issue by instituting a requirement that the government file a report on the implementation of the ODNI policy on interagency recall.[207] Upon reviewing the reports submitted by the government in 2021 and 2022 in response to this requirement, the FISC concluded that there was a continued need for coordination within the Intelligence Community regarding the interagency recall process.[208] The FISC's continued attention to this issue prompted renewed engagement on revising recall policies and procedures and ODNI began holding regular working group meetings with FISA agencies to discuss progress, troubleshoot issues, and gain feedback from the agencies on operational impacts.

F. Directives

As explained above, Section 702 targeting occurs with the assistance of ECSPs. Once Section 702 acquisition has been authorized, the Attorney General and the DNI send written directives to ECSPs compelling the providers' assistance in the acquisition.[209] Providers that receive a Section 702 directive may challenge the legality of the directive before the FISC.[210] The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government in its acquisition of foreign intelligence information.[211] The FISC's decisions regarding challenges and enforcement actions regarding the directives are appealable to the FISC-R and either the government or the provider may request U.S. Supreme Court review of a FISC-R decision.[212]

Certain provisions of FISA, including Section 702, require the government to provide notice to individuals and entities if evidence "obtained or derived from" FISA collection is used against them in a trial, hearing, or other proceeding.[213] The statutory notice provision applies, however, only if the individual or entity is an "aggrieved person" as to that collection, which is defined to mean that the individuals and entity was the target of the acquisition or a person whose

[207] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 74.

[208] *Id.* at 73.

[209] 50 U.S.C. § 1881a(i).

[210] *Id.* § 1881a(i)(4).

[211] *Id.* § 1881a(i)(5).

[212] *Id.* § 1881a(i)(6).

[213] *Id.* §§ 1806(c), 1801(h), 1881e(a). Generally, information is "derived" from surveillance when it would be considered the "fruit of surveillance." *See, e.g.*, *Wong Sun v. U.S.*, 371 U.S. 471, 485-86 (1963).

communications or activities were subject to electronic surveillance, and the evidence used against the individual or entity was obtained or derived from that collection.[214]

As set forth in FISA, this statutory notice obligation applies where: (a) the government "intends to enter into evidence or otherwise use or disclose;" (b) against an "aggrieved person;" (c) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States;" (d) any "information obtained or derived from;" (e) an "electronic surveillance [or physical search] of that aggrieved person."[215]

From 2008—after enactment of Section 702—through 2013, no criminal defendant or other individual or entity was provided notice of use of information obtained or derived from Section 702 collection.[216] In 2012, in *Clapper v. Amnesty International*, the government represented to the U.S. Supreme Court that it had been complying with this notice requirement, but the government subsequently disclosed that it, in fact, had not been complying with the Section 702 notice requirement.[217] Thereafter, DOJ undertook a review of prosecutions in an effort to determine where notice should have been given.[218] The government has represented to the Board that since that time, it has fully complied with its Section 702 notice requirements.[219]

Section 106 of FISA provides a mechanism for individuals or entities who have received notice of the use of Section 702 information to challenge the lawfulness of Section 702 collection through a motion to suppress.[220] The statutory notice provision, however, does not require the government to identify specifically how it retrieved the information from the government's Section 702 holdings, and thus does not require the government to state whether it retrieved the information specifically through a U.S. person query.[221]

---

[214] 50 U.S.C. § 1806 (c)-(d).

[215] *Id.* § 1806(c); *see id.* § 1825(d); Government's Classified Memorandum in Opposition to Defendants' Motion to Suppress Evidence Obtained or Derived From Surveillance Under the FISA Amendments Act and Motion for Discovery, at 65, *U.S. v. Muhtorov*, 20 F.4th 558 (2021) (No. 18-1366); Government's Classified Memorandum in Opposition to Defendants' Motion to Suppress Evidence Obtained or Derived From Surveillance Under the FISA Amendments Act and Motion for Discovery, at 65, *U.S. v. Jumaev*, 20 F.4th 518 (2021) (No. 18-1296).

[216] *U.S. v. Muhtorov*, 20 F.4th 558 (2021).

[217] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).

[218] Sari Horwitz, *Justice is reviewing criminal cases that used surveillance evidence gathered under FISA*, WASH. POST (Nov 15. 2013).

[219] U.S. Dep't of Just., Responses to PCLOB Questions 3 and 4, at 1 (Jan. 26, 2023).

[220] 50 U.S.C. § 1806(a)-(e).

[221] *Id.*

G. Limitations from Executive Order 14086

In October 2022, President Biden issued Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities (E.O. 14086). Among other provisions, that executive order limits the purposes for which the United States may conduct signals intelligence activities to a specified list of twelve legitimate objectives:

(1) Understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and its allies and partners;

(2) Understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) Understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

(4) Protecting against foreign military capabilities and activities;

(5) Protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(6) Protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(7) Protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) Protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) Protecting against threats to the personnel of the United States or of its allies or partners;

(10) Protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified [herein as legitimate objectives];

(11) Protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) Advancing collection or operational capabilities or activities in order to further a legitimate objective identified [herein].[222]

This limitation narrowing the purposes for which signals intelligence may be collected covers all U.S. signals intelligence activities, including collection under Section 702.

[222] Exec. Order No. 14,086, 87 Fed. Reg. 62283, 62283-62284 (Oct. 7, 2022).

PART 3: OPERATIONS AND OVERSIGHT

I. Targeting and Tasking

Under Section 702, non-U.S. persons reasonably believed to be located outside the United States may be "targeted" through the "tasking" of "selectors." *Targets* are individuals, groups, or entities[1] that are expected to receive, communicate, or possess foreign intelligence information within the scope of a specific Section 702 certification. *Selectors* may be communications facilities that are assessed to be used by the target, such as the target's email address or telephone number, as described in more detail below. Selectors associated with targets are *tasked*—i.e., provided—to the relevant ECSP in order to acquire the communications to and from the tasked selector as well as metadata associated with those communications.[2]

To illustrate this process:

- Terrorist 1 uses email address Terrorist1@us-emailco.com to communicate foreign intelligence information about future attacks;
    - Terrorist 1 is the target, a non-U.S. person located outside the United States who is expected to communicate or receive foreign intelligence;
    - Terrorist1@us-emailco.com is the selector associated with the target;
- Terrorist1@us-emailco.com is tasked by the government agency to U.S. Email Co. (the provider);
- U.S. Email Co. provides emails and associated metadata to and from Terrorist1@us-emailco.com back to the government.

The targeting procedures govern this acquisition process.

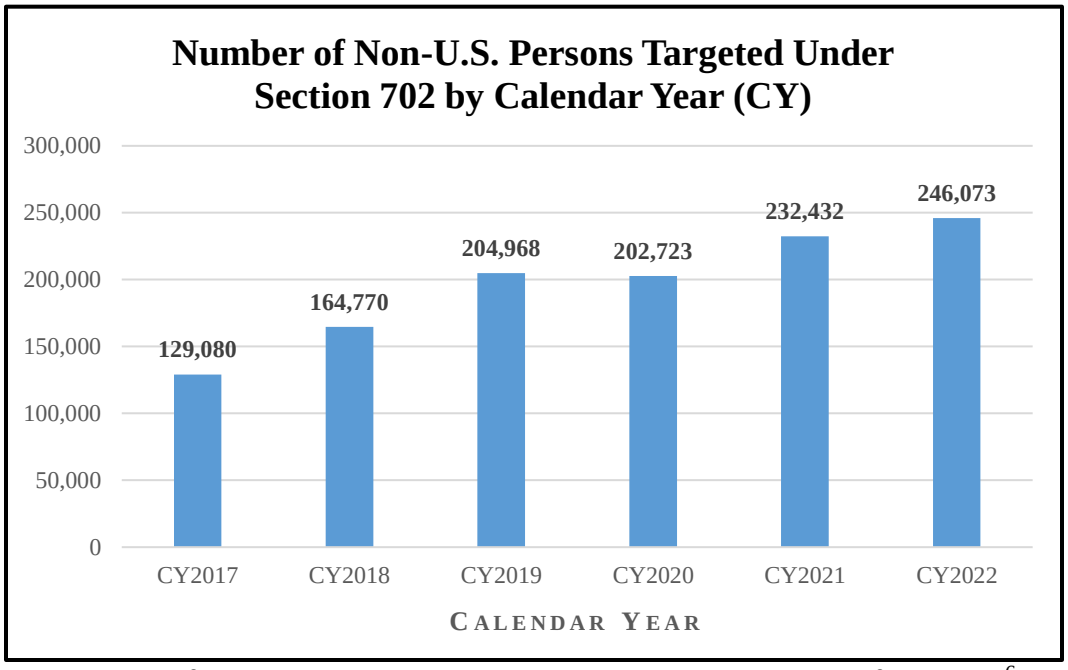
During calendar year 2022, approximately 246,073 non-U.S. persons located abroad were targeted under Section 702.[3] This number is approximate because a single target may use multiple selectors (e.g., multiple email accounts, or an email account and a phone number), but unless and

[1] Under FISA, "person" is defined as "any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m).

[2] Under Section 702, selectors are not names nor keywords, but must be unique identifiers used by communication providers.

[3] Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2022, at Figure 4 (2023) [hereinafter CY2022 ASTR].

until the government "has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target,"[4] which could lead to a potential over-count of the number of targets. On the other hand, in certain circumstances multiple targets may use a single selector (such as a shared email address),[5] leading to the potential under-counting of some targets.



The number of Section 702 targets has nearly doubled over the last five years.[6]

Figure 1

[4] As of December 2021, NSA tasked selectors for collection used by these 232,432 targets. *Id.* at 17.

[5] NSA Procedures and FISC opinions have generally acknowledged that multiple targets may use the same selector. *See, e.g.*, Nat'l Sec. Agency, Exhibit B, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 6 (2022) [hereinafter 2021 NSA Minimization Procedures] ("[N]ote that any user of a tasked selector is regarded as a person targeted for acquisition.").

[6] *See* Bar Graph. CY2022 ASTR, *supra*; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2021 (2022) [hereinafter CY2021 ASTR]; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2020 (2021) [hereinafter CY2020 ASTR]; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2019 (2020) [hereinafter CY2019 ASTR]; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2018 (2019) [hereinafter CY2018 ASTR]; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY

A number of factors have contributed to this increase in the number of non-U.S. persons targeted under Section 702, including:

- The Intelligence Community's use of Section 702 to target cyber actors, which has increased since 2016.
- The Intelligence Community's use of Section 702 to respond to "dynamic intelligence needs," including an increased need for foreign intelligence concerning China and Russia, which has steadily increased since 2016.
- The use of Section 702 by more Intelligence Community analysts who had not been previously trained on the use of the authority.[7]

II. Types of Section 702 Collection

Once a selector has been approved for collection under the Section 702 targeting procedures, it is tasked (or sent to) an ECSP to begin acquisition.[8] As noted above, collection under Section 702 includes messages that are sent or received by targets in communication with other persons.

Depending on the role and function of the provider and the type of information being acquired, the particular manner of acquisition differs. Generally, acquisition under Section 702 falls into one of several categories: upstream, telephony, and downstream. Additionally, in the April 21, 2022 Memorandum and Order, the FISC authorized NSA to use an additional "highly sensitive technique."[9] Within each category, the details of acquisition procedures depend on differing mission requirements and the capabilities and operations of individual providers.[10]

REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2017 (2018) [hereinafter CY2017 ASTR].

[7] Off. of the Dir. of Nat'l Intel., ODNI Supplement for Part III: Response to PCLOB Report Question, at 3 (Feb. 2, 2023).

[8] Nat'l Sec. Agency, Text for training for course OVSC1203 which concerns FISA 702 for training that is operational as of September 16, 2022, at 13 (2022) [hereinafter NSA, OVSC1203: FISA Section 702 Training].

[9] Off. of the Dir. of Nat'l Intel., *Release of Documents Related to the 2021 FISA Section 702 Certification and Title III Physical Search Opinions* (May 19, 2023), https://www.intel.gov/ic-on-the-record-database/results/1259-release-of-two-fisc-decisions-authorizing-novel-intelligence-collection [hereinafter Release of Documents Related to the 2021 FISA Section 702 Certification and Title III Physical Search Opinions].

[10] Upstream and downstream capture electronic communications, also referred to as Digital Network Intelligence, while telephony captures telephone communication and metadata, also referred to as Dialed Number Recognition.

A. Upstream

1. *Overview*

Upstream collection occurs with the compelled assistance of U.S. electronic communications providers that control, operate, or maintain the telecommunications "backbone" over which communications transit.[11] The Internet backbone is a term generally used to describe the set of physical and organizational links that carry Internet traffic along and between individual networks. It encompasses connections such as long-distance fiber-optic connections, undersea cables, and "exchange points" where traffic moves between different providers. Upstream collection occurs inside the United States and only at locations that are likely to carry traffic associated with tasked Section 702 selectors.

These collection accesses, therefore, do not necessarily occur at a provider with whom the targeted person has an account, but instead occur "upstream" in the flow of Internet traffic.[12] Upstream collection is generally used when downstream collection (discussed below) is not.

In most instances, steps are taken to remove known or likely both ends domestic communications from the traffic before further analysis or processing occurs.

The list of tasked selectors for collection in upstream is used to identify a subset of Internet traffic that will be screened for the presence of selectors. The selected traffic is then screened to identify communications that are to or from the tasked selectors. Those identified communications are then ingested into NSA repositories where they are subject to review by NSA analysts.[13]

---

[11] *See* Memorandum Opinion, at 5 n.3, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *2 (FISA Ct. Oct. 3, 2011) [hereinafter Bates October 2011 Opinion] ("The term 'upstream collection' refers to NSA's interception of Internet communications as they transit the facilities of an Internet backbone carrier, […] rather than to acquisitions directly from Internet service providers."); Letter from Kathleen Turner, Dir. of Legis. Aff., Off. of the Dir. of Nat'l Intel., and Ronald Weich, Assistant Att'y Gen., Off. of Legis. Aff., U.S. Dep't of Just., to the Honorable Dianne Feinstein, Chairman, S. Select Comm. on Intel., et al. (May 4, 2012), https://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf; *see also* Priv. and C.L. Oversight Bd., *Transcript of Hearing on Government Surveillance Programs*, at 26 (Mar. 19, 2014), https://documents.pclob.gov/prod/Documents/EventsAndPress/d974abd8-af20-4c8c-8a61-13f4b71ee1ac/20140319-Transcript.pdf [hereinafter PCLOB March 2014 Hearing Transcript] (statement of Rajesh De, Gen. Couns., Nat'l Sec. Agency) ("The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers").

[12] *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, Gen. Couns., Nat'l Sec. Agency) ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

[13] *Id.* at 37 ("To identify and acquire Internet transactions associated with the Section 702-tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are

Upstream collection is not routed to the Central Intelligence Agency (CIA), FBI, or the National Counterterrorism Center (NCTC), and resides only in NSA systems, where it is subject to NSA's minimization procedures.[14] CIA, FBI, and NCTC personnel, therefore, lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in their respective systems. CIA, FBI, NCTC, and other government agencies have access only to minimized upstream collection disseminated by NSA in intelligence reports.

As of 2011, NSA acquired approximately 26.5 million Internet transactions a year from upstream collection.[15] As of 2021, NSA acquired approximately 85.3 million Internet transactions a year from upstream collection, which represents a small portion of NSA's Section 702 collection.[16]

2. *Upstream Collection and the Suspension of "Abouts" Collection*

Prior to 2017, upstream collection acquired not only communications to or from Section 702-tasked selectors, but also "abouts" communications. The need for "abouts" collection stemmed in part from NSA's inability to fully mitigate the technical possibility that it might collect communications that were neither to nor from its target in certain circumstances. "Abouts" communications included communications in which the tasked selector was neither the sender nor the recipient of the communication, but the selector was contained in the body of the communication. An example would be if an individual sent an email to a friend saying "do not open an email from 'JohnTarget@example.com' as it contains malware." In this situation, NSA was targeting the selector JohnTarget@example.com, but the communication was neither to nor from that selector.

As of 2021, NSA acquired approximately 85.3 million Internet transactions a year from upstream collection, which represents a small portion of NSA's Section 702 collection.

The collection of communications that contained a tasked selector, but were not to or from

screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases.").

[14] Nat'l Sec. Agency, Classified Background Information on Upstream from 2014 to 2022, at 2 (Dec. 13, 2022) [hereinafter NSA Classified Background Information on Upstream from 2014 to 2022].

[15] Bates October 2011 Opinion, *supra*, at 73. Although "transaction" has multiple meanings in computer science, NSA and the FISC use it to describe a complete stream of communication between two points (e.g., a complete TCP/IP transmission). A transaction can contain one or multiple discrete communications.

[16] NSA Classified Background Information on Upstream from 2014 to 2022, *supra*, at 2.

the target, caused NSA to collect additional types of traffic. So-called "multi-communication transactions" ("MCTs")[17] described interactions between a service provider and a user such that several individual communications were bundled into a single Internet interaction. If any of those individual messages were to or from a tasked selector, or contained a tasked selector in the body, the entire transaction would be acquired by NSA as one piece of traffic. However, both the overall MCT as well as individual messages within the MCT may have been communications solely between persons located inside the United States and thus ineligible for collection.

As described in Part 2 above, the NSA Director suspended the practice of "abouts" collection in 2017. In the 2018 Reauthorization Act, Congress codified that the government must first obtain approval from the FISC and inform Congress thirty days before restarting "abouts" collection.[18] During the subsequent 2018 Section 702 certification, the FISC considered whether this statutory prohibition bars certain types of downstream collection; the amici argued that the new statutory provision applied to "downstream abouts." The FISC agreed with amici that the statute applied to downstream abouts but held that the specific type of collection proposed did not violate this prohibition.

To date, NSA has not sought to restart "abouts" upstream collection, and NSA's 2023 targeting procedures state that NSA "will not intentionally acquire communications that contain a reference to, but are not to or from, a person targeted" under Section 702.[19]

[17] The term "MCT" was coined by NSA and adopted by the FISC in the Bates October 2011 Opinion to refer to this particular issue within the context of "abouts" collection. PCLOB used the term "MCT" in its 2014 Section 702 Report in discussing the Bates Opinion. However, the reference should be treated as a discrete term of art. PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, at 7 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%20%2014%202022%201548.pdf [hereinafter 2014 PCLOB Report].

[18] *See* description of 2018 Reauthorization Act in Part 2 of this Report.

[19] Nat'l Sec. Agency, Exhibit A, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 2 (2022) [hereinafter 2021 NSA Targeting Procedures].

As also described in Part 2 of this Report, following the 2017 suspension of upstream "abouts" collection,[20] NSA removed from its repositories all unminimized and unevaluated information previously acquired through upstream collection pursuant to Section 702.[21]

3. *Upstream Collection After the Suspension of Abouts*

In 2017, following the end of "abouts" collection, NSA developed a new approach to upstream collection designed to ensure that it only collects communications that are to or from a target, and thereby substantially narrowed the scope of upstream collection.[22] The Board addresses changes made in upstream collection in more detail in the Classified Annex (Annex C) to this Report.

NSA no longer collects "abouts" upstream communications. NSA no longer collects transactions containing multiple communications where the sender or recipient of that transaction is not a targeted selector, even if certain communications within that transaction might be to or from a targeted selector. While NSA may still collect transactions containing multiple communications during upstream collection, it collects only those transactions "to" or "from" a tasked selector.

The government is required to submit quarterly reports to the FISC related to upstream collection that explain how the government is ensuring that it will acquire only communications to or from a Section 702 target, and methods the government is using to monitor compliance with the "abouts" limitation.[23] Further, the government must provide prompt notice to the FISC in the event that new types of selectors are tasked for upstream collection.[24]

B. New Highly Sensitive Technique

In its April 21, 2022 Memorandum and Order, the FISC authorized NSA to use an additional "highly sensitive technique" pursuant to Section 702 "in a manner that is reasonably

[20] NSA Classified Background Information on Upstream from 2014 to 2022, *supra*, at 5. NSA retained certain categories of information, such as serialized reporting and "evaluated minimization traffic" disseminations, completed transcripts and transcriptions of Internet transactions, and information related to taskings and FISA applications.

[21] Memorandum Opinion and Order, at 23, *In re DNI/AG 702(g) Certification 2016-A, In re DNI/AG 702(g) Certification 2016-B, In re DNI/AG 702(g) Certification 2016-C* (FISA Ct. Apr. 26, 2017) [hereinafter 2016 Cert FISC Opinion and Order].

[22] *Id.* at 23.

[23] Memorandum Opinion and Order, at 124, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) [hereinafter Apr. 21, 2022 FISC Opinion and Order].

[24] *Id.* at 124.

expected to result in no incidental collection of U.S. persons' communications."[25] Before approving this technique, the FISC invited briefing by an amicus curiae. In response to issues raised by the FISC and amicus, the government amended the 2021 Certifications to modify NSA's Section 702 targeting and minimization procedures.[26]

The Board has reviewed classified information regarding this collection technique and discusses it in further detail in Annex C to this Report.

C. Telephony[27]

Like upstream collection of Internet traffic, collection of telephone communications begins with NSA's tasking of a selector. Selectors for telephony collection refer to unique signaling information used by network providers to identify the source or destination of a call, such as phone numbers. While implementation differs across ECSPs, for the majority of telephony collection, the ECSP identifies the calls to and from the tasked selectors and provides a copy of those communications to NSA. NSA can acquire the signaling information and content of the phone calls associated with those selectors.

D. Downstream

To facilitate the acquisition of downstream collection,[28] if requested by NSA, FBI may serve a 702 directive on an ECSP, for example an email provider, compelling the provider to collect and produce the communications of an identified selector, for example an email address.[29] In such a case, the ECSP provides the government with communications using that selector until the government detasks that selector. Unlike upstream collection, which is captured as it transits the backbone, downstream collection is retrieved at the beginning or end of its journey, i.e., from a service provider.[30] As of 2023, the vast majority of the Internet communications NSA acquired pursuant to Section 702 were obtained through downstream collection.[31]

---

[25] Off. of the Dir. of Nat'l Intel., *Release of Two FISC Decisions Authorizing Novel Intelligence Collection* (May 19, 2023), https://www.intel.gov/ic-on-the-record-database.

[26] *Release of Documents Related to the 2021 FISA Section 702 Certification and Title III Physical Search Opinions*, *supra*.

[27] The 2014 PCLOB Report grouped "telephony" under upstream, as the two programs are similar in many respects. Following current IC usage, this current report breaks telephony out into a separate type of collection, but this does not reflect any substantive changes in the operation of the program.

[28] Previously, such as in the 2014 PCLOB Report, this type of collection was referred to as PRISM.

[29] 2014 PCLOB Report, *supra*, at 33-34.

[30] NSA Classified Background Information on Upstream from 2014 to 2022, *supra*, at 1.

[31] Nat'l Sec. Agency, Email Response, PCLOB Questions and 702 resources (Dec. 22, 2022).

FBI receives all downstream raw collection from ECSPs.[32] FBI technical personnel process and review the collection only for technical and quality control purposes prior to sending it to other agencies.[33] Depending on which agency has requested collection on that target's selector, FBI sends the collection to CIA, NCTC, and/or sends the data for loading into FBI repositories.[34] NSA receives a copy of all downstream collection, even in cases where, for example, CIA is the only agency that requested collection pertaining to a selector.[35] Each agency must apply their own minimization procedures to any downstream-acquired data.

As noted above, in approving the FBI targeting procedures in 2018, the FISC considered whether certain types of collection could be considered "downstream abouts" collection in violation of the statutory prohibition on "abouts." The FISC concluded that the information did not constitute "abouts" collection and was authorized under the statute.[36]

The Board has reviewed further classified information regarding the technical details of downstream acquisition and discusses them in the Annex C to this Report.

III. Targeting Procedures

As discussed previously, under Section 702, the government targets non-U.S. persons located abroad by tasking selectors that the government assesses will be used by those persons to possess, communicate, or receive foreign intelligence that falls within one of the authorized Section 702 certifications.[37] The government uses targeting procedures to effectuate this process and ensure compliance with the applicable provisions of FISA and the Constitution. While the

[32] Email from Fed. Bureau of Investigation to Priv. and C.L. Oversight Bd. (Feb. 10, 2023).

[33] Off. of the Dir. of Nat'l Intel., Actions from IC Meetings with PCLOB Feb. 24, 2023, at 3-4 (Feb. 27, 2023). These activities include various normalization, processing, and compliance checks.

[34] 2016 Cert FISC Opinion and Order, *supra*, at 34. NCTC only receives raw collection from selectors tasked under the international counterterrorism certification. NCTC does not nominate or task selectors; instead, it requests to be dual routed on selectors that are nominated by other IC elements and tasked by NSA. U.S. DEP'T OF JUST., SEMIANNUAL REPORT OF THE ATTORNEY GENERAL CONCERNING ACQUISITIONS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, at 15 (Sept. 2021) [hereinafter 26th SAR].

[35] 2014 PCLOB Report, *supra*, at 34. This request must meet NSA's targeting procedures.

[36] Memorandum Opinion and Order, at 45, In re DNI/AG 702(h) Certifications 2018-A and Predecessor Certifications, Docket No. 702(j)-18-01 and predecessor dockets, In re DNI/AG 702(h) Certifications 2018-B and Predecessor Certifications, Docket No. 702(j)-18-02 and predecessor dockets, In re DNI/AG 702(h) Certifications 2018-C and Predecessor Certifications, Docket No. 702(j)-18-03 and predecessor dockets (FISA Ct. Oct. 18, 2018) [hereinafter 2018 Cert FISC Opinion and Order].

[37] *See, e.g.*, 26th SAR, *supra*, at A-2.

targeting procedures are subject to judicial review by the FISC, individual targeting determinations are subject to agency compliance mechanisms and oversight review by DOJ and ODNI.[38]

Only NSA and FBI are authorized to conduct acquisitions under Section 702 and thus are the only agencies that have targeting procedures.[39] Other agencies nominating targets for collection under Section 702 must provide information to NSA and FBI regarding those targets. When processing these nominations and their own nominations, NSA and FBI must comply with their respective targeting procedures. Neither NSA's nor FBI's targeting procedures have been declassified in full, but redacted versions are made public following certification each year.[40]

NSA reviews all nominations for Section 702 collection and applies its targeting procedures before making a targeting decision. FBI conducts an additional review of all targeting requests made to FBI as part of applying its targeting procedures.

A. Nominations

Only NSA, FBI, and CIA currently nominate targets and their associated selectors for collection under Section 702. However, FBI, CIA, and NCTC may all request unminimized dual-routed downstream collection.[41] Dual-routed collection is collection that any agency receives based on the nomination of another agency. Dual-routed collection may be valuable for joint investigations or when each agency has an independent intelligence-collecting interest in the same target.

Section 702 targeting steps begin when an analyst discovers or is informed of a foreign intelligence lead—specifically, information indicating that a particular person may possess, receive, or communicate the types of foreign intelligence information described within one of the Section 702 certifications.[42] Lead information may also provide insight into a target's physical location. Lead information could come from any number of sources, including human intelligence,

[38] In certain instances, targeting may be subject to additional judicial review in a criminal prosecution. There have been nine instances where a defendant has been given notice and six of those were litigated.

[39] *See* 2021 NSA Targeting Procedures, *supra*; Fed. Bureau of Investigation, Exhibit C, Procedures Used by the Federal Bureau of Investigation for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (2021) [hereinafter 2021 FBI Targeting Procedures].

[40] *See* Off. of the Dir. of Nat'l Intel., *IC on the Record Database*, https://www.intelligence.gov/ic-on-the-record-database (last visited July 31, 2023).

[41] Unminimized upstream collection is not available for dual-routing and may be accessed only by NSA.

[42] Nat'l Sec. Agency, NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, at 4 (2014), https://media.defense.gov/2021/Aug/18/2002833876/-1/-1/0/NSA_REPORT_ON_SECTION_702_PROGRAM.PDF [hereinafter NSA DCLPO Report].

signals intelligence, foreign partners, other law enforcement information, or other Section 702-acquired information. Because Section 702 acquisition is selector-based, the analyst must discover or be informed of one or more specific selectors used by the target that could be tasked for collection.

When appropriate, the nominating agency uses available information to develop additional targeting information, including information to support a reasonable belief that the proposed target is a non-U.S. person located outside the United States. Using this original nominating information, NSA will run checks against its available databases to search for corroborating or contrary information. This process helps ensure the nomination is appropriate for targeting under Section 702.[43]

B. Foreignness Determination

To target under Section 702, both the nominating agency and the targeting agency must assess that all known users of the selector are non-U.S. persons reasonably believed to be located outside the United States. This is referred to as a foreignness determination.

In making this foreignness determination, the government considers that the NSA targeting procedures implicitly impose a requirement that the analyst conduct "due diligence" in identifying relevant information. What constitutes due diligence will vary depending on the target and the known facts. For example, NSA may use existing knowledge of current location and non-U.S. person status to add a new selector belonging to a known target. On the other hand, more research may be required to task a selector belonging to a previously unknown target.[44]

In assessing the location of a target, the analyst may examine lead information, information retained in agency databases, and information available to the agency through other sources (e.g., intelligence reporting or source reporting).

In the absence of definitive location or nationality information, the analyst will apply a set of presumptions based on available information to assess whether there is a reasonable belief that the person is a non-U.S. person, located outside the United States.[45]

However, if there is any information giving rise to a reasonable belief that the target is located in the United States or is a U.S. person, NSA must resolve that information before targeting that person under Section 702. For example, if there is evidence that a target traveled to the U.S. recently, in order to submit the target's selector for collection, the analyst is required to obtain

[43] Accuracy checks and deconfliction are terms used by the government. Accuracy confirms the information is correct based on information available to the government. Deconfliction confirms that no other information exists to invalidate a presumption. FED. BUREAU OF INVESTIGATION, FOREIGN INTELLIGENCE SURVEILLANCE ACT AND STANDARD MINIMIZATION PROCEDURES POLICY GUIDE, at 314-17 (2021) [hereinafter SMP PG].

[44] *See* 2021 NSA Targeting Procedures, *supra*.

[45] 2021 NSA Targeting Procedures, *supra*, at 4.

additional information demonstrating that the target in fact left the country. Failure to conduct sufficient due diligence is considered a targeting compliance incident that must be reported to the FISC. The government has asserted that all identified compliance incidents have been reported to the FISC.

After conducting due diligence and reviewing the available information, the analyst is required to determine, based on the totality of the circumstances, whether the target is a non-U.S. person reasonably believed to be located outside the United States.[46]

C. Foreign Intelligence Purpose Determination

In addition to the foreignness determination, the analyst must also make a particularized and fact-based foreign intelligence purpose determination. Specifically, the targeting procedures require the analyst to "reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or authorization executed by the Director of National Intelligence and the Attorney General."[47] Additionally, the analyst must assess that each tasked selector is reasonably likely to be used to communicate foreign intelligence information.[48] The analyst considers the circumstances that led to the identification of the intended target and associated selector(s), along with more particularized factual information such as contacts or association with a foreign power or territory.[49]

Section 702 prohibits "reverse targeting," i.e., targeting a non-U.S. person outside the United States "if the purpose of such acquisition is to target a particular, known person reasonably believed to be located in the United States."[50] Agencies must determine whether the Section 702 target is of interest or whether the purpose of targeting that individual is in fact to obtain information on another individual who may not be lawfully targeted. While conducting oversight over targeting, minimization, querying, and post-targeting review, oversight entities look for indications of potential reverse targeting.

[46] *See* PCLOB March 2014 Hearing Transcript, *supra*, at 40-42 (statement of Rajesh De, Gen. Couns., Nat'l Sec. Agency).

[47] 2021 NSA Targeting Procedures, *supra*, at 4.

[48] If, after initial tasking, an analyst determines that a particular selector is not likely to produce foreign intelligence information, it must be detasked. NSA DCLPO Report, *supra*, at 6.

[49] 2021 NSA Targeting Procedures, *supra*, at 4-5.

[50] 50 U.S.C. § 1881a(b)(2).

D. Documentation Requirements

Under NSA's targeting procedures, analysts must document the facts and circumstances giving rise to the foreignness and foreign intelligence purpose determinations.[51] Analysts must cite specific documents and communications that led them to assess that the Section 702 target is located outside the United States.[52] Citations must facilitate independent review and oversight of the targeting decision and identify the foreign power or foreign territory about which they expect to obtain foreign intelligence.[53] With regard to the foreign intelligence purpose, analysts must provide a written explanation of the basis of that determination sufficient to demonstrate that the targeting of each target is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISC.[54]

E. Approvals

Once analysts have documented their determinations and submitted their nomination, the nomination must be reviewed by the relevant NSA targeting office.[55] The tasking request undergoes two layers of review at NSA before tasking and acquisition is initiated. Two different senior NSA analysts must review the documentation accompanying the tasking request to ensure it meets the requirements of the targeting procedures. Either senior analyst may request additional information prior to approving or denying the tasking request. Once the tasking request receives all of the necessary approvals, it is sent by NSA or FBI to one or more ECSPs that have received a Section 702 directive in order to initiate Section 702 acquisition.

F. FBI Targeting and Technical Assistance

Once NSA determines that a Designated Account satisfies NSA's targeting procedures and tasks it, FBI applies its own targeting procedures to the Designated Account and conducts additional review.[56] NSA provides FBI with identifying information and certain targeting data on

[51] 2021 NSA Targeting Procedures, *supra*, at 9.

[52] *Id.*

[53] *Id.*.

[54] *Id.* Subsequent to the publication of the 2014 PCLOB Report, which included a recommendation to document this written explanation, NSA revised its targeting procedures to reflect the requirement discussed above. NSA did not implement the full recommendation, which also called for NSA to specify the "criteria for determining the expected foreign intelligence value of a particular target." *See* 2014 PCLOB Report, *supra*, at 11; *see also* PRIV. AND C.L. OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT, at 11 (2022), https://documents.pclob.gov/prod/Documents/OversightReport/c29f61be-88e1-47bf-bc76-3d39215a5ceb/2022%20Recommendations%20Assessment%20Report.pdf.

[55] 2021 NSA Targeting Procedures, *supra*, at 9.

[56] NSA, OVSC1203: FISA Section 702 Training, *supra*, at 17.

the Designated Accounts and FBI runs checks to ensure it has no information to contradict or undermine the reasonable belief that the target is a non-U.S. person, located outside the United States.[57] Since the beginning of the Section 702 program in 2008, following these additional checks, FBI has rejected 0.07% of the Designated Account requests.[58] If FBI identifies any such information, it coordinates with NSA to deconflict and, if appropriate, NSA detasks the selector.

In the event of an immediate threat to human life or property, FBI may initially rely on NSA's targeting assessment and information without first reviewing and evaluating the sufficiency of either.[59] If FBI relies on this emergency provision, it must satisfy its normal targeting obligations at the first available opportunity, but no later than the next business day after the request is approved.[60]

If FBI receives any indication that the target could be a U.S. person or was/is located inside the United States, it must select one of the following courses of action. It could reject the Designated Account if the information indicates the target is not eligible for Section 702 targeting.[61] It could also return the request to the nominating agency to provide information to rebut the potentially disqualifying information.[62]

If, after requesting that FBI approve a targeting request for a Designated Account, NSA discovers that any user of the Designated Account is a U.S. person or a person located inside the United States, NSA must notify FBI, DOJ, and ODNI. NSA must take steps to detask the account without delay.[63] Likewise, if FBI discovers that any user is a U.S. person or a person located inside the United States, FBI must reject the targeting request and NSA must take steps to detask the account without delay and purge any unauthorized collection. NSA will then notify DOJ and ODNI. Discovery and notification may occur any time after NSA submits a request.

G. Post-Tasking Review

In addition to defining the process by which Section 702 tasking is initiated, the NSA targeting procedures also impose a duty to conduct ongoing review of the targets and their

[57] 2021 FBI Targeting Procedures, *supra*, at 1.

[58] Actions from IC Meetings with PCLOB Feb. 24, 2023, *supra*, at 3-4.

[59] 2021 FBI Targeting Procedures, *supra*, at 5.

[60] As of the time of this Report, FBI has never used this emergency provision. Response from Fed. Bureau of Investigation to Priv. and C.L. Oversight Bd. Staff (Feb. 6, 2023).

[61] 2021 FBI Targeting Procedures, *supra*, at 6.

[62] *Id.* at 6-7.

[63] *Id.*

associated collection. This review is designed to ensure that users of tasked selectors continue to meet the requirements for collection under Section 702.[64] Specifically, that the targets remain non-U.S. persons, located outside the United States, that they continue to be of interest from a foreign intelligence perspective, that the tasked selectors are still expected to be or in fact are used to communicate or receive foreign intelligence, and that the foreign intelligence is within the scope of an authorized Section 702 certification.

This ongoing review of the targets and their associated collection must be conducted by NSA or any dual routed agency assuming primary review responsibility.[65] First, the agencies must determine whether any new information has come to light that calls into question the original determination that the individual could be targeted under Section 702.[66] Second, the agencies evaluate whether the status of the individual has changed such that the individual is now a U.S. person or is now located in the United States.[67] Third, the agencies evaluate whether the individual continues to be a valid foreign intelligence target, i.e., is expected to receive, communicate, or possess foreign intelligence within the approved category identified for collection.[68] Fourth, while the individual may continue to be a valid target, information may have come to light indicating that the target's selector is no longer appropriate for collection. In other words, even if the target is appropriate, not all of the target's selectors or communications accounts may be used to communicate foreign intelligence. Additionally, the selector might have multiple users, one or more of which could be ineligible for targeting.[69]

If NSA cannot resolve an apparent conflict between information concerning the U.S. location of the target, NSA must presume that the target is located in the United States and terminate collection.[70] In general, all nominating agencies must conduct an initial review of

[64] 2021 NSA Targeting Procedures, *supra*, at 6-7.

[65] *Id.* at 3-4.

[66] *Id.* at 6-8.

[67] *Id.* at 8.

[68] *See id.* In addition to removing targeting for reasons related to the Targeting Procedures, the agencies might determine that the individual is a low priority target and resources are better spent elsewhere. If any agency receiving collection determines that it no longer wishes to receive that collection, the dual route to that agency will be terminated.

[69] Detasking or termination of dual-routing is not limited to instances when a target is no longer eligible for targeting under Section 702; they may occur as a matter of discretion. Agencies may detask a selector because they determine that the individual is a low priority target and resources are better spent elsewhere. In addition, if any agency receiving collection for an eligible target determines that it no longer wishes to receive that collection, the dual route to that agency will be terminated.

[70] The obligation to review is heightened in cases where NSA would be unable to detect whether the tasked selector is being used from the United States.

tasking within five business days of its first receipt of collection and at least every thirty business days thereafter.[71]

If any agency receiving Section 702 collection determines that a target no longer meets the criteria for targeting, NSA must detask the selectors associated with the target. If NSA receives collection from a target that no longer meets the criteria for collection under Section 702 because a user is a U.S. person or a user is inside the United States, that information must be reported to DOJ (and any resulting compliance incidents must be reported to the FISC) and the collection generally must be purged.[72]

Section 702 certifications are valid for one year and the nominating agency must affirmatively decide if each individual selector will remain tasked over time, to include under each successor certification. The nominating agency and the tasking agency evaluate whether the target and the associated selectors remain eligible for targeting under Section 702 and whether they continue to retain foreign intelligence value within the scope of an authorized Section 702 certification. All nominations must continue to comply with NSA's targeting procedures and must be updated as needed to conform to the new certifications. In addition, both NSA's ongoing post-targeting analysis requirement and internal policy requiring revalidation for selectors that remain tasked beyond one year function as additional controls.

IV. Minimization Procedures and Related Requirements

The 2014 PCLOB Report described minimization as "one of the most confusing terms in FISA."[73] The Board's previous report attempted to clarify the confusion and introduced generally the concept of minimization, how minimization occurs at NSA, and the three aspects of minimization (i.e., acquisition, retention, and dissemination).[74] Since the 2014 PCLOB Report, more minimization procedures have been released to the public and an additional agency, NCTC,

[71] 2021 NSA Targeting Procedures, *supra*, at 8.

[72] 2021 NSA Minimization Procedures, *supra*, at 11. In certain limited circumstances, if the information is of significant importance to national security, the Director of the NSA may grant a waiver permitting NSA to maintain the collection so long as it was not the result of a compliance incident. Between January 2020 and December 2022, the Director of the NSA, in consultation with DOJ and ODNI, granted six destruction waivers applicable to twenty-two Section 702-acquired communications. CIA has submitted two destruction waiver requests: one in 2012 and one in 2014. NCTC has made no such requests.

[73] 2014 PCLOB Report, *supra*, at 50.

[74] *Id.* at 50-66.

has begun receiving unminimized Section 702-acquired information and accordingly now has minimization procedures covering such information.[75]

Section 702 requires that agencies adopt minimization procedures designed to reduce the privacy and civil liberties impact of the acquisition, retention, and dissemination of incidentally collected U.S. person information.[76] Section 702 does not contain its own definition of what constitutes sufficient minimization procedures but instead directs that Section 702 minimization procedures must follow the standard applicable to either Title I or Title III, as appropriate. Thus, the procedures must contain certain provisions, three of which are most relevant to Section 702. Specifically, the procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[77] Further, the procedures require that non-publicly available information that is not foreign intelligence information shall not be disseminated in a manner that identifies any U.S. person without that person's consent, unless the identity is necessary to understand such foreign intelligence information or assess its importance.[78] The definition of minimization procedures also states that, notwithstanding these requirements, the procedures must allow for the retention and dissemination of U.S. person information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.[79]

---

[75] NCTC was first approved to access unminimized information acquired by NSA and FBI under Section 702 on April 26, 2017. On April 26, 2017, the FISC also approved NCTC's first minimization procedures covering unminimized Section 702-acquired information. *See* 2016 Cert FISC Opinion and Order, *supra*, at 30.

Previously, in 2012, the FISC approved NCTC Section 702 minimization procedures covering NCTC's access to minimized Section 702-acquired information in FBI general indices. *See* Memorandum Opinion, at 25, *In re DNI/AG 702(g) Certification 2009-C, In re DNI/AG 702(g) Certification 2010-C, In re DNI/AG 702(g) Certification 2011-C, In re DNI/AG 702(g) Certification 2012-C,* Docket No. 702(i)-12-01, *In re DNI/AG 702(g) Certification 2008-A, In re DNI/AG 702(g) Certification 2009-A, In re DNI/AG 702(g) Certification 2010-A, In re DNI/AG 702(g) Certification 2011-A, In re DNI/AG 702(g) Certification 2012-A*, Docket No. 702(i)-12-02, *In re DNI/AG 702(g) Certification 2008-B, In re DNI/AG 702(g) Certification 2009-B, In re DNI/AG 702(g) Certification 2010-B, In re DNI/AG 702(g) Certification 2011-B, In re DNI/AG 702(g) Certification 2012-B*, Docket No. 702(i)-12-03 (FISA Ct. Sept. 20, 2012).

[76] 50 U.S.C. § 1801(h). While the procedures are designed to protect U.S. person information, the implementation of certain provisions provides collateral protections for non-U.S. persons.

[77] *Id.* § 1801(h)(1); *see also id.* § 1821(4), which uses identical language except "the particular physical search" instead of "the particular surveillance."

[78] *Id.* § 1821(4)(B).

[79] *Id.* § 1821(4)(C).

The minimization procedures adopted by each agency with access to unminimized Section 702 collection, both content and non-content (including metadata), must be approved by the FISC.[80] Under Section 702, unminimized collection is the raw data received from providers that has not yet been determined to meet the standards for retention— i.e., that has not been determined to be (i) foreign intelligence information, (ii) necessary to understand foreign intelligence information or to assess its importance, or (iii) evidence of a crime.

As previously noted, four agencies currently receive unminimized[81] Section 702 collection, namely NSA, CIA, FBI, and, since 2017, NCTC.[82] Although there are similarities across agency minimization procedures, each set of procedures also reflects differences in agency authorities, missions, systems, internal processes, and policies.[83] These procedures are reviewed annually by the FISC as part of the Section 702 certification package to ensure both the language of the procedures and agency implementation of the procedures continue to meet the standards set by FISA.[84] Specifically, as noted above, minimization procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[85]

[80] *Id.* § 1805.

[81] For example, NCTC Minimization Procedures define "raw" information as "section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance." NAT'L COUNTERTERRORISM CTR., EXHIBIT G, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 2 (2021) [hereinafter 2021 NCTC Minimization Procedures].

[82] Off. of the Dir. of Nat'l Intel., *NCTC Foreign Intelligence Surveillance Act Section 702* (2017), https://www.dni.gov/files/NCTC/documents/news_documents/MDAFISA-702_Fact-Sheet.pdf. In 2016, the government requested and, in 2017, the FISC permitted NCTC to receive certain unevaluated counterterrorism information acquired pursuant to Section 702. The government asserted that access was necessary because of "NCTC's role as the government's "primary organization for analyzing and integrating all intelligence pertaining to international terrorism and counterterrorism." As mentioned previously, the FISC noted that the limited scope of the raw information NCTC receives is consistent with NCTC's mission. 2016 Cert FISC Opinion and Order, *supra*, at 31, 34.

[83] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 19.

[84] 50 U.S.C. § 1881a(j)(1)(A).

[85] *Id.* § 1801(h).

A. Minimization at the Acquisition Stage[86]

NSA's minimization procedures begin with a requirement that Section 702 collection be conducted in accordance with the Section 702 certification and "in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition."[87] The government informs the FISC regarding how NSA and FBI actually conduct the acquisition to comply with this requirement. This is done through affidavits submitted to the FISC and may include witness testimony in hearings before the FISC as part of the certification process, along with periodic filings.[88] These representations detail the method and techniques by which the collection is conducted, as described above. A failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the Section 702 certifications can, and has, led to incidents of noncompliance with the targeting and/or minimization procedures that have been reported to the FISC and Congress.[89]

In addition to actually acquiring the data, the agencies employ certain technical actions in order to facilitate later compliance with minimization rules. Agencies employ methods such as data-tagging[90] and logical or physical separation to identify Section 702-acquired data at, or just after, acquisition to effectuate other access and routing controls, certain controls limiting the scope of queries, and age-off and purge requirements.[91]

B. Access and Training

Each agency with access to raw or unminimized Section 702 collection limits access to such data to personnel who have been trained to apply their respective agency's minimization procedures.[92] To enforce these restrictions, all unminimized Section 702-acquired data is stored

[86] While it is noted that certain aspects of minimization occur at the "acquisition" stage, minimization occurs at the initial filtering, acquisition, and analysis of Section 702 data.

[87] *See* 2021 NSA Minimization Procedures, *supra*, at 3 (defining "acquisition" as "the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party").

[88] *See*, *e.g.*, Affidavit of the Director of the National Security Agency, at 2, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Mar. 18, 2022) [hereinafter FISC 2021 DIRNSA Aff.].

[89] *See* U.S. DEP'T OF JUST., SEMIANNUAL REPORT OF THE ATTORNEY GENERAL CONCERNING ACQUISITIONS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Mar. 2022) [hereinafter 27th AG SAR].

[90] Data-tagging means labeling Section 702-acquired information as deriving from Section 702, so that when an analyst reviews the collection, the analyst knows to apply Section 702 procedures; it is a compliance control.

[91] Fed. Bureau of Investigation, Exhibit D, Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 15-16 (2021) [hereinafter 2021 FBI Minimization Procedures].

[92] *See*, *e.g.*, 2021 NSA Targeting Procedures, *supra*, at 9-10; 2021 NSA Minimization Procedures, *supra*, at 2-3.

in repositories with access controls designed to prevent unauthorized access of the data by those within or outside of the relevant agency.[93]

While all agencies require system users to have a mission need and undergo mandatory Section 702 training prior to being granted access to Section 702 datasets, agencies employ different training methods and post-training resources and refreshers. For example, NSA analysts complete a virtual training course and are required to pass a test at the conclusion of their training prior to receiving access to unminimized Section 702-acquired data.[94] NSA, FBI, and NCTC require that all personnel refresh their training on an annual basis in order retain their access.[95] CIA's training includes live and web-based training modules involving handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process.[96] FBI agents and analysts complete virtual (and sometimes in-person) training and, when DOJ has conducted on-site field office reviews, receive trainings from DOJ.[97]

Although updates to training do not occur at regular intervals at FBI, CIA, and NCTC, updates to policies and guidelines are disseminated to users as issued by DOJ and ODNI, or as updated by agency personnel.[98] Focused trainings may also be issued in response to compliance incidents. For example, in response to FISC concerns over repeated FBI query compliance incidents, FBI worked with DOJ and ODNI in 2021 and 2022 to update and expand Section 702 query-specific training.[99]

Each agency maintains different levels of legal support as resources. For example, each agency designates FISA-trained attorneys who may answer legal questions related to technical,

[93] *See generally* NSA, OVSC1203: FISA Section 702 Training, *supra*; NSA DCLPO Report, *supra*, at 4.

[94] *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 11 (2023) (joint statement of Chris Fonzone, Gen. Couns., Off. of the Dir. of Nat'l Intel., et al.) [hereinafter June 2023 Joint Statement to Senate Judiciary]; NSA, OVSC1203: FISA Section 702 Training, *supra*; Response from Nat'l Counterterrorism Ctr. to Priv. and C.L. Oversight Bd. (Sept. 9, 2022); NSA DCLPO Report, *supra*, at 4.

[95] *E.g.*, Nat'l Counterterrorism Ctr., NCTC Raw FBI (RTM) and Section 702 FISA Annual Refresher Course (Sept. 2, 2022); NSA DCLPO Report, *supra*, at 4.

[96] U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 01 June 2020—30 November 2020, at 16 (Apr. 2022) [hereinafter 25th Joint Assessment]; NSA, OVSC1203: FISA Section 702 Training, *supra*. CIA will be requiring annual refresher trainings beginning in 2023.

[97] Briefing, Fed. Bureau of Investigation Briefing for Priv. and C.L. Oversight Bd. Staff (July 29, 2022).

[98] For example, although NSA's annual training was last updated in 2022, NSA also continuously provides informal and ad hoc training and compliance notices/mandates.

[99] *E.g.*, Fed. Bureau of Investigation, FISA Query Training (Dec. 2021) [hereinafter FBI FISA Query Training].

policy, or operational aspects of the program. These attorneys frequently communicate directly with DOJ and/or ODNI to obtain additional guidance and report compliance incidents.[100] Depending on agency practices, these attorneys also provide review and oversight of certain uses of Section 702-acquired information, as discussed throughout this Report.[101]

When an analyst, agent, or officer is granted access to unminimized Section 702-acquired data after receiving the requisite training, this does not mean that the analyst, agent, or officer has access to all such data. Agencies may further tag or segregate data as a security measure. Furthermore, FBI, CIA, and NCTC receive only downstream collection for Section 702 targets that they nominate or for which they request dual routing. FBI receives collection for only those targets who are relevant to a pending, full national security investigation, which was approximately 3.2% of total targets in 2022.[102] NSA does not route other types of unminimized collection to any other agency.[103]

C. Retention and Purging

The Section 702 minimization procedures include provisions designating when data may be retained, what data must be purged (i.e., destroyed or deleted) upon recognition, when data must be "aged off" agency systems (i.e., deleted at the end of its retention period), and what types of evaluated information may be retained indefinitely, subject to any other retention periods that may be specified by law.[104] Unless a specific exception applies, such as a preservation obligation in connection with a litigation matter, Section 702 collection is generally not authorized for indefinite retention if it (a) has not been reviewed, (b) has been reviewed and has not been affirmatively determined to contain foreign intelligence information, (c) is not necessary to understand foreign intelligence or assess its importance, or (d) is not evidence of a crime. Further, NSA's minimization procedures specifically require that Section 702 collection that has been reviewed and has been affirmatively identified as not meeting one of these categories for retention must be destroyed upon recognition. While FBI, CIA, and NCTC's[105] minimization procedures include

[100] 25th Joint Assessment, *supra*, at 16.

[101] *Id.* at A-11.

[102] Off. of the Dir. Of Nat'l Intel, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authoritites, Calendar Year 2022, at 18, 22 (Apr. 2023) [hereinafter CY2022 ASTR]; *see* SMP PG, *supra*, at 314.

[103] CY2022 ASTR, *supra*, at 28-29.

[104] 50 U.S.C. § 1801(h)(1).

[105] *E.g.*, 2021 NCTC Minimization Procedures, *supra*, at 6-7, 9 (requiring that any communications "that contain a reference to, but are not to or from, a person targeted in accordance with section 702 targeting procedures . . . . will be destroyed upon recognition"; requiring that information acquired through targeting of person who was a U.S. person or located in the United States at the time of collection "will be promptly destroyed upon recognition"; and

purge requirements for specific categories of information, NSA's minimization procedures are the only ones that contain a general purge requirement that applies regardless of the type of information. However, as a practical matter, individual agents and analysts at all four agencies do not affirmatively purge communications upon review if not immediately recognized as containing foreign intelligence information because they maintain that communications that initially do not appear to contain foreign intelligence or evidence of a crime may have foreign intelligence value in the future or for another concurrent investigation.[106] Anecdotal evidence suggests that communications are rarely purged before their designated age-off date. Further, agencies can seek retention extensions to prolong the lifecycle of certain data.[107]

The retention period for Section 702 data is specified in each agency's minimization procedures… [which] dictate whether data must be purged as soon as practicable, or may be retained for 5 years, 15 years, or indefinitely…

The retention period for Section 702 data is specified in each agency's minimization procedures.[108] The particular retention limits that apply are dependent on the type of data contained in the communication (e.g., foreign intelligence information or evidence of a crime) and the circumstances under which the communication was obtained (e.g., information lawfully collected or information associated with a compliance incident). These variations, including whether or not the information has been reviewed, dictate whether data must be purged as soon as practicable, or may be retained for 5 years, 15 years, or indefinitely in accordance with the specific agencies' procedures.

requiring that an attorney-client communication that "does not contain foreign intelligence information or evidence of a crime . . . must be destroyed").

[106] *See, e.g.*, 2021 NSA Minimization Procedures, *supra*, at 5 ("Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy information of or concerning a United States person at the earliest practicable point at which such information can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures."). In addition, Section 4(c) requires destruction upon recognition for information that is known to contain U.S. person information and does not meet the retention standards set forth in the procedures.

[107] *See* 2021 NSA Minimization Procedures, *supra*, at 6-8; 2021 NCTC Minimization Procedures, *supra*, at 5-6; 2021 FBI Minimization Procedures, *supra*, at 25; 2021 CIA Minimization Procedures, *supra*, at 2; *see also* 2014 PCLOB Report, *supra*, at 7, 62.

[108] *See* 2021 NSA Minimization Procedures, *supra*; 2021 NCTC Minimization Procedures, *supra*; 2021 FBI Minimization Procedures, *supra*; 2021 CIA Minimization Procedures, *supra*.

1. *Retention Schedules*

Retention schedules vary based on several factors, including: (a) whether the communication has been reviewed or evaluated; (b) whether agents or analysts have identified any U.S. person information in the communication; (c) whether the communication contains foreign intelligence information or evidence of a crime; and (d) whether the communication contains domestic communications or attorney-client privileged material. Retention of communications is laid out in the agency minimization procedures, but such retention may be further restricted pursuant to executive branch direction and agency policy (e.g., PPD-28 and E.O. 14086).

- Raw Section 702-acquired data that has not been reviewed must be aged off the NSA, FBI, CIA, and NCTC systems no later than five years after the expiration of the Section 702 certification under which that data was acquired.[109]
- The FBI and NCTC minimization procedures permit the retention of data that has been reviewed but not yet determined to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime for ten years. After ten years, the data is placed in restricted status for an additional five years.[110]
- Section 702-acquired data that has been evaluated and determined to contain either no U.S. person information or U.S. person information that is foreign intelligence information or evidence of a crime may generally be retained indefinitely under the minimization procedures.[111] As noted above, however, agency policies, including E.O 14086, further restrict retention.

Each set of minimization procedures contains certain exceptions to each of the rules discussed above. For example, pursuant to FBI and NSA's minimization procedures, encrypted communications or communications that "contain secret meaning" may be retained for "a

[109] *See* 2021 NSA Minimization Procedures, *supra,* at 6-8; 2021 NCTC Minimization Procedures, *supra,* at 5-6; 2021 CIA Minimization Procedures, *supra,* at 2; 2021 FBI Minimization Procedures, *supra,* at 25. Prior to the 2017 suspension of "abouts" collection, NSA's unminimized upstream collection was required to age off NSA systems no later than two years after the expiration of the Section 702 certification under which the data was acquired.

[110] (U) 2021 NCTC Minimization Procedures, *supra,* at 6; 2021 FBI Minimization Procedures, *supra,* at 17. During this restricted status, users receive notice of the existence of the data if it is responsive to a query but must seek executive-level approval to access it.

[111] 2021 NSA Minimization Procedures, *supra*; 2021 NCTC Minimization Procedures, *supra*; 2021 FBI Minimization Procedures, *supra*; 2021 CIA Minimization Procedures, *supra*. In addition, NCTC may only retain and disseminate evidence of a crime that is not foreign intelligence information for law enforcement purposes, such as by disseminating it to FBI. *See* 2021 NCTC Minimization Procedures, *supra,* at 6.

sufficient period to permit exploitation," or decryption.[112] In addition, FBI must retain information that does not otherwise meet the standard for retention if the information has been reviewed and reasonably appears to be exculpatory or impeachment material for a criminal proceeding.[113] There are also exceptions for information subject to litigation holds.[114] Further, FBI may indefinitely retain emergency backup or original evidence copies of information, provided that only system administrators or other technical personnel have access to such information.[115]

2. *Purge Requirements*

As noted above, NSA's minimization procedures are the only procedures that contain a general purge requirement that applies regardless of the type of information at issue.[116] As a practical matter, all four agencies typically rely on age-off requirements. The agencies have not sought to implement a purge-upon-recognition requirement in part because they maintain that a single agent or analyst cannot definitively determine whether a communication does not contain foreign intelligence or evidence of a crime. The agencies state that communications that initially do not appear to contain foreign intelligence or evidence of a crime may have foreign intelligence value based on other intelligence or information that the agent or analyst is not aware of, or for another concurrent investigation or future value.

There are a number of instances that trigger other purge requirements, including when the agency has identified communications it is not permitted to retain. For example, when a non-U.S. person located abroad travels to the United States, the government must terminate collection without delay and any collection received during the time when the target was located in the United States must generally be purged.[117] New information indicating a target should have been or subsequently will be treated as a U.S. person may also trigger a purge requirement, in addition to the associated selectors being detasked. Finally, collection otherwise received pursuant to an improper or insufficient tasking or other compliance incident must also be

[112] (U) 2021 NSA Minimization Procedures, *supra,* at 13 ("A sufficient duration may consist of any period of time during which the encrypted information is subject to, or of use in, cryptanalysis or deciphering secret meaning. Once information is decrypted or deciphered, the retention period, if applicable for such information, is five years from the date of decryption or decipher."); 2021 FBI Minimization Procedures, *supra,* at 40.

[113] 2021 FBI Minimization Procedures, *supra,* at 13.

[114] Id. at 39-40.

[115] *Id.* at 38-39. FBI's minimization procedures require that no such intelligence analysis may be performed on such data, nor may it be accessed for performing intelligence analysis, and in the event such backup copies are needed to restore lost data, or to provide an original evidence copy, the otherwise applicable retention limits will apply.

[116] 2021 NSA Minimization Procedures, *supra,* at 6-8.

[117] *E.g.*, *id.* at 8; 2021 NCTC Minimization Procedures, *supra,* at 6-7.

purged.[118]

Separately, pursuant to NSA's March 17, 2017 suspension of upstream "abouts" collection, NSA proposed to sequester and destroy upstream collection acquired on or prior to that date, with notable exceptions.[119] This proposal was subsequently memorialized in NSA's FISC-approved minimization procedures.[120] Further, any future communication acquired that is not to or from a person targeted for collection under Section 702 must be destroyed upon recognition.[121]

NSA, FBI, CIA, and NCTC have created systems and processes to track the purging of information from their systems. The agencies also must coordinate such purges with other agencies to ensure that disseminations based on that collection or dual-routed collection is also purged. FBI, CIA, and NCTC receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that FBI, CIA, and NCTC can meet their respective obligations and conduct similar purges.[122] For each incident requiring a purge, NSA also has a process to identify and, as appropriate, revise or recall reporting based on collection subject to purge.[123] FBI, CIA, and NCTC have similar processes.[124]

---

[118] *E.g.*, 2021 NSA Minimization Procedures, *supra*, at 8.

[119] Any upstream communications acquired on or before that date that were mistakenly retained following that destruction must be purged upon recognition. In a 2017 filing, NSA notified the FISC that it would retain Section 702 upstream collection in the following categories: (a) in Serialized Reporting and "evaluated minimized traffic" disseminations; (b) completed transcriptsand transcriptions of Internet transactions; and (c) information used in Section 702 taskings and FISA applications. The FISC approved this approach in an April 26, 2017 order. 2016 Cert FISC Opinion and Order, *supra*. In this context, "evaluated minimized traffic" was Section 702-acquired information that NSA determined was both (a) foreign intelligence information, and (b) included no unmasked U.S. person information. Litigation hold information was not included in the categories of Section 702 upstream collection NSA would be retaining because the NSA minimization procedures broadly allow for the retention of Section 702-acquired information that is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. 2021 NSA Minimization Procedures, *supra*, at 5.

[120] Any upstream communications acquired on or before that date that were mistakenly retained following that destruction must be purged upon recognition. *Id.* at 6.

[121] *Id.*

[122] *See* U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, at 7-9 (Sept. 2022) [hereinafter 28th SAR] (describing the respective purge processes of FBI, CIA, and NCTC).

[123] 25th Joint Assessment, *supra*, at 6.

[124] U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 01 December 2020—31 May 2021, at A-14 (Aug. 2022) [hereinafter 26th Joint Assessment].

D. Use and Dissemination

Agency minimization procedures and practices impose additional restrictions on the use and dissemination of Section 702-acquired data. "Dissemination" of FISA-acquired information generally refers to the reporting of acquired information outside of the agency.[125] This may include disseminating reports throughout the Intelligence Community and, as appropriate, to other federal agencies, and foreign, state, local, and tribal partners. Consistent with the overall goal of minimization, dissemination rules impose a layer of protection for non-publicly available information of or concerning an unconsenting U.S. person.[126] In general, non-publicly available information that identifies an unconsenting U.S. person may be included in a disseminated intelligence report only if it is foreign intelligence information or is necessary to understand the foreign intelligence information.[127] Such disseminations are also permissible if they contain evidence of a crime and are being disseminated for law enforcement purposes.[128] A disseminated intelligence report may only contain U.S. person identifiers that meet the standard above; if they do not meet the standard, agency minimization procedures require the substitution of a generic phrase or term, such as "U.S. person 1" or "named U.S. person."[129] This substitution is often referred to as "masking."

NSA's minimization procedures permit NSA to disseminate U.S. person information if NSA masks any information that could identify the U.S. person.[130] As a matter of practice and policy, NSA typically initially masks all information that could identify a U.S. person in its reports.[131] Recipients of NSA reports, such as other federal agencies, may then request that the

[125] For FBI, the term "dissemination" also includes the internal sharing of acquired information with FBI personnel who do not have access to unminimized FISA collection. FBI personnel, therefore, are only permitted to upload FISA collection to the FBI's internal case management system after applying the minimization procedures to that collection.

[126] Dissemination of Section 702-acquired information that does not contain U.S. person information is governed by other laws, regulations, and policies (such as Executive Order 12333, Executive Order 14086, and related implementing regulations), as well as by certain provisions of Section 702 minimization procedures.

[127] 2021 NCTC Minimization Procedures, *supra*, at 11.

[128] 2021 NSA Minimization Procedures, *supra*, at 13-15; *id.*; 2021 FBI Minimization Procedures, *supra*, at 41-47; 2021 CIA Minimization Procedures, *supra*, at 4-5.

[129] 2021 NSA Minimization Procedures, *supra*, at 13-15; 2021 NCTC Minimization Procedures, *supra*, at 11; 2021 FBI Minimization Procedures, *supra*, at 41-47; 2021 CIA Minimization Procedures, *supra*, at 4, 9.

[130] 2021 NSA Minimization Procedures, *supra*, at 13-15.

[131] Off. of the Dir. of Nat'l Intel, Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act, at 7-8 (2017), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/CLPT-USP-Dissemination-Paper-FINAL-clean-111717_OCR.pdf.

U.S. person identity be unmasked.[132] NSA approves requests if the user has a "need to know" and disseminating the U.S. person identity would be consistent with NSA's minimization procedures.[133] Requesters must include a justification for access to the U.S. person information, and that justification should fall within the categories provided in the minimization procedures.[134] As a matter of NSA policy, there are no more than twenty individuals serving in twelve positions across NSA who possess the authority to approve requests for unmasking identity release.[135]

NSA may disseminate a U.S. person's identity for one of a specific list of reasons, including that the U.S. person has consented to the dissemination, the information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities.[136] In 2020, in 3,627 disseminated intelligence reports, NSA included 9,354 unmasked U.S. person identities.[137]

CIA's minimization procedures permit CIA to disseminate U.S. person information if information that identifies the U.S. person is masked in the dissemination.[138] However, CIA may disseminate U.S. person information in a manner that identifies the U.S. person if that person's identity is necessary to understand foreign intelligence information or (if concerning an attack by a foreign power, sabotage by a foreign power, international terrorism, international proliferation of weapons of mass destruction by a foreign power, or clandestine intelligence activities by a

[132] 2021 NSA Minimization Procedures, *supra*, at 13-15; Nat'l Sec. Agency, Off. of C.L. and Priv., Review of U.S. Person Privacy Protections in the Production and Dissemination of Serialized Intelligence Reports Derived from Signals Intelligence Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act, at 8 (2017), https://media.defense.gov/2021/Aug/18/2002833866/-1/-1/0/20171011-NSA-CLPO-DISSEMINATION-REPORT.PDF [hereinafter 2017 NSA CLPO Report]. NSA now refers to this as "released" or "identity release."

[133] 2021 NSA Minimization Procedures, *supra*, at 13-15.

[134] Id.

[135] 2017 NSA CLPO Report, *supra*, at 8. Cryptologic Requirements & Dissemination (CRD) Chief; Chief Operations Officer (COO); the NSOC Senior Reporting Officers (SROs); the Virtual SROs (VSROs); or the SRO Desk Coordinator/Alternate Desk Coordinator (known as the CRD cadre) may approve the dissemination of a U.S. person identity.

[136] *Id.* at 5-6.

[137] Letter from Robert Storch, Nat'l Sec. Agency, Off. of the Inspector Gen., to the Chairman of the S. Select Comm. on Intel., at 2 n.2 (Oct. 4, 2021) ("NSA stated that it does not maintain records that allow it to readily determine if the source of the U.S. person identity was derived from collection pursuant to subsection 702(a) of the FISA or from other authorized collection. The term U.S. persons encompasses both individuals and non-individual entities, to include but not limited to, U.S. citizens, aliens lawfully admitted for permanent residence (i.e., green card holders), . . . and corporations incorporated in the United States, all of which NSA masks pursuant to law or policy.").

[138] 2021 CIA Minimization Procedures, *supra*, at 4-5, 9-10.

foreign power) it may become necessary to understand the foreign intelligence information.[139] CIA may further disseminate evidence of a crime to federal law enforcement authorities.[140]

FBI's minimization procedures permit FBI to disseminate Section 702-acquired U.S. person information. Raw Section 702-acquired information may be disclosed beyond NSA, CIA, and NCTC only for technical and linguistic purposes.[141] FBI may disseminate minimized Section 702-acquired information in a number of circumstances as discussed below. Between September 2021 and August 2022, FBI disseminated 3,527 reports containing Section 702-acquired U.S. person information.[142]

First, FBI may disseminate information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information.[143] Disseminations concerning the national defense or security of the United States or the conduct of foreign affairs of the United States are permitted under the procedures to identify U.S. persons only if necessary to understand the foreign intelligence information or to assess its importance.[144] For example, if the communications collected indicate that a U.S. person is engaging in unauthorized communications with a Section 702 target about U.S. military operations, FBI may include information about that U.S. person in disseminated intelligence reports.

Second, FBI is also permitted to disseminate U.S. person information that reasonably appears to be evidence of a crime, but not foreign intelligence information, to other law enforcement authorities.[145] In both foreign intelligence and evidence of a crime disseminations, FBI may disseminate information to federal prosecutors, as well as to federal, state, local, and tribal law enforcement officials and agencies.[146] Where there is evidence of a crime related to

[139] 2021 CIA Minimization Procedures, *supra*, at 4-5, 9-10; *see* Cent. Intel. Agency, Off. of Priv. and C.L., Review of Procedures and Practices of CIA to Disseminate United States Person Information Acquired to Titles I and III and Section 702 of the Foreign Intelligence Surveillance Act (FISA), at 12-13 (Aug. 2017), https://dni.gov/files/documents/icotr/Annex-3---CIA-Report-on-Protecting-USP-Information-in-FISA-Dissemination.pdf.

[140] 2021 CIA Minimization Procedures, *supra*, at 4-5, 9-10.

[141] 2021 FBI Minimization Procedures, *supra*, at 44-45.

[142] Fed. Bureau of Investigation, Supplemental Response to Accuracy Review (Jan. 2023).

[143] 2021 FBI Minimization Procedures, *supra*, at 41 (limited to federal, state, local, and tribal officials, not private entities).

[144] *Id.*

[145] *Id.* at 41-42 ("Nothing in these procedures authorizes the dissemination of non-publicly available information that identifies any United States person without such person's consent unless…(3) the information is evidence of a crime which has been, is being, or is about to be committed and that is to be disseminated for law enforcement purposes.").

[146] *Id.* at 36-37, 41-42.

child exploitation, including child sexual abuse material (CSAM), FBI may disseminate the information to the National Center for Missing and Exploited Children.[147]

Further, similar to NSA, FBI's minimization procedures also authorize dissemination to foreign governments, and specify the approvals required to do so.[148] FBI does not, however, track the number of disseminations of Section 702-acquired information made for various purposes.

Communications and data identified as foreign intelligence information or, in certain cases, evidence of a crime, may also be disseminated to other recipients for a number of specifically enumerated purposes, including terrorist screening,[149] to support terrorism-related cases and counterterrorism efforts by NCTC,[150] to private entities and individuals to assist in the mitigation or prevention of computer intrusions or attacks,[151] and to private entities and individuals where FBI determines the information is capable of providing assistance in mitigating or preventing serious economic harm or serious physical harm to life or property.[152]

Like NSA, NCTC may only disseminate a U.S. person's identity for one of a specific list of reasons, including that the U.S. person has consented to the dissemination, the U.S. person's identity is necessary to understand foreign intelligence information or assess its importance, the information is itself foreign intelligence information, or the information is evidence of a crime and is being disseminated to law enforcement authorities.[153]

E. Privileged Communications

Use and dissemination requirements also apply to specific sensitive communications. When attorney-client communications are acquired through Section 702 collection, agencies must adhere to specific guidelines set forth in the minimization procedures. The FISC has found that the attorney-client communication provisions in the agency minimization procedures meet the

[147] *Id.* at 42.

[148] *Id.* at 42-44.

[149] *Id.* at 46.

[150] *Id.* at 46-47.

[151] *Id.* at 47.

[152] *Id.* at 47-48.

[153] 2021 NCTC Minimization Procedures, *supra*, at 11. Similar to other agency minimization procedures, the full list of authorized disseminations of information that identifies a U.S. person includes: (a) consent to the dissemination; (b) such person's identity is necessary to understand the foreign intelligence information or assess its importance; the information is foreign intelligence information as defined in 50 U.S.C. § 1801(e)(1); (c) the information is evidence of a crime which has been, is being, or is about to be committed and that is to be disseminated for law enforcement purposes.

requirements for minimization procedures in Section 1801(h). The FISC has also found that these provisions are constitutionally sufficient and reasonably designed to protect the privacy interests in attorney-client communications, consistent with the need to review those communications for legitimate foreign intelligence purposes.[154] Specifically, the FISC found in 2015 that these provisions "serve to enhance the protection of privileged information" and "present no concern under Section 1801(h)."[155] The procedures for each agency require special handling of intercepted communications that are between attorneys and clients (or agent to a client) and concern privileged information. There are substantive differences when comparing the procedures, and there have been many changes over the years regarding the handling of these communications.

In 2015, based on discussions with the Intelligence Oversight Board and the American Bar Association, the government made modifications to the attorney-client communication provisions in the NSA and CIA Section 702 minimization procedures to add additional protections regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to Section 702.[156] Each set of provisions requires the destruction of attorney-client communications that are determined not to contain foreign intelligence information or evidence of a crime.[157] However, there are substantive differences when comparing FBI's procedures regarding attorney-client communications to the other agencies' procedures, and this reflects each agency's different role in the handling and use of such communications.

First, as explained above, if NSA, CIA, or NCTC determines that an attorney-client communication does not contain foreign intelligence information or evidence of a crime, the agency must destroy the communication, irrespective of whether it contains information protected by the attorney-client privilege.[158] However, if the agency personnel handling or processing the communication determine that an attorney-client communication appears to contain foreign

[154] Memorandum Opinion and Order, at 16-18, In re DNI/AG 702(g) Certification 2015-A and Predecessor Certifications, Docket No. 702(i)-15-01 and predecessor dockets, In re DNI/AG 702(g) Certification 2015-B and Predecessor Certifications, Docket No. 702(i)-15-02 and predecessor dockets, In re DNI/AG 702(g) Certification 2015-C and Predecessor Certifications, Docket No. 702(i)-15-03 and predecessor dockets (FISA Ct. Nov. 6, 2015) [hereinafter 2015 Cert FISC Opinion and Order].

[155] Id. at 18.

[156] U.S. Dep't of Just., DOJ Responses to PCLOB Questions Received on 8/23/22, at 9 (Oct. 3, 2022). In 2015, NCTC was not yet authorized to receive unminimized Section 702-acquired information. Similar provisions have appeared in NCTC's Section 702 minimization procedures since the FISC approved NCTC's access to unminimized Section 702-acquired information in 2017. *See, e.g.*, 2021 NCTC Minimization Procedure, *supra*, at 9-11.

[157] *See* 2021 NSA Minimization Procedures, *supra*, at 9-11; 2021 NCTC Minimization Procedures, *supra*, at 9; 2021 FBI Minimization Procedures, *supra*, at 17-23; 2021 CIA Minimization Procedures, *supra*, at 6-8.

[158] 2021 NSA Minimization Procedures, *supra*, at 10; 2021 NCTC Minimization Procedures, *supra*, at 9; 2021 CIA Minimization Procedures, *supra*, at 6.

intelligence information or evidence of a crime, those personnel are required to bring the communication to the attention of the agency attorneys for further handling in accordance with the other provisions of the procedures.[159] Agency counsel will then determine whether the communications contain privileged information (i.e., information that would be protected by the attorney-client privilege in a U.S. federal court).[160] Privileged communications are required to be "segregated" when the privileged information pertains to a criminal charge in the United States.

The attorney-client communication provisions in FBI's Section 702 minimization procedures significantly differ from those adopted by NSA, CIA, and NCTC insofar as FBI's procedures include requirements for the establishment of review teams, also known as taint teams, and for sequestration of communications related to a charged offense.[161] These differences are due to FBI's status as a law enforcement agency and the fact that FBI is more likely to be considered part of the prosecution team.[162]

For example, FBI's procedures require that in instances where a target has been charged with a crime in the United States, either pursuant to U.S. Code or on non-federal charges, or where a non-target has been charged with a crime in the United States, and FBI intercepts attorney-client privileged communications in the charged matter, FBI must identify such communications and then take steps to remove those communications from FBI systems and sequester them with the FISC.[163] Further, when a target has been charged with a crime in the United States pursuant to the U.S. Code, FBI must establish a review team whose purpose is to review all collection and identify any attorney-client privileged communications.[164] The establishment of a review team is not required for targets who have been charged with a non-federal crime in the United States; however, in the absence of a review team, FBI personnel in these instances are still required to identify, remove, and sequester with the FISC any attorney-client privileged communications in the charged

[159] 2021 NSA Minimization Procedures, *supra*, at 10; 2021 NCTC Minimization Procedures, *supra*, at 9; 2021 CIA Minimization Procedures, *supra*, at 7.

[160] *See, e.g.*, 2021 NSA Minimization Procedures, *supra*, at 10; 2021 NCTC Minimization Procedures, *supra*, at 9.

[161] DOJ Responses to PCLOB Questions Received on 8/23/22, *supra*, at 7.

[162] See, e.g., Memorandum Opinion and Order, at 25, In re DNI/AG 702(h) Certification 2020-A and its Predecessor Certifications, Docket No. 702(j)-20-01 and predecessor dockets, In re DNI/AG 702(h) Certification 2020-B and its Predecessor Certifications, Docket No. 702(j)-20-02 and predecessor dockets, In re DNI/AG 702(h) Certification 2020-C and its Predecessor Certifications, Docket No. 702(j)-20-03 and predecessor dockets (FISA Ct. Nov. 18, 2020) [hereinafter 2020 Cert FISC Opinion and Order].

[163] *See* 2021 FBI Minimization Procedures, *supra*, at 18-21, 26.

[164] *See id.* at 18-19.

matter.[165]

The only instances where FBI may retain and use attorney-client privileged communications are instances where a target or non-target has not been charged with a crime in the United States.[166] Nonetheless, FBI personnel are subject to additional restrictions on their ability to retain and use such communications. FBI personnel must identify attorney-client privileged communications stored in FBI systems in a manner that is apparent to anyone who accesses the information.[167] Before disseminating the information to any other agency within the Intelligence Community, FBI personnel must first obtain the approval of FBI's Office of General Counsel or their FBI Division Counsel, and must make reasonable efforts to use non-privileged sources and tailor the dissemination to minimize or eliminate the disclosure of attorney-client privileged communications, consistent with the need to disseminate foreign intelligence information or evidence of a crime.[168] Moreover, any disseminations of attorney-client privileged communications must include language advising recipients that the report contains information subject to the attorney-client privilege, is provided solely for intelligence or lead purposes, and that it may not be disseminated further or used in any trial, hearing, or other proceeding without FBI's express approval.[169]

In sum, although the agencies' respective minimization procedures have differences as they relate to the treatment of attorney-client privileged communications, each set of procedures contains restrictions on the ability of each agency to retain and use such communications.

V. Querying Procedures

Agencies conduct queries to search through *unminimized* data that has already been lawfully collected and identify pertinent information.[170] Hence, a query does not cause the government to obtain any new communications. Queries are thus similar to an Internet search, in this case searching Section 702 data repositories to identify and return records that include a match to the query terms used (e.g., an email address, phone number, name, or other terms relating to the subject of an analyst's investigation).

[165] DOJ Responses to PCLOB Questions Received on 8/23/22, *supra,* at 8; U.S. Dep't of Just., Training: FISA Minimization. No notice is provided to the attorney whose communications are acquired through Section 702.

[166] 2021 FBI Minimization Procedures, *supra,* at 21-23.

[167] *Id.* at 21-22.

[168] *Id.* at 22.

[169] *Id.* at 22-23.

[170] *See* PCLOB March 2014 Hearing Transcript, *supra*.

Prior to 2018, agencies were not required to adopt a separate set of procedures regarding queries. Rather, agencies' minimization procedures contained some requirements for conducting queries of unminimized Section 702-acquired information. In the 2018 Reauthorization Act, Congress required that all agencies that have access to unminimized Section 702-acquired information—at that time, NSA, FBI, CIA, and NCTC—develop separate querying procedures and submit them annually to the FISC for its review and approval.[171]

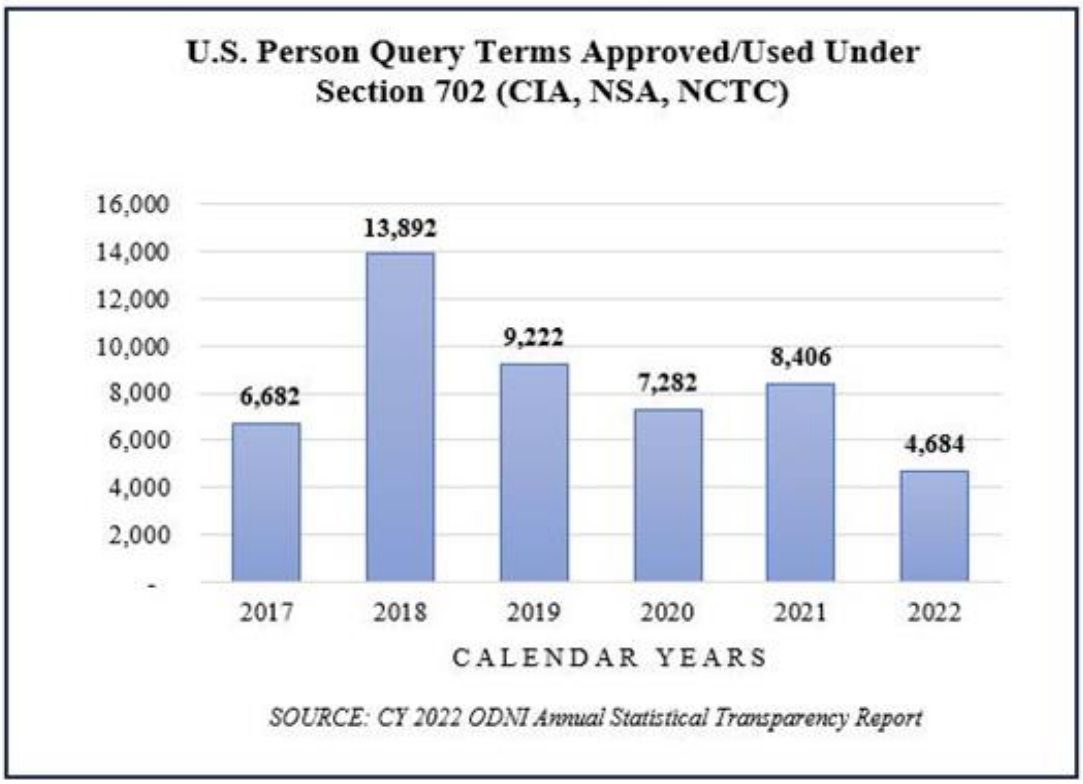


Figure 2

The 2018 Reauthorization Act further required that the querying procedures be "consistent with the requirements of the Fourth Amendment to the Constitution" and that the Attorney General and the DNI ensure the procedures adopted include a technical procedure to maintain a record of each U.S. person query term used for a query.[172] The FISC most recently approved the procedures on April 11, 2023.[173]

[171] 50 U.S.C. § 1881a(f)(1)(A), a(f)(3)(B).

[172] *Id.* § 1881a(f)(1)(A)-(B).

[173] Memorandum Opinion and Order, at 111, In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications, Docket No. 702(j)-23-01 and predecessor dockets, In re DNI/AG 702(h) Certification 2023-B and its Predecessor Certifications, Docket No. 702(j)-23-02 and predecessor dockets, In re DNI/AG 702(h) Certification

In addition, the Section 702 querying procedures must be reasonably designed to guard against the indiscriminate or improper accessing or use of Section 702-acquired information.[174] Each agency's procedures further define what a query is, what a U.S. person query is, the standard that must be met to run the query, the maintenance of query records, and any exceptions thereto.[175]

In addition to other exceptions discussed below, every agency's querying procedures include an emergency exception authorizing agencies to take action in apparent departure from the procedures.[176] The exception authorizes agencies to depart from the procedures to protect against an immediate threat to human life if it is "not feasible to obtain a timely modification" of the procedures.[177] The applicable sections in the agencies' procedures mandate that the agency make a record of the action taken and the query term(s) used and report the action to DOJ and ODNI, which must promptly inform the FISC of such activity.[178] To date, the emergency exception has not been used by any agency.

A. Definition of a "Query"

FISA defines the term "query" as "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic storage systems of communications of or concerning

2023-C and its Predecessor Certifications, Docket No. 702(j)-23-03 and predecessor dockets (FISA Ct. Apr. 11, 2023).

[174] 2018 Cert FISC Opinion and Order, *supra*, at 64 (stating that the Section 702 querying procedures are meant to "guard against indiscriminate or improper accessing or use of U.S. person information").

[175] Nat'l Sec. Agency, Exhibit H, Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2021) [hereinafter 2021 NSA Querying Procedures]; Nat'l Counterterrorism Ctr., Querying Procedures Used by the National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2021) [hereinafter 2021 NCTC Querying Procedures]; Fed. Bureau of Investigation, Exhibit I, Querying Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2021) [hereinafter 2021 FBI Querying Procedures]; Cent. Intel. Agency, Exhibit J, Querying Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2021) [hereinafter 2021 CIA Querying Procedures].

[176] 2021 NSA Querying Procedures, *supra*, at 1; 2021 NCTC Querying Procedures, *supra*, at 1; 2021 FBI Querying Procedures, *supra*, at 1; 2021 CIA Querying Procedures, *supra*, at 1.

[177] 2021 FBI Querying Procedures, *supra*, at 1.

[178] 2021 NSA Querying Procedures, *supra*, at 1 (Upon such a departure, NSA "will make a record of the action taken, to include any query term(s) used, and report the action taken to the Office of the Director of National Intelligence ("ODNI") and to the Department of Justice's National Security Division ("NSD"), which is directed to promptly notify the foreign Intelligence Surveillance Court ("FISC") of such activity."). For similar language, *see* 2021 NCTC Querying Procedures, *supra*, at 1; 2021 FBI Querying Procedures, *supra*, at 1; 2021 CIA Querying Procedures, *supra*, at 1.

U.S. persons obtained through acquisitions authorized under" Section 702.[179] Notwithstanding the statutory definition, the FISC and the Intelligence Community have applied a common definition to all queries of systems containing unminimized Section 702-acquired information, as such information has the potential to contain communications of or concerning U.S. persons. The procedures for CIA, NCTC, NSA, and FBI contain nearly identical definitions of a "query."[180]

B. Definition of a U.S. Person Query

Agency procedures approved by the FISC permit querying Section 702 collection using terms related to U.S. persons or presumed U.S. persons.[181] A U.S. person query is one conducted using a term that "is reasonably likely to identify one or more specific United States persons."[182] Such terms may include: names or unique titles; government-associated personal or corporate identification numbers; street addresses; and telephone numbers.[183]

Each agency's querying procedures note that a "United States person query term" does not include a reference to a product by brand or manufacturer's name (or related nomenclature, including part numbers) or the use of a name in a descriptive sense, "as, for example, 'Ford Crown Victoria' or 'Boeing 737,' so long as such term is not intended to retrieve information concerning a specific United States person (e.g., 'Ford Crown Victoria with License Plate Number CBA 321')."[184] In short, depending on the context, information that in isolation would not identify a U.S. person could, when combined with other information, be considered a U.S. person query term if it is reasonably likely to identify one or more specific U.S. persons.[185]

[179] 50 U.S.C. § 1881a(f)(3)(B).

[180] 2021 NSA Querying Procedures, *supra*, at 2; 2021 NCTC Querying Procedures, *supra*, at 2; 2021 FBI Querying Procedures, *supra*, at 2; 2021 CIA Querying Procedures, *supra*, at 2.

[181] All agencies' querying procedures contain presumptions to be used when the agency cannot determine whether the query term belongs to a U.S. person or a non-U.S. person. 2021 NSA Querying Procedures, *supra*, at 2-3; 2021 NCTC Querying Procedures, *supra*, at 2-3; 2021 FBI Querying Procedures, *supra*, at 2-3; 2021 CIA Querying Procedures, *supra*, at 2-3. Agencies may not have certainty around the identity of the person or the U.S. person status determinations and are forced to rely on presumptions when they lack definitive information.

[182] 2021 NSA Querying Procedures, *supra*, at 1-2; 2021 NCTC Querying Procedures, *supra*, at 1-2; 2021 FBI Querying Procedures, *supra*, at 1-2; 2021 CIA Querying Procedures, *supra*, at 1-2.

[183] 2021 NSA Querying Procedures, *supra*, at 1-2; 2021 NCTC Querying Procedures, *supra*, at 1-2; 2021 FBI Querying Procedures, *supra*, at 1-2; 2021 CIA Querying Procedures, *supra*, at 1-2.

[184] 2021 NSA Querying Procedures, *supra*, at 1-2; 2021 NCTC Querying Procedures, *supra*, at 1-2; 2021 FBI Querying Procedures, *supra*, at 1-2; 2021 CIA Querying Procedures, *supra*, at 1-2.

[185] 2021 NSA Querying Procedures, *supra*, at 1-2; 2021 NCTC Querying Procedures, *supra*, at 1-2; 2021 FBI Querying Procedures, *supra*, at 1-2; 2021 CIA Querying Procedures, *supra*, at 1-2.

C. Searches That Are Not Defined as Queries

Lastly, agency query procedures except certain types of searches from the definition of a "query."[186] This means that the agencies do not define certain searches of databases that contain Section 702 information as "queries" under their query procedures and these searches need not satisfy the querying standard.

Under NSA's procedures, queries do not include searches when (a) unminimized Section 702-acquired information is not received in response either because the user lacks access to unminimized Section 702-acquired information or because personnel with access structure the search so that "it cannot retrieve" unminimized Section 702-acquired information; (b) a subsequent user action sorts by attribute the results of a query that returns Section 702-acquired information; (c) examining or manipulating the communication or document returned for the purpose of minimization; or (d) a search is conducted in user activity monitoring systems.[187]

CIA's query definitions are similar to NSA's, while NCTC contains only NSA's first three exclusions as listed above.[188] FBI's querying procedures further expand NSA's exclusions to also include searches conducted in "special purpose systems," like systems used solely for audits and oversight.[189] Similarly, searches of *minimized* Section 702 data are not governed by Section 702 querying procedures, but may be governed by other agency policy or executive branch order or guidance.[190]

D. The Query Standard

As stated above, queries must be reasonably likely to retrieve foreign intelligence information or, in the case of FBI, may alternatively be reasonably likely to retrieve evidence of a crime.[191] In order to satisfy this query standard, queries must:

[186] 2021 NSA Querying Procedures, *supra*, at 2; 2021 NCTC Querying Procedures, *supra*, at 2; 2021 FBI Querying Procedures, *supra*, at 2; 2021 CIA Querying Procedures, *supra*, at 2.

[187] 2021 NSA Querying Procedures, *supra*, at 2.

[188] 2021 CIA Query Procedures, *supra*, at 1-2; 2021 NCTC Querying Procedures, *supra*, at 1-2.

[189] The full list of Special Purpose Systems include Collection Platforms, systems Used Solely for Audits and Oversight, Systems or Other repositories that contained Data Obtained through User Activity Monitoring Activities, Backup and Evidence Copies into FBI Systems, and Queries in Special Purpose Systems. 2021 FBI Minimization Procedures, *supra*, at iii-iv.

[190] 2021 FBI Querying Procedures, *supra*, at 2; *see* 2021 NSA Querying Procedures, *supra*; 2021 NCTC Querying Procedures, *supra*; 2021 CIA Querying Procedures, *supra*.

[191] 2021 FBI Querying Procedures, *supra*, at 3; *see* 2021 NSA Querying Procedures, *supra*; 2021 NCTC Querying Procedures, *supra*; 2021 CIA Querying Procedures, *supra*.

- Be conducted for the purpose of retrieving foreign intelligence information or, in the case of FBI, alternatively evidence of a crime;
- Be reasonably tailored so that they retrieve the information sought and limit the retrieval of unnecessary or irrelevant information; and
- Be supported by a proper justification (the facts indicate that the information sought is reasonably likely to be contained in the agency's Section 702 collection).[192]

1. *The Query Purpose*

The purpose of the query is a threshold question. Other than under specific exceptions that are delineated in the querying procedures, queries conducted by NSA, CIA, and NCTC must be conducted for the purpose of retrieving foreign intelligence information.[193] Queries conducted by FBI must be reasonably likely to retrieve foreign intelligence information, evidence of a crime, or both.[194] FBI maintains this broader query standard because it is the only FISA agency with a dual intelligence and law enforcement mission.[195] Some examples of queries lacking a proper purpose may include:

- A linguist querying his own user ID in agency systems in order to look for products he had translated for his self-assessment at rating time;
- An analyst conducting a query only to log some activity in a system to meet a system access requirement for continuous activity; or
- A query performed for purposes of determining the proper spelling of an agency case codename.

[192] *See* 2021 FBI Querying Procedures, *supra*, at 3. In the case of FBI, the justification must indicate that the information sought is reasonably likely to be contained in the agency's FISA collection because FBI agents may choose to have queries run through both Section 702-acquired data and data obtained through traditional FISA authorities. *See also* 2021 NSA Querying Procedures, *supra*; 2021 NCTC Querying Procedures, *supra*; 2021 CIA Querying Procedures, *supra*.

[193] 2021 NSA Querying Procedures, *supra*, at 3-6; 2021 NCTC Querying Procedures, *supra*, at 3-5; 2021 FBI Querying Procedures, *supra*, at 3-7; 2021 CIA Querying Procedures, *supra*, at 3-5.

[194] 2021 FBI Querying Procedures, *supra*, at 3. As discussed later, such dual purpose queries oftentimes seek information on international terrorism or espionage.

[195] *See* 50 U.S.C. § 1801 et seq.; Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, 118 Stat. 3638 (2004) (outlining FBI intelligence authorities); 28 U.S.C. § 533 (authorizing the Attorney General to appoint officials to detect and prosecute crimes against the United States); 50 U.S.C. § 401 et seq.; Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981); 18 U.S.C. § 3052 (authorizing special agents and officials of FBI to make arrests, carry firearms, and serve warrants); 18 U.S.C. § 3107 (empowering special agents and officials to make seizures under warrant for violation of federal statutes).

2. *The Query Design*

The design of a query allows an analyst to filter collected information to extract the most relevant information from the Section 702 collection.[196] Query terms need not be communications facilities or tasked selectors. Analysts may use selectors such as a phone number or email address to query data to retrieve collection relating to a selector, but analysts may also use terms such as names, addresses, or keywords to query Section 702 collection.[197] A query works similarly to an Internet search, where the more specific or focused the terminology used to search available data and the more restricted the dataset queried, the less amount of non-relevant information retrieved. For example, a query using just the word "bomb" with no limiters would generally be considered to be overly broad and would likely return a subset of results that is not foreign intelligence information or, in FBI's case, evidence of a crime or inquiry, but using the term "bomb" and another more nuanced term or limiting the search to a specific subset of data or inquiry would limit the results retrieved to a more focused set of data. Queries that contain typos like "br" or an individual's generic first name without any other limiting terms are also considered to have a deficient design.[198]

3. *The Query Justification*

To be compliant with the Section 702 querying procedures, a query must also be supported by specific, articulable facts that lead the analyst to believe a query of the agency's Section 702 collection is reasonably likely to be fruitful.[199] Whether or not a query is reasonably likely to return foreign intelligence information or evidence of a crime is not a *post hoc* determination dependent on whether the query actually retrieved relevant results. Rather, it is a preliminary judgment based on the facts available to the analyst or agent prior to conducting the query.[200] As noted, justifications must be fact-specific and lay out the case for why the analyst or agent believes the query is reasonably likely to return foreign intelligence from the agency's FISA collection.[201]

---

[196] *See, e.g.*, FBI FISA Query Training, *supra*, at 18-19.

[197] 2021 NSA Querying Procedures, *supra*, at 2; 2021 NCTC Querying Procedures, *supra*, at 2 n.1; 2021 FBI Querying Procedures, *supra*, at 2; 2021 CIA Querying Procedures, *supra*, at 2.

[198] *See* Fed. Bureau of Investigation, 2019 FISA Section 702 Query Procedure Training (Nov. 2019).

[199] 26th Joint Assessment, *supra*, at A-16.

[200] Id. at A-15.

[201] For example, under one Section 702 certification, an agency is permitted to obtain foreign intelligence information relating to international terrorism. If there is an incident of purely domestic terrorism that is neither inspired by nor related to international terrorism, there would not be specific articulable facts indicating that a query of Section 702 collection pertaining to international terrorism would be likely to return Section 702 data. Because the agency does not obtain Section 702 collection on purely domestic terrorism and there is no link between the act of domestic terrorism and a foreign power that carries out terrorist acts, there is no reason to believe that the agency has obtained any collection related to this act. If, however, facts specific to an act link one of the perpetrators to an

However, as explained further below, agency querying procedures do not always require documentation of this justification prior to conducting the query.

When conducting a foreign intelligence query in a database of information collected because it was believed to have foreign intelligence value, it is often more likely to meet the justification threshold for a proper foreign intelligence query than for a proper evidence of a crime query. When searching for evidence of a crime unrelated to national security, however, an FBI analyst or agent must be able to demonstrate why information about that particular crime or type of crime would be contained in a database mostly composed of foreign intelligence information. An example would be a situation in which the perpetrator of a crime about which an analyst seeks information is known to associate with or operate in the same network as a Section 702 target without the perpetrator also conspiring with the target's national security-related activities. In addition, a routine vetting query such as a query intended to inform whether an individual should be granted access to information, a sensitive position, or permission to enter government space is likely, in the absence of additional facts, to have an improper justification under the querying procedures.

E. Exceptions to the Querying Procedures

Each agency's querying procedures also codify several exceptions such that the requirements contained in the procedures do not apply in certain circumstances.[202] Unlike the situations described above in which the searches are not defined as queries, these exceptions involve searches that meet the query definition, but where the procedures do not apply. The querying procedures include an emergency exception that allows agencies to take action in apparent departure from the procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) when it is not feasible to obtain a timely modification from the procedures.[203] The agency must make a record of the action taken, to include any query term(s)

international terrorist cell or social media posts indicate an allegiance to an international terrorist organization, the act of domestic terrorism may be henceforth characterized as an act of international terrorism and one that might be referred to in the agency's Section 702 collection pertaining to international terrorism. The justification would lay out these relevant facts, providing an explanation of why the analyst decided to query Section 702 collection and why he or she believed the query was compliant.

[202] 2021 NSA Querying Procedures, *supra*, at 1, 5-6; 2021 NCTC Querying Procedures, *supra*, at 1, 4-5; 2021 FBI Querying Procedures, *supra*, at 2, 5-7; 2021 CIA Querying Procedures, *supra*, at 1, 4-5.

[203] 2021 NSA Querying Procedures, *supra*, at 1; 2021 NCTC Querying Procedures, *supra*, at 1; 2021 FBI Querying Procedures, *supra*, at 1; 2021 CIA Querying Procedures, *supra*, at 1.

used, and report the action taken to DOJ and ODNI, which must promptly inform the FISC of such activity.[204]

FBI's procedures do not apply to "conducting queries it determines are necessary to": perform lawful training functions of its personnel, conduct technical maintenance of FBI systems, comply with Freedom of Information Act requests, conduct queries to comply with a court order or congressional mandate, conduct queries to identify information that must be produced or preserved in connection with a litigation matter, and others. NSA, NCTC, and CIA all have similar exceptions to their querying procedures.[205]

In 2020, NSA's querying procedures were updated to exempt queries conducted to identify and remove child exploitation material from NSA systems from the query standard and additional querying requirements.[206] NSA noted that it has an interest in proactively identifying, removing, and destroying child exploitation material to prevent its personnel from unneeded exposure to highly disturbing and illegal material. Neither FBI, CIA, nor NCTC's querying procedures contain a similar provision; at the time of this Report, no other agencies had asked for a similar exception.[207]

In its *ex parte* submission to the FISC detailing amendments included in its 2021 reauthorization package and reflected in its initial draft of its 2021 querying procedures, NSA requested that the FISC grant a new exception to the querying procedures for certain vetting queries.[208] Specifically, NSA requested that queries supporting vetting activities for non-U.S. persons located outside the United States who have applied or are being processed for immigration

[204] 2021 NSA Querying Procedures, *supra*, at 1; 2021 NCTC Querying Procedures, *supra*, at 1; 2021 FBI Querying Procedures, *supra*, at 1; 2021 CIA Querying Procedures, *supra*, at 1.

[205] 2021 NSA Querying Procedures, *supra*, at 5-6; 2021 NCTC Querying Procedures, *supra*, at 4-5; 2021 CIA Querying Procedures, *supra*, at 4-5.

[206] Nat'l Sec. Agency, Exhibit H, Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 5 (2020) [hereinafter 2020 NSA Querying Procedures].

[207] *See generally* 2021 NCTC Querying Procedures, *supra*; 2021 FBI Querying Procedures, *supra*; 2021 CIA Querying Procedures, *supra*. According to FBI, if FBI personnel were to conduct a query in order to identify child exploitation material, such a query would likely have a permissible evidence of a crime purpose. As such, FBI believes it does not need an exemption for such a query in its querying procedures. In the unlikely event that a situation arose where such a query would not be for an evidence of a crime purpose, FBI would likely seek a departure in order to conduct a query.

[208] Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications, at 17, *In re DNI/AG 702(h) Certification 2021-A and its Predecessor Certifications, In re DNI/AG 702(h) Certification 2021-B and its Predecessor Certifications, In re DNI/AG 702(h) Certification 2021-C and its Predecessor Certifications* (FISA Ct. Oct. 18, 2021).

or travel to the United States be exempt from the query standard or additional querying requirements.[209] This amendment was ultimately removed from the querying procedures approved in April 2022 and reserved for amendment following review by amici and consideration by the FISC. In April 2023, the FISC approved the government's proposal in connection with the 2023 Querying Procedures.

F. U.S. Person Queries

While Section 702 collection may not target U.S. persons or persons located in the United States, incidental collection or collection of information concerning U.S. persons may occur when targeting non-U.S. persons located abroad. This collection occurs when a properly targeted non-U.S. person located abroad communicates with a U.S. person (incidental collection) or refers to a U.S. person in communications with others (information concerning U.S. persons).[210] While the government is restricted from targeting U.S. persons, agency procedures permit querying Section 702 collection using terms that identify one or more U.S. persons when there is a valid foreign intelligence purpose, or for FBI, alternatively, to seek evidence of a crime.[211] The same query standard applies to both U.S. person queries and non-U.S. person queries.

Agencies conduct U.S. person queries with different frequency and for different purposes. As noted previously, NSA, CIA, and NCTC are authorized to query unminimized Section 702 collection only to retrieve foreign intelligence information. In CY 2020, 2021, and 2022, these agencies used a total of 7,282, 8,406, and 4,684 U.S. person query terms to query unminimized Section 702-acquired content.[212] These numbers, however, do not include U.S. person searches that are excluded from the query definition or exempted from querying procedures. Multiple query terms may be associated with a single U.S. person, resulting in fewer than 7,282, 8,406, and 4,684 U.S. persons that were the subject of such queries. However, each query term may have been used

[209] *Id.* at 13.

[210] Off. of the Dir. of Nat'l Intel., Section 702: Incidental Collection in a Targeted Intelligence Collection Program (2023), https://www.odni.gov/files/FISA_Section_702/Incidental_Collection_Section_702_FISA.pdf.

[211] 2021 NSA Querying Procedures, *supra*, at 3-4; 2021 FBI Querying Procedures, *supra*, at 4.

[212] CY2022 ASTR, *supra*, at 20. Additionally, during the same timeframe, the three agencies conducted 9,051, 3,958, and 3,656 U.S. person queries of noncontent. As discussed below, NSA's metrics are based on U.S. person query terms whereas FBI's metrics are based on U.S. person queries. The CY2022 ASTR clarifies that FBI's counting methodology has been updated. The counting methodology FBI used for the CY2021 ASTR counted duplicate queries since, at the time, FBI systems were only designed to identify the total number of queries, not the number of unique U.S. person query terms. FBI updated their counting methodology for the CY2022 ASTR to eliminate duplicate queries and more closely align with other IC elements' counting methodologies. FBI recalculated statistics for the periods December 2019–November 2020 and December 2020–November 2021 using the updated counting methodology. This Report uses the figures calculated with the updated counting methodology, unless where explicitly noted.

multiple times or at regular intervals, resulting in a potentially larger number of U.S. person queries.

By contrast, FBI, with its domestic-focused mission and additional permissible purpose to query for evidence of a crime, uses significantly more query terms associated with U.S. persons.[213] Based on the nature and scope of FBI's work, which includes a significant number of queries prior to opening an assessment or during an assessment stage, unlike other agencies, FBI does not have a system in place to run repeated or recurring queries. For example, in the twelve-month period ending November 30, 2021, FBI reported 3,394,053 U.S. person queries consisting of 2,964,643 unique query terms, approximately 1.9 million of which were associated with a single cyber threat.[214] For the twelve-month period from December 1, 2021 through November 30, 2022, FBI conducted U.S. person queries using 119,383 unique U.S. person identifiers.[215] The government asserts that queries are a basic analytic step used for a variety of purposes, including searching to verify, follow up on, or investigate preliminary information made known to or provided by an analyst.[216] The government has asserted that U.S. person queries "help the government detect and evaluate connections between U.S. persons and foreign adversaries involved in perpetrating terrorist attacks or other serious crimes."[217]

Specifically, agencies use U.S. person queries to identify potential victims or unwitting participants in potential threats to national security so that the government might take steps to warn or protect the individual and mitigate the foreign threat. For example, in a 2021 investigation into a cyber-attack on critical infrastructure, FBI conducted victim queries to understand the types of victims that might be targeted by this type of attack.[218] In other cases, FBI has conducted queries to determine if particular accounts had been compromised by a cyber-attack.[219] U.S. person queries are also conducted to identify knowing and willing participants.[220] If the U.S. person is a willing and knowing participant, the government may determine whether to open an investigation into and target the U.S. person under an alternate FISA authority such as Title I.[221]

---

[213] CY2022 ASTR, *supra*, at 22.

[214] CY2021 ASTR, *supra*, at 21. The report includes a description of how FBI defined queries for this purpose.

[215] CY2022 ASTR, *supra*, at 24.

[216] Off. of the Dir. of Nat'l Intel., *Section 702 Overview*, at 10, https://dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

[217] Id.

[218] CY2021 ASTR, *supra*, at 20.

[219] Fed. Bureau of Investigation, Response from FBI to PCLOB (Sept. 2022).

[220] Id.

[221] OFF. OF THE DIR. OF NAT'L INTEL., SECTION 702: TARGETING UNDER FISA SECTION 702 (2023), https://www.odni.gov/files/FISA_Section_702/Targeting _Under_Section_702_FISA.pdf. However, no such U.S. person could be a target under Section 702.

While targeting prohibitions apply to both U.S. persons and anyone located in the United States, heightened querying requirements and restrictions only extend to U.S. persons. In assessing whether a person is a U.S. person, agencies apply specific presumptions when the status of the person is unknown.[222] For example, for the purpose of querying, a person known to be located in the United States is treated as a U.S. person unless the person is identified as an alien who has not been admitted for lawful permanent residence "or the circumstances give rise to the belief that such person is not a [U.S.] person."[223] Alternatively, an unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a U.S. person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.[224]

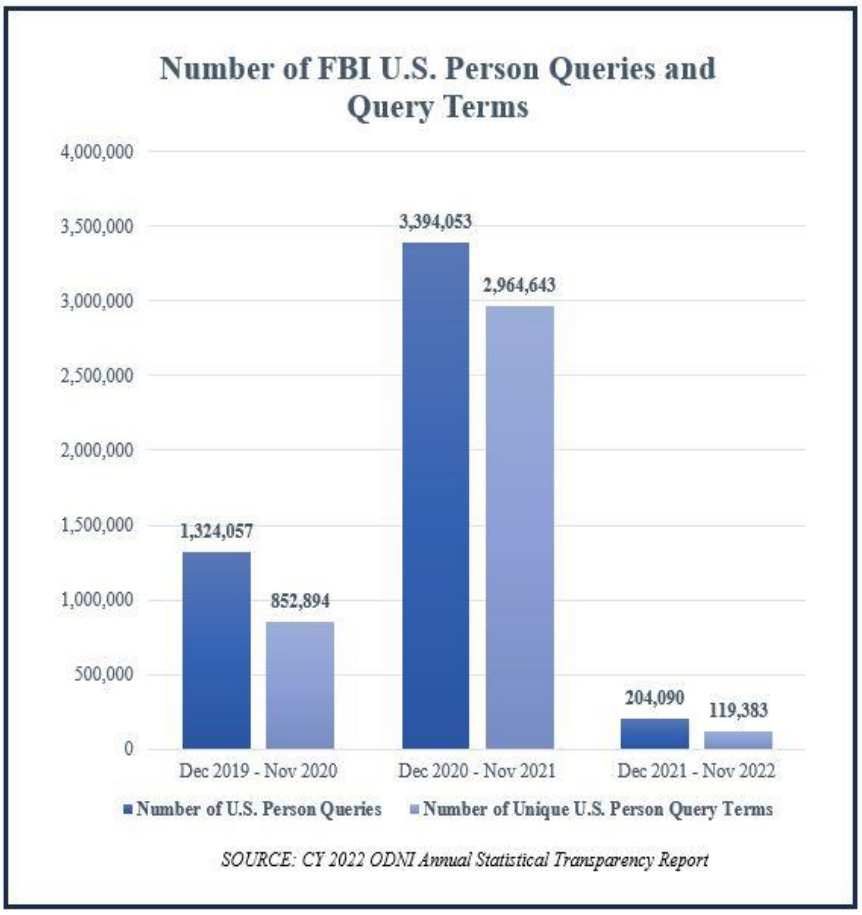


Figure 3

As noted above, while non-U.S. person and U.S. person queries are governed by the same query standard, there are specific reporting and approval requirements for U.S. person queries.

[222] *See* 2021 NSA Querying Procedures, *supra*, at 3; 2021 NCTC Querying Procedures, *supra*, at 2-3; 2021 FBI Querying Procedures, *supra*, at 3; 2021 CIA Querying Procedures, *supra*, at 2-3.

[223] *See* 2021 NSA Querying Procedures, *supra*, at 3; 2021 NCTC Querying Procedures, *supra*, at 2-3; 2021 FBI Querying Procedures, *supra*, at 3; 2021 CIA Querying Procedures, *supra*, at 3.

[224] *See* 2021 NSA Querying Procedures, *supra*, at 3; 2021 NCTC Querying Procedures, *supra*, at 3; 2021 FBI Querying Procedures, *supra*, at 3; 2021 CIA Querying Procedures, *supra*, at 3.

For example, NSA's querying procedures require that analysts obtain approval from the NSA Office of General Counsel for all U.S. person query terms before they may be used to query content.[225] Such approval is granted for a period of up to one year and may be renewed annually thereafter.[226] Further, prior to using U.S. person query terms, NSA, CIA, and NCTC are required to document and maintain a statement of facts demonstrating that the use of the U.S. person query term is reasonably likely to retrieve foreign intelligence information.[227]

FBI, unlike its peer agencies with access to unminimized Section 702 information, is not bound by the same approval and documentation requirements prior to conducting a query, but is subject to distinct requirements prior to accessing the results of a U.S. person query. After conducting a Section 702 query using a U.S. person query term, but prior to accessing any responsive unminimized content, FBI personnel must input a written justification describing the specific factual basis to believe that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime.[228] FBI announced in the summer of 2023 that it plans to implement a requirement that personnel enter a written justification for all U.S. person queries prior to conducting the query.[229] In addition, as described further below, Congress has enacted specific requirements that apply to certain types of FBI queries seeking evidence of a crime.

All agencies are required to keep a record of each U.S. person query term used to query unminimized Section 702 information.[230] Section 702 explicitly requires that all agencies' querying procedures must "include a technical procedure whereby a record is kept of each United States person query term used for a query."[231] Reporting requirements for this information differ. NSA, CIA, and NCTC are statutorily required to submit information to ODNI to publicly report the number of U.S. person query *terms* used to retrieve the unminimized contents of Section 702-acquired information, as well as the number of U.S. person *queries* of unminimized noncontents.[232]

---

[225] 2021 NSA Querying Procedures, *supra*, at 3-4. This requirement of prior OGC approval does not apply for queries of metadata.

[226] Id.

[227] *Id.* at 4; 2021 NCTC Querying Procedures, *supra*, at 3-4; 2021 FBI Querying Procedures, *supra*, at 4-5; 2021 CIA Querying Procedures, *supra*, at 3-4.

[228] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 39-41; 2021 FBI Querying Procedures, *supra*, at 4.

[229] Off. of the Dir. of Nat'l Intel. et al., Section 702 of the Foreign Intelligence Surveillance Act, at 22 (2023).

[230] *See* 2021 NSA Querying Procedures, *supra*, at 4; 2021 NCTC Querying Procedures, *supra*, at 3-4; 2021 FBI Querying Procedures, *supra*, at 4-5; 2021 CIA Querying Procedures, *supra*, at 3-4.

[231] 50 U.S.C. § 1881a(f)(1)(B); *see* 2021 NSA Querying Procedures, *supra*, at 4; 2021 NCTC Querying Procedures, *supra*, at 3-4; 2021 FBI Querying Procedures, *supra*, at 4-5; 2021 CIA Querying Procedures, *supra*, at 3-4.

[232] *See* 50 U.S.C. § 1873(b)(2)(B)-(C). The number of query terms used or queries conducted is not equivalent to and is generally higher than the number of individuals associated with those terms or queries. For example, the government may query several terms associated with a single individual, such as, name, alternate spellings, known

FBI is exempt from this statutory public reporting requirement,[233] but starting with the Intelligence Community's CY2021 ASTR, the government has reported the number of U.S. person queries conducted by FBI. Further, pursuant to court order, FBI is required to report similar data to the FISC. In quarterly reports to the FISC, FBI must report the number of U.S. person queries conducted; the number of such queries that were identified as evidence of a crime only queries; the number of instances in which a user conducted a batch job query that included 100 or more query terms; each instance in which FBI personnel accessed unminimized contents retrieved pursuant to a U.S. person evidence of a crime only query (other than instances described in Section 702(f)(2) of FISA, as noted below).[234]

G. Evidence of a Crime Only Queries

As noted, unlike NSA, CIA, and NCTC, FBI may query unminimized Section 702-acquired information for both foreign intelligence information and evidence of a crime.[235] Pursuant to a 2015 FISC order, FBI must report to the FISC every time FBI personnel review the contents of communications retrieved pursuant to an evidence of a crime only U.S. person query.[236] As of 2020, FBI systems automatically alert FBI attorneys whenever FBI personnel perform a query of Section 702-acquired information for evidence of a crime only; this permits FBI attorneys to determine whether this reporting requirement applies.[237]

For certain U.S. person queries conducted against Section 702-acquired information that are not designed to find and extract foreign intelligence information, FBI must obtain a Section 702(f)(2) order from the FISC before accessing the contents of communications retrieved pursuant to those queries. Specifically, a Section 702(f)(2) order is required before FBI may access the contents of communications retrieved pursuant to a U.S. person evidence of a crime only query[238] if the query was conducted in connection with a predicated criminal investigation that is unrelated

alias, phone number, email address, or physical address. Further, the government may conduct repeated queries to determine if any new collection contains a match to the query terms.

[233] *Id.* § 1873(d)(2)(A).

[234] For example, in the reporting period December 1, 2020 to November 2021, there were 2,964,643 U.S. person queries and 13 evidence of a crime only U.S. person queries. CY2022 ASTR, *supra*, at 24, 27.

[235] 2021 FBI Querying Procedures, *supra*, at 3-4.

[236] 2015 Cert FISC Opinion and Order, *supra*, at 78.

[237] This Reporting requirement is referred to as the "modified Hogan reporting requirement."

[238] Section 9-90.020 of the Department of Justice Manual notes 20 different criminal provisions "affecting, involving, or relating to the national security." Agents can still be alerted to the existence of results that contain Section 702 content. U.S. DEP'T OF JUST., JUSTICE MANUAL, Title 9-90.020 (2020).

to the national security.[239] The FISC shall issue the order to review the results of the query if "the Court finds probable cause to believe that such contents would provide"[240] evidence of "criminal activity; contraband, fruits of a crime, or other items illegally possessed by a third party; or property designed for use, intended for use, or used in committing a crime."[241] FBI, however, is not required to seek a Section 702(f)(2) order for such queries where there is a reasonable belief that the resulting contents could assist in mitigating or eliminating a threat to life or serious bodily harm.[242]

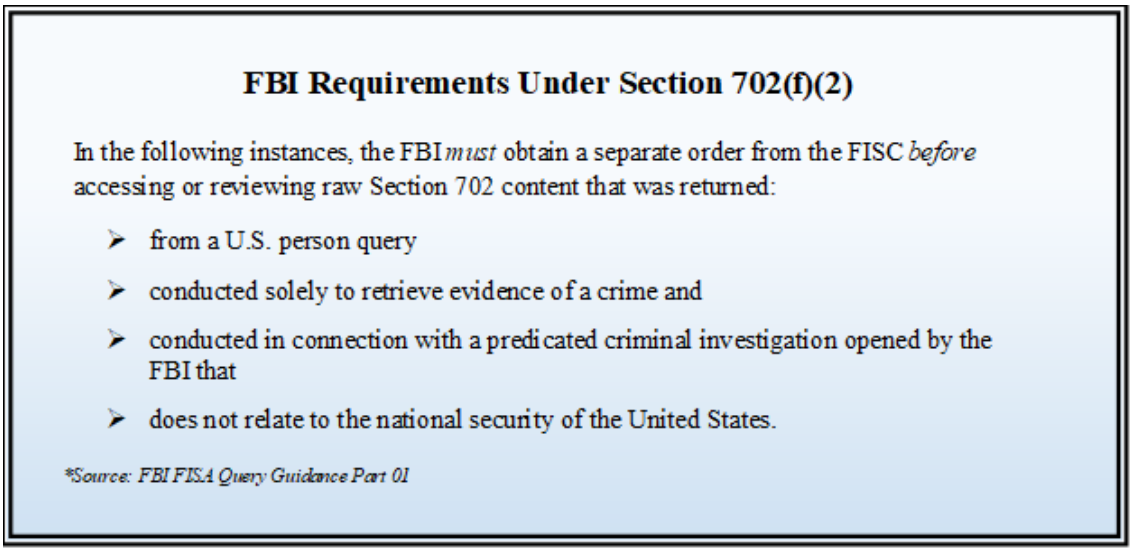


Figure 4

Further, the Section 702(f)(2) requirement to seek a FISC order applies only at the criminal predicated investigation stage, and does not apply to the results of queries that were conducted prior to a pre-assessment or during an assessment.[243] However, FBI personnel may conduct U.S.

[239] 50 U.S.C. § 1881a(f)(2)(A). Predicated criminal investigations must meet the standards set forth in the Attorney General Guidelines (for a preliminary investigation, the standard is that there must be information or an allegation indicating criminal activity; for a full investigation, the standard is that there must be an "articulable factual basis" concerning crimes or threats to national security and indicating criminal activity), may be opened on the basis of any "allegation or information" indicative of a possible criminal activity or threats to the national security, and require supervisor approval prior to opening. *See* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2021) [hereinafter FBI DIOG].

[240] 50 U.S.C. § 1881a(f)(2)(D).

[241] *Id.* § 1881a(f)(2)(C)(ii).

[242] 2021 FBI Querying Procedures, *supra*, at 4. As of August 2023, FBI had not identified any queries that would fall under this exception.

[243] *Id.* According to FBI's Domestic Investigations and Operations Guide, assessments do not require factual predication, but do require an authorized purpose and clearly defined objectives. FBI DIOG, *supra*, at 5-1 ("Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence."). A predicated investigation is "opened on the

person queries of Section 702 information when initiating assessments.[244] Although these queries rarely return Section 702-acquired information, the results retrieved by FBI's U.S. person evidence of a crime queries are not subject to the Section 702(f)(2) requirement because it is limited to queries connected to a predicated criminal investigation. However, FBI routinely conducts queries prior to that stage.[245]

As of August 2023, FBI has never sought a Section 702(f)(2) order, though the government has reported compliance incidents identifying instances in which a Section 702(f)(2) order was required and not sought or obtained.[246] In one instance, an FBI analyst in one field office queried Section 702-acquired information using a U.S. person query term.[247] Unbeknownst to the analyst at the time of the query, the U.S. person was the subject of a predicated investigation opened by another FBI field office.[248] DOJ determined that the analyst should have obtained a Section 702(f)(2) order prior to accessing the results from the query.[249]

basis of 'information or an allegation' indicating the existence of" a federal crime or threat to national security." *Id.* at 6-3.

[244] Fed. Bureau of Investigation, FISA Systems Briefing (June 2022) [hereinafter FBI FISA Systems Briefing]. The FBI technical change to "opt in" has led to a substantial reduction in total FBI U.S. person queries. FBI believes this likely includes queries in the course of an assessment.

[245] *Id.*

[246] The CY2021 ASTR identified four compliance incidents reported to the FISC involving a failure to obtain a Section 702(f)(2) order prior to accessing the results of a query in circumstances when such an order was required. In prior years, ODNI reported a combined number that included both Section 702(f)(2) compliance incidents and instances in which personnel accessed the results of a U.S. person query that was not designed to find and extract foreign intelligence information (circumstances that are not considered compliance incidents). The number of actual Section 702(f)(2) incidents may be higher than reported. When an analyst mistakenly labels the purpose of a query as seeking foreign intelligence information or identifies a dual purpose, the analyst is not restricted from accessing the results of the query and an attorney would not be notified by the system. Because DOJ does not have the resources to review every query, it is possible that these misidentified queries could in fact be Section 702(f)(2) incidents. In addition, between 2018 and 2020, DOJ reported 97 "potential" evidence of a crime-only query compliance incidents. At the time the queries were conducted, FBI personnel were able to see a "preview pane" of Section 702 contents retrieved by the query; thus it could not be determined whether these users "viewed" the results.

[247] 27th AG SAR, *supra*, at 113.

[248] *Id.*

[249] *Id.* DOJ also determined that the query itself did not comply with the query standard, and consequently the government would not have sought a Section 702(f)(2) order in this case.

H. Evidence of a Crime and Foreign Intelligence "Dual Purpose" Queries

At FBI, there are certain instances when a query has both a foreign intelligence and evidence of a crime purpose. These queries are referred to as "dual purpose" queries by FBI.[250] Guidance provided by FBI to its analysts notes that some investigations "regarding international terrorism, espionage, and malicious cyber activity by foreign powers concern both foreign intelligence and criminal activity" and associated queries commonly seek both foreign intelligence information and evidence of a crime.[251] FBI does not track how many queries are performed for a dual purpose or at what stage of investigative activity. Agents and analysts are trained to treat such queries as foreign intelligence queries, which need not meet requirements for evidence of a crime only queries.[252]

VI. Agency Implementation of the Query Procedures

A. Introduction

This section provides a focused review of the ways in which agencies implement their procedures and the policies, processes, and resources deployed to support that implementation.[253] Specific emphasis is placed on areas where policies or processes are different for queries conducted using query terms associated with U.S. persons or presumed U.S. persons.

This section will focus primarily on the querying policies and processes implemented by NSA and FBI. Over the years, NSA and FBI have experienced the greatest number of querying compliance challenges.[254] NSA has developed an internal compliance program that sets controls on the ways personnel may query Section 702-acquired information. FBI has deployed incremental mitigation strategies, but has had more compliance challenges, as discussed later in this Report.[255] As the only FISA agency with a dual intelligence and law enforcement mission, FBI's application of the querying procedures can be more complex than implementation by the

[250] Fed. Bureau of Investigation, Responses to May 4, 2022 Written Questions Submitted by PCLOB to FBI, at 14 (Sept. 9, 2022).

[251] Fed. Bureau of Investigation, FBI FISA Query Guidance, at 3 (March 17, 2022).

[252] (U) Fed. Bureau of Investigation Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Feb. 17, 2023). Dual purpose queries would not trigger the Section 702(f)(2) order requirement, which applies to evidence of a crime only queries conducted in connection with a predicated criminal investigation unrelated to national security.

[253] *See*, *e.g.*, 27th AG SAR, *supra*; 26th SAR, *supra*; 25th Joint Assessment, *supra*.

[254] *See generally* NSA, OVSC1203: FISA Section 702 Training, *supra*; 2021 NSA Querying Procedures, *supra*; NSA DCLPO Report, *supra*, at 6-7.

[255] *See*, *e.g.*, Apr. 21, 2022 FISC Opinion and Order, *supra*, at 23-49.

other agencies.[256] In addition, because FBI has a domestic focus, its personnel are more likely to conduct U.S. person queries than personnel at other agencies.[257] FBI's mission and its impact on how FBI implements the Section 702 program is further discussed in Part 4 of this Report.

By contrast to NSA and FBI, CIA and NCTC have consistently demonstrated high levels of compliance with their respective querying procedures and conduct relatively few U.S. person queries.[258] Further, neither of these agencies maintain unique or nuanced query authority. However, where further discussion of the policies and procedures implemented by these agencies is relevant to later analysis or recommendations, CIA and NCTC practices will be noted.

B. Conducting Queries at NSA

1. *History and the Query Standard*

NSA's querying procedures allow NSA to conduct queries into unminimized Section 702-acquired content and noncontent that is reasonably likely to retrieve foreign intelligence information.[259] NSA first obtained the authority to conduct U.S. person queries into downstream collection in 2011, but was not permitted to query upstream collection using U.S. person identifiers until 2017.[260] Today, NSA's querying procedures permit NSA to query all unminimized Section 702 collection using U.S. person and non-U.S. person terms without distinguishing between types of collection.[261]

2. *Training and Access*

In order to maintain access to unminimized Section 702-acquired information, NSA personnel must have a mission need and must complete annual Section 702 training.[262] NSA's training pertaining to querying is designed to identify the guidelines, procedures, and assistive

[256] CY2022 ASTR, *supra*, at 22.

[257] *Id.*

[258] *See generally* NSA, OVSC1203: FISA Section 702 Training; Response from Nat'l Sec. Agency to Priv. and C.L. Oversight Bd. (Oct. 2022); 2021 NSA Querying Procedures, *supra*; NSA DCLPO Report, supra, at 6-7.

[259] 2021 NSA Querying Procedures, *supra*, at 3-4. CIA and NCTC maintain the same standard.

[260] Nat'l Sec. Agency, Responses to PCLOB requests numbered 5, 11, 12.a, 13, 14, and 16 (dated August 30, 2022), at 2 (Oct. 14, 2022). The prohibition on conducting U.S. person queries in upstream data stemmed from NSA's collection of upstream "abouts" communications, which were at greater risk of containing wholly domestic communications. With the end of "abouts" collection in 2017, this prohibition was lifted and NSA was permitted to conduct U.S. person queries of all its Section 702 collection.

[261] Id.

[262] *Id.* at 2-3.

resources for conducting compliant queries.[263] Failure to complete this annual training in a timely manner results in a suspension of access, including a suspension of the ability to query and retrieve or review query results acquired from Section 702.[264] "NSA leverages a series of interconnected credential systems to grant (or deny) access to various systems and data held within NSA's SIGINT" collection.[265]

3. *Pre-Query Due Diligence and Approvals*

Prior to querying unminimized Section 702 datasets, NSA analysts must conduct pre-query due diligence to determine necessary requirements and additional steps.[266] NSA personnel are required to obtain approval prior to conducting queries of Section 702-acquired information for the following types of queries: (a) all U.S. person queries of Section 702-acquired content; and (b) "sensitive queries."

a. U.S. Person Queries

For example, NSA analysts are encouraged to conduct research in other non-FISA datasets to determine if query terms are associated with a U.S. person.[267] If the query terms are associated with a U.S. person, prior to running the query of unminimized Section 702 data, the analyst would be required to record the query terms associated with a U.S. person and provide a statement of facts establishing that any queries conducted using such terms would be reasonably likely to retrieve foreign intelligence information.[268] Prior to performing queries of Section 702-acquired content constituting sensitive queries under NSA's Enhanced Safeguard Query Policies, the request must be routed through and approved by Compliance for Cybersecurity and Operations as well as OGC. The request must then be routed to and approved by at least one level of internal leadership.[269] Other U.S. person query terms must be approved by NSA's OGC prior to use. U.S. person query terms are approved for use for a maximum duration of one year and may be renewed.[270] However, changes to circumstances or the query justification may necessitate

[263] NSA, OVSC1203: FISA Section 702 Training, *supra*, at 1.

[264] Responses to PCLOB requests numbered 5, 11, 12.a, 13, 14, and 16 (dated August 30, 2022), *supra*, at 2-3.

[265] *Id.*

[266] NSA, OVSC1203: FISA Section 702 Training, *supra*, at 45.

[267] *Id.* at 10.

[268] 2021 NSA Querying Procedures, *supra*, at 3-4.

[269] Nat'l Sec. Agency, Compliance Target Validation Standard Operating Procedure: USP Query tool, at 10 (Aug. 25, 2021).

[270] *Id.* at 8.

renewed review and approval prior to expiration of the prevailing approval. U.S. person queries against metadata generally do not require OGC approval.[271]

Documenting the query terms and associated justification is also required prior to conducting non-U.S. person queries of Section 702.[272] Analysts are trained to be specific and use facts associated with the individual or circumstances to justify the query.[273] Additionally, analysts must design the query using appropriate BOOLEAN logic and/or defeats to ensure the query returns relevant and focused results.[274]

b. Sensitive Queries

For certain U.S. person queries, NSA applies Enhanced Safeguard Query Policies.[275] NSA has been able to conduct U.S. person queries in Section 702 since 2011, and following the suspension of upstream "abouts" collection in 2017, NSA obtained permission to run U.S. person queries in upstream collection as well. In 2018, NSA leadership began developing rules to govern particular types of sensitive queries, which were formalized into NSA's Enhanced Safeguard Query Policies. The policies cover queries that are otherwise permitted under NSA's procedures and policies, but still deemed to be sensitive and thus requiring elevated approval. This policy requires analysts to apply enhanced safeguards procedures to certain U.S. person queries of Section 702-acquired information. Queries falling into this category require heightened approvals and are approved for shorter periods of time.[276]

The Enhanced Safeguard Query Policies require various levels of approval for certain U.S. person query terms. Depending on the particular category, review and approval is required by various offices and officials including the NSA Office of General Counsel, NSA Office of Compliance, and NSA Directorate.[277]

NSA determined the core of these professions and organizations are integral to the exercise of First Amendment protected rights and the protection of our democratic political system, thus demanding higher levels of scrutiny. NSA Compliance Group has promulgated a training

[271] NSA, OVSC1203: FISA Section 702 Training, *supra*, at 27. The Enhanced Safeguard Query Policy was established in 2019 pursuant to NSA Policy 2019-02.

[272] *Id.* at 25-26.

[273] *Id.* at 26.

[274] *Id.*

[275] *Id.*

[276] Nat'l Sec. Agency, Annex A to the Enhanced Safeguards Query Table (Apr. 6, 2022).

[277] *Id.*

pertaining to sensitive queries and tracks all such queries and their approvals.[278] However, NSA has not provided further guidance on its methodology.[279]

4. *Conducting the Query and Retrieving Results*

Queries may be conducted using a single query term or multiple query terms, including permutations of terms. There is no limit to the number of terms that may be included in a single query action, though each and every term must be supported by a proper purpose and justification.[280] NSA does not restrict the analyst's ability to review query results, so long as the analyst maintains proper clearance, a mission need, and has completed the required trainings. NSA does not track the number or type of responses received from a particular query.[281]

5. *Post-Query Due Diligence*

NSA delivers all relevant records associated with approved U.S. person query terms to DOJ and ODNI as part of a bimonthly oversight review process.[282] This includes, but is not limited to, query terms, identifiers, justifications, and any required approvals.

C. Conducting Queries at FBI

1. *History and the Query Standard*

The language used to articulate the query standard currently set forth in FBI's Section 702 querying procedures has evolved over time. Prior to 2018, the standard codified in FBI's minimization procedures (where querying rules were discussed prior to the adoption of independent querying procedures) was, "[t]o the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime."[283] As noted in Part 2 of this Report, this language was interpreted differently by FBI than the querying standard documented in the current querying procedures. In 2015, DOJ represented during a hearing before the FISC that queries must be

[278] *See* Nat'l Sec. Agency, iAgree Training, USP Queries in SIGINT Requiring Enhanced Safeguards (May 5, 2022) [hereinafter NSA Training, USP Queries].

[279] Call from Nat'l Sec. Agency to Priv. and C.L. Oversight Bd. Staff (Oct. 17, 2022).

[280] These multi-term queries may be conducted at all agencies; in addition, FBI has the ability to run "batch jobs," which are described elsewhere in this Report. The query terms may be entered individually by personnel or, to gain efficiencies, may be uploaded from a spreadsheet or other document. Multi-term queries with a significant number of query terms, such as a list of potential victims of a cyber intrusion, generally employ the latter method.

[281] Responses to PCLOB requests numbered 5, 11, 12.a, 13, 14, and 16 (dated August 30, 2022), *supra*, at 4.

[282] NSA, OVSC1203: FISA Section 702 Training, *supra*, at 27.

[283] 2021 FBI Minimization Proceduresm, *supra*, at 11.

"reasonably likely" to return foreign intelligence information or evidence of a crime, but did not adopt that language in its procedures until 2018.[284]

2. *Training and Access*

Prior to gaining access to unminimized Section 702-acquired information, FBI personnel must demonstrate a need for access to FISA information to perform their official duties or assist in a lawful and authorized government function.[285] Personnel must complete training regarding the proper implementation of FISA, including Section 702, and FBI's relevant policies and procedures.[286] As of late 2021, FBI personnel must also complete annual query-specific training in order to maintain access, and ad hoc training or guidance may be provided or required pursuant to the identification of individual compliance incidents or systemic compliance challenges.[287]

3. *Pre-Query Approvals and Requirements*

In general, FBI does not require consultation or approval prior to querying unminimized Section 702-acquired information. There are, however, certain categories of queries that have resulted in compliance challenges and have, consequently, been designated by FBI for heightened review as a matter of policy. These categories involve: (a) "batch job queries" and (b) queries involving Sensitive Investigative Matters, or "sensitive queries."

a. Batch Job Queries

All agencies maintain the technical capability to run multi-term searches.[288] In addition, FBI has a technological tool to run "batch job queries." A batch job query is one in which multiple query terms are run as part of a single query action, pursuant to the same justification.[289] FBI's FISA Query Guidance states that each query must independently satisfy the query standard.[290] The query terms used in batch job queries may be entirely distinct from one another, such as a series

[284] U.S. Dep't of Just., Off. of the Inspector Gen., Audit of the Roles and Responsibilities of the Federal Bureau of Investigation's Office of the General Counsel in National Security Matters, at 23 (2022), https://oig.justice.gov/sites/default/files/reports/22-116.pdf [hereinafter DOJ OIG Audit].

[285] 2021 FBI Minimization Procedures, *supra,* at 15.

[286] *Id.* at 14-15.

[287] FBI FISA Query Training, *supra*.

[288] These are searches that run multiple query terms at once.

[289] CY2021 ASTR, *supra,* at 20.

[290] FBI FISA Query Guidance, *supra,* at 6.

of email addresses, or they may be different types of terms or use alternate spellings.[291] The batch job query function allows personnel to run queries involving large numbers of query terms, and FBI asserts that they are helpful when analysts need to perform a significant amount of lead generation or identify connections in collected data.[292] A common example of a batch job query involves a contact list for a target (e.g., John Terrorist's phonebook), where an analyst would like to see if any of the target's phone contacts are referenced in Section 702-acquired information. However, a batch job query may also result in different combinations of the same terms or alternate spellings. For example, the user might run Al Qaeda as one query term, Al-Qaeda as a second query term, and Al Qaida as a third query term.

The following is an example of an FBI batch job query that was found to both be compliant with the querying procedures and operationally valuable to FBI:

- Since 2021, FBI has been conducting a national security cyber investigation into a Russian-government affiliated ransomware actor responsible for multiple international computer intrusions. FBI personnel identified a set of approximately twenty-one phone numbers associated with these intrusions,[293] which, when combined with other identifiers, resulted in more than 100 query terms. A batch job query of these terms led to the identification of three individuals with potential links to Russian Intelligence Services.[294]

In a batch job query, each query term counts as a separate query for the purposes of query counting and compliance reporting.[295] Additionally, because each batch job query is given a single U.S. person query term label, either U.S. person or non-U.S. person, if any of the query terms used in a batch job query are identified as a U.S. person query term, all terms in the batch will carry that label, thus potentially resulting in an over-counting of U.S. person queries.[296]

Pursuant to FBI policy established in June 2021, but not delineated in the statute or querying procedures, FBI users must obtain attorney approval to conduct batch job queries

[291] CY2021 ASTR, *supra*, at 20. Because a batch job query may include queries using different combinations, a batch job query may include fewer than 100 terms but result in 100 or more queries due to the various combinations.

[292] Responses to May 4, 2022 Written Questions Submitted by PCLOB to FBI, *supra*, at 10-11.

[293] Thus, FBI assessed that the phone numbers were reasonably believed to be used by Russian-government linked hackers and that these query terms were reasonably likely to retrieve foreign intelligence and/or evidence of a crime from Section 702-acquired information.

[294] Response from Fed. Bureau of Investigation to Priv. and C.L. Oversight Bd. Staff (Jan. 27, 2023).

[295] CY2021 ASTR, *supra*, at 20.

[296] *Id.* at 21.

resulting in 100 or more query terms.[297] The government asserts that the batch job query threshold was designated to provide heightened review for queries with the greatest potential to impact the privacy of multiple U.S. persons.[298] Over the last several years, some of the more significant compliance incidents have been those related to batch job queries.[299] Since FBI's attorney approval requirement, however, all FBI batch job queries of 100 or more query terms have been compliant. [300] Nonetheless, in June 2023, FBI began requiring attorney pre-query approval to conduct batch job queries of any size. Because batch job queries rely on a single purpose, design, and justification, if a single batch job query consists entirely or largely of noncompliant queries it can result in hundreds or thousands of improper queries.[301]

b. Sensitive Queries

In March 2022, FBI issued its Sensitive Query Guidance, which established guidelines for internal approval of "sensitive queries," which involve categories of queries that are similar to Sensitive Investigative Matters as defined in FBI's DIOG. Pursuant to a DOJ mandate, FBI established this policy in response to a series of noncompliant queries of Section 702-acquired information involving public officials and members of the news media.[302] FBI's Sensitive Query Guidance is similar to NSA's Enhanced Safeguard Query Policies, but among other differences,

[297] June 2023 Joint Statement to Senate Judiciary, *supra,* at 11 (joint statement of Chris Fonzone, Gen. Couns., Off. of the Dir. of Nat'l Intel., et al.). Since FBI's attorney approval requirement was instituted, however, none of the batch job queries that received attorney approval were found to be noncompliant.

[298] FBI FISA Systems Briefing, *supra*.

[299] 25th Joint Assessment, *supra,* at 55.

[300] June 2023 Joint Statement to Senate Judiciary, *supra,* at 11 (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

[301] 25th Joint Assessment, *supra,* at 55.

[302] For example, in 2021, following an audit of an FBI field office, DOJ reported a noncompliant batch job query that involved the names of over 19,000 donors to a congressional campaign, most of whom were U.S. persons. These queries, which were run against information acquired under FISA provisions other than Section 702, were found to be noncompliant with the FISA query standard. The FBI analyst who conducted the queries was not able to articulate why each individual name would likely be found in FISA-acquired information, resulting in thousands of queries that were not supported by a sufficient justification. 27th AG SAR, *supra,* at 115-16.

FBI's policy on sensitive queries requires various levels of approvals for certain types of queries of raw FISA-acquired information, such as terms covering certain political and religious officials, members of academia, and members of the media.

FBI's policy is not specific to U.S. person queries.[303] FBI's policy on sensitive queries requires various levels of approvals for certain types of queries of raw FISA-acquired information, such as terms covering certain political and religious officials, members of academia, and members of the media. Depending on the particular category, review and approval is required by various offices and officials including Chief Division Counsel, the FBI National Security Law Branch Section Chief, and the FBI Deputy Director. [304]

Prior to running such a query, FBI personnel must indicate in the system whether the query is sensitive, and, if so, whether they have obtained pre-approval to run the query.[305] FBI National Security and Cyber Law Branch (NSCLB) has promulgated a detailed training regarding sensitive queries, including answers to common questions.[306] Neither CIA nor NCTC have issued policies regarding the handling of sensitive queries. However, CIA is in the final stages of implementing a sensitive query policy and NCTC is working to develop one as well.

4. *Conducting the Query*

When initiating a query, FBI personnel often use a single system to query multiple datasets, including information obtained through unminimized Section 702, other provisions of FISA, and other sources. Historically, when conducting such queries systems defaulted to automatically include all FISA datasets to ensure all potentially relevant information was identified, meaning FBI personnel were required to opt-out of Section 702 datasets when their query did not meet the appropriate standard.[307] However, queries of datasets are not all subject to the same query standard. The FISA query standard is a heightened standard compared to the standard for querying

[303] Fed. Bureau of Investigation, Sensitive Query Guidance (Mar. 22, 2022) [hereinafter FBI Sensitive Query Guidance].

[304] *Id.*

[305] *Id.*

[306] *Id.*

[307] Fed. Bureau of Investigation, Attachment C—List of Significant Changes to FBI Section 702 Program, at 2 (Sept. 9, 2022). This system design was initially motivated by a desire to mitigate the likelihood that FBI personnel would fail to opt in when querying the federated system and miss significant threat info.

certain other non-FISA datasets and, therefore, more difficult to satisfy. FBI and DOJ identified that a number of query incidents were occurring because personnel did not realize their queries would run against unminimized FISA datasets and did not consider the heightened standard before querying. For this reason, in summer 2021, FBI modified its systems so the default setting is to not include Section 702 datasets.[308] FBI personnel must now affirmatively opt in to have their queries run against Section 702 datasets.[309]

After opting in to Section 702 datasets, personnel must designate whether the query will use any query terms that reasonably identify one or more U.S. persons or, in circumstances when there are facts indicating that a query term likely identifies a U.S. person, but it cannot be determined with certainty, a presumed U.S. person.[310]

While FBI personnel must conduct the query for an authorized purpose and possess a sufficient justification, there is no requirement, outside the two pre-approval requirements noted above, that they document the purpose or justification or consult with peers or supervisors prior to conducting the query. As discussed further below, documentation is only required in certain circumstances before accessing and reviewing the contents of communications retrieved by a query. However, as of the summer of 2023, FBI announced plans to incorporate a requirement that personnel enter a written justification for all U.S. person queries prior to conducting the query.[311] Further, like NSA analysts, FBI personnel must design the query using appropriate BOOLEAN logic and/or limiters (e.g., confining the dataset queried to a particular FBI investigation or account).

5. *Retrieving Results*

For non-U.S. person queries, FBI personnel may retrieve and review any results without further consultation or restriction and, except in limited circumstances, they are generally not required to document the purpose of or justification for the query.[312] If results are retrieved in response to a U.S. person query against Section 702-acquired information and personnel would like to review the results, they must document a justification and designate whether the purpose of

[308] *Id.*

[309] According to FBI, this change, along with other changes, led to a drop of more than 95% in U.S. person queries run against Section 702 datasets in 2022 versus 2021. *See, e.g.*, CY2022 ASTR, *supra*, at 24.

[310] *See, e.g.*, Fed. Bureau of Investigation, Attachment A: Screenshots (Sept. 9, 2022).

[311] Section 702 of the Foreign Intelligence Surveillance Act, *supra*, at 22.

[312] FBI personnel are required to document the purpose of or justification for queries of non-U.S. person query terms when they involve sensitive queries, are part of a batch job query, or are requested to by oversight entities.

the query is solely to retrieve evidence of a crime.[313] If the U.S. person query is solely to retrieve evidence of a crime and is conducted pursuant to a predicated criminal investigation that is unrelated to national security,[314] personnel must consult with an NSCLB attorney and request and obtain a Section 702(f)(2) order from the FISC prior to accessing the contents of communications that were retrieved pursuant to the query, except in the event of an emergency.[315] To date, FBI has never requested or obtained a Section 702(f)(2) order from the FISC.[316] However, as discussed above, in 2021 and 2022 combined, there were at least six instances in which FBI personnel failed to seek a Section 702(f)(2) order before accessing query results even though a Section 702(f)(2) order was required. These instances were reported as Section 702(f)(2) compliance incidents to the FISC and in ODNI's Annual Statistical Transparency Report.[317]

6. *Exemptions and Exceptions to the Query Standard*

Although FBI retains records regarding queries that are considered exceptions to the query standard, FBI does not track metrics on them, nor does it maintain any records or metrics for searches that are exempted from the query standard. For example, FBI does not maintain any metrics concerning the number of queries conducted for training purposes or in response to a congressional request.[318]

7. *Use in Prosecutions of Information Identified Through U.S. Person Queries*

While the government keeps records that enable it to fulfill its notice obligations under Section 1806(c) and 1881e(a), and the government also keeps records of all U.S. person queries as required by Section 1881(f)(1), the government does not systematically track when or whether particular Section 702 information was identified through a U.S. person query. Thus, the government is unable to identify how many times it has used, as part of a criminal investigation or prosecution, evidence that was identified through a U.S. person query specifically. Nor is the government able to identify any instance in which it has used evidence identified through a U.S. person query in a criminal investigation or prosecution.

On nine occasions, the government has intended to use information obtained or derived from Section 702 collection in criminal trials in a manner that has triggered FISA's notice requirement (i.e., against an aggrieved party). In each of these nine instances, the government provided notice to the defendant(s) of the use of Section 702 information, but it has not provided

[313] 2021 FBI Querying Procedures, *supra*, at 4(a)(3).

[314] FBI guidance and training on Section 702(f)(2) instruct FBI personnel to consult with an FBI attorney if they are unsure as to whether their query meets each of the elements requiring a Section 702(f)(2) order.

[315] FBI FISA Query Training, *supra,* at 46-52.

[316] *See, e.g.*, CY2022 ASTR, *supra,* at 26.

[317] *See id.*

[318] Fed. Bureau of Investigation Briefing to Priv. and C.L. Oversight Bd. Staff (Sept. 29, 2022).

notice that evidence was retrieved through a U.S. person query. In response to defense filings in three of these cases, the government affirmatively asserted to the courts that no evidence relied upon was identified from U.S. person queries. Two cases involved defendants who were non-U.S. persons. The government does not assert, and has not identified, that any evidence in the remaining four cases was identified through a U.S. person query.

VII. Internal Agency Compliance Mechanisms

The implementation of Section 702 involves both internal agency compliance mechanisms and oversight as described in the next section of this Report. NSA, FBI, CIA, and NCTC have each developed an internal compliance program to oversee compliance with the targeting, minimization, and querying procedures discussed above.[319] Of the four, NSA and FBI have the largest internal compliance programs, as these agencies are responsible for acquiring certain types of data pursuant to Section 702 on behalf of the Intelligence Community.[320] These internal compliance programs also coordinate with a variety of oversight entities, which are described in the next section. For example, instances of noncompliance that are identified through these internal compliance programs are reported to DOJ and ODNI, who report these matters to the FISC and to Congress.[321]

A. NSA's Internal Section 702 Program

Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities.[322] NSA's Section 702 internal compliance program is jointly run by several agency entities, each with a focus on compliance, mission, legal, or privacy issues, respectively: NSA's Compliance Group, which provides the most granular oversight of the agency's implementation of Section 702; NSA's Authorities Integration Group, which advises mission personnel on how to apply NSA capabilities most effectively, including Section 702; NSA's OGC, which reviews pre-tasking information and other Section 702-related decisions to ensure they comply with various laws, policies, and internal agency guidance; and NSA's Civil Liberties, Privacy, & Transparency Office

[319] 25th Joint Assessment, *supra*, at A-7-A-15.

[320] As discussed herein, CIA and NCTC receive Section 702-acquired data from NSA and FBI. Where these internal compliance programs have areas for improvement, the Board discusses potential reforms in Part 5 of this Report.

[321] 26th Joint Assessment, *supra*, at iii-iv (noting that the semiannual report required by Section 702 is given to both Congress and the FISC and describes all identified incidents of noncompliance); 50 U.S.C. § 1881f(b)(1)(G) (requiring all incidents of noncompliance with the targeting procedures, minimization procedures, and Attorney General Guidelines, as well as any incidents of noncompliance by a provider, to be reported in the Section 707 report); U.S. FOREIGN INTEL. SURVEILLANCE CT., RULES OF PROCEDURE, at 5 (2010) [hereinafter FISC Rules of Procedure] (requiring incidents of noncompliance to be reported to the FISC).

[322] *See* 25th Joint Assessment, *supra*, at A-7-A-8.

(CLPT), which provides policy reviews similar to OGC from the privacy and civil liberties perspective and is responsible for the public transparency activities related to the authority.[323]

NSA's Compliance Group, part of the agency's Engagement & Policy Directorate,[324] focuses on both preventative and detective controls.[325] NSA's Compliance Group maintains several groups focused on Section 702 compliance, including the Office of Compliance for Cybersecurity and Operations and the Office of Compliance for Capabilities.[326] NSA's Office of Compliance for Cybersecurity and Operations is primarily focused on *individual* Section 702 compliance: counseling the operational workforce on how to leverage NSA's authorities in a way that safeguards the rights of U.S. persons; alerting NSA personnel of factors that may make their Section 702 targets ineligible for tasking; investigating individual incidents of noncompliance; and ensuring compliant implementation of NSA's Section 702 program.[327] NSA's Office of Compliance for Capabilities is more focused on *systemic* Section 702 compliance: certifying that systems and analytics meet existing compliance requirements; deploying forward-looking system controls that help prevent, detect, and address incidents as quickly as possible; and investigating systematic compliance incidents.[328] The Section 702 compliance-related approvals and reviews conducted by NSA's Compliance Group include: (a) pre-query approval of all sensitive queries; (b) establishing post-query review through either active or passive processes; (c) post-tasking review of all targeting decisions; and (d) reviewing a sample of disseminations implicating Section 702-acquired information.[329] NSA's Compliance Group has a team of compliance personnel available as needed 24 hours a day, seven days a week for any compliance-related questions.[330]

[323] *See* Nat'l Sec. Agency Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Oct. 17, 2022). According to NSA, NSA's Risk Management Office, NSA's Cybersecurity Policy Group, and NSA's Office of Inspector General also contribute to the agency's Section 702 internal compliance program.

[324] Prior to a 2016 re-organization, NSA compliance functions were performed by the Office of the Director of Compliance and compliance-focused organizations integrated into various directorates.

[325] *See generally* 25th Joint Assessment, *supra*, at A-7-A-8.

[326] Nat'l Sec. Agency, Classified Website, *Compliance* (last visited July 31, 2023).

[327] Nat'l Sec. Agency, Classified Website, *Compliance, Compliance for Cybersecurity and Operations (P75)* (last visited July 31, 2023).

[328] Nat'l Sec. Agency, Classified Website, *Compliance, Compliance for Capabilities (P76)* (last visited July 31, 2023).

[329] 25th Joint Assessment, *supra*, at A-7; Nat'l Sec. Agency Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Oct. 17, 2022).

[330] (U) Nat'l Sec. Agency Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Oct. 17, 2022).

NSA's Compliance Group also conducts periodic risk assessments to assess the risk of noncompliance with the rules designed to protect privacy and safeguard information.[331]

The NSA OGC reports to the Department of Defense General Counsel, and is composed of more than 100 attorneys who function in a manner comparable to in-house counsel.[332] Among other things, these attorneys help ensure the agency executes its mission with adherence to the U.S. Constitution and compliance with various U.S. laws.[333] As part of its role in overseeing the agency's implementation of Section 702, NSA OGC advises on and reviews certain Section 702-related targeting, minimization, and querying decisions to ensure they comply with FISA, the Section 702 procedures, and other legal parameters.[334] NSA OGC's Section 702-related tasks include reviewing agency Section 702 training and reviewing U.S. person query terms before they may be used to conduct queries of Section 702-acquired content, including sensitive queries.[335]

NSA CLPT was established in 2014 in the aftermath of the initial Snowden disclosures to provide an additional civil liberties and privacy perspective within all of NSA's programs, including its foreign intelligence programs.[336] Several NSA CLPT functions already existed within NSA, but the assignment of a Director of Civil Liberties, Privacy, and Transparency helped ensure that privacy and civil liberties considerations would be a priority for strategic agency decisions. In 2018, NSA CLPT added transparency to its portfolio due to increased Intelligence Community focus on transparency as a foundational element for securing public trust. As part of its role in overseeing the agency's implementation of Section 702, NSA CLPT reviews Section 702-related policies and procedures through a civil liberties and privacy policy lens.[337] For example, NSA CLPT employs approximately six to twelve privacy-trained professionals to evaluate whether individual and systemic applications of the Section 702 authority adequately protect the privacy rights of U.S. persons and whether the agency is being appropriately transparent regarding how it implements the program.[338]

---

[331] 25th Joint Assessment, *supra*, at A-8.

[332] Nat'l Sec. Agency, *General Counsel Overview*, https://www.nsa.gov/Culture/General-Counsel/Overview/ (last visited July 31, 2023).

[333] Id.

[334] *See, e.g.*, 2021 NSA Targeting Procedures, *supra*, at 4; 2021 NSA Minimization Procedures, *supra*, at 10; 2021 NSA Querying Procedures, *supra*, at 3.

[335] *See* 26th Joint Assessment, *supra*, at 9; 2021 NSA Querying Procedures, *supra*, at 3-4.

[336] Nat'l Sec. Agency, *Civil Liberties & Privacy Overview*, https://www.nsa.gov/Culture/Civil-Liberties-and-Privacy/Overview/ (last visited July 31, 2023).

[337] Call from Nat'l Sec. Agency to Priv. and C.L. Oversight Bd. Staff (Oct. 17, 2022).

[338] Id.

All of these NSA entities contribute to a Section 702 internal compliance program that involves internal training programs, access control procedures, standard operating procedures, and compliance incident reporting measures.[339] For example, only authorized personnel are granted access to Section 702-acquired information in NSA systems.[340] In order to be granted access, these personnel must complete an annual comprehensive training program as approved by NSA OGC and NSA's Compliance Group; review the targeting, minimization, and querying procedures as well as other documents filed with the certifications; and pass a competency test.[341] For guidance, personnel are instructed to consult NSA's Section 702 standard operating procedures, supervisors, NSA's Compliance Group, or NSA OGC, and personnel must receive remedial training if human error contributes to any compliance incidents.[342] NSA has also established a standardized process for incident tracking and reporting to DOJ and ODNI.[343] NSA Compliance Group compliance officers work with NSA analysts and CIA and FBI points of contact, as necessary, to compile incident reports that are forwarded to NSA OGC, who then forward the incidents to DOJ and ODNI.[344]

B. FBI's Internal Section 702 Program

As the second agency with Section 702 targeting authority, FBI's Section 702 internal compliance structure also has several components, and it has been restructured several times.[345] FBI's Section 702 internal compliance program is jointly run by FBI's Office of Integrity and Compliance (FBI OIC);[346] FBI's Inspection Division (FBI INSD);[347] FBI OGC; FBI NSCLB; and, as of recently, FBI's Office of Internal Auditing (FBI OIA). Operational and technical entities like FBI's Technology and Data Innovation Section (FBI TDI), which processes requests from NSA, and FBI's Operational Technology Division, which coordinates with ECSPs to facilitate the actual acquisition, also contribute to FBI's Section 702 internal compliance program. FBI's Privacy and Civil Liberties Unit provides privacy policy analysis regarding Section 702 programmatic decisions, and hands-on legal guidance is provided by attorneys embedded at each

[339] 25th Joint Assessment, *supra*, at A-7.

[340] *Id.*

[341] *Id.*

[342] *Id.*

[343] *Id.*

[344] *Id.*

[345] *See* DOJ OIG Audit, *supra*.

[346] FBI OIC performs risk assessment and management by identifying and addressing potential systemic compliance risks in FBI systems.

[347] FBI INSD evaluates agency compliance with internal FBI policies.

of the field offices. In addition, FBI has created certain inter-divisional working groups—the Compliance Trends Analysis Group (CTAG) and the Training Working Group—in an effort to enhance compliance by leveraging the expertise of various internal offices.[348]

FBI NSCLB is comprised of approximately seventy attorneys who advise clients on national security and cyber law matters, including both operational and programmatic issues.[349] In 2019, FBI created the NSCLB Strategic Projects Law Unit (NSCLB SPLU), a small unit of about six attorneys, to focus on programmatic issues and trends in FBI national security compliance matters, including Section 702.[350] NSCLB reports incidents of noncompliance to DOJ and ODNI, and coordinates with oversight entities for compliance reviews.[351]

Although several FBI entities are involved in internal compliance review of the agency's Section 702 program, the majority of FBI's compliance review has been done by DOJ and ODNI.[352] As a result, most of FBI's compliance incidents have been discovered through audits by oversight entities rather than through internal compliance review. In 2020, the Attorney General issued a memorandum directing FBI to establish an Office of Internal Auditing (FBI OIA) to further supplement the work being done by the DOJ National Security Division (NSD) and to apply auditing processes to FBI's national security activities.[353] In 2021 and 2022, FBI OIA performed its first two audits of queries performed in FBI systems of, among other information, unminimized

[348] Fed. Bureau of Investigation Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Oct. 26, 2022); 25th Joint Assessment, *supra*, at A-14.

[349] Until 2016, NSCLB had a Compliance, Oversight, and Training Unit; a Policy & Legislative Review Unit; and a Classified Litigation Support Unit; which provided centralized offices for compliance, policy, and litigation matters, respectively. In a 2016 re-organization of NSCLB, FBI disbanded these three specialized units and spread compliance work across the NSCLB operational units.

[350] *See* DOJ OIG Audit, *supra*. Within NSCLB, SPLU has a special focus on training, legislative review, and compliance matters.

[351] *See* 25th Joint Assessment, *supra*, at A-14.

[352] *See id.* at 12.

[353] Memorandum from William Barr, Att'y Gen., to the Deputy Att'y Gen. et al., "Augmenting the Internal Compliance Functions of the Federal Bureau of Investigation," at 1 (Aug. 31, 2020) ("A robust internal compliance program is critical to ensure faithful compliance with the laws, policies, and procedures that govern agency activities." . . . "[R]igorous and robust auditing . . . is an essential ingredient to an effective compliance regime"); *see also* DOJ OIG Audit, *supra*; Attachment C—List of Significant Changes to FBI Section 702 Program, *supra*. FBI INSD focuses on FBI's compliance with internal policies. Historically, it conducted audits of FBI's compliance with the Section 702 targeting procedures, but this responsibility will be assumed by OIA. In addition, FBI's Senior Advisor for National Security Oversight and Compliance, which was a position created in 2021 at the direction of DOJ, also provides advice to FBI leadership on issues and resourcing needs to accomplish reforms and better position FBI to prevent, detect, and remedy national security compliance risks, as well as ensuring coordination amongst the FBI entities involved in internal compliance.

Section 702-acquired information.[354] OIA plans on performing other Section 702 auditing, such as reviews of compliance with FBI's Section 702 Targeting Procedures, and continues to develop the structure of its auditing processes.[355]

The above-described FBI entities contribute to a Section 702 internal compliance program that involves internal training, access control, and compliance incident reporting.[356] For example, FBI's Training Working Group includes representatives from FBI NSCLB, FBI OIA, FBI OIC, and FBI's Privacy and Civil Liberties Unit, among others, to assess the efficacy of training on national security legal authorities and issue recommendations on improvement.[357] Only authorized personnel who have received Section 702 training may be provided access to unminimized Section 702-acquired information in FBI systems.[358] In addition, hands-on training and supervision are provided to FBI personnel at the field office level.[359] All 56 FBI field offices have a Chief Division Counsel, and many field offices have at least one Associate Division Counsel.[360] These individuals are trained on the legal requirements of Section 702, and FBI personnel are instructed to contact them for guidance on compliance with the procedures.[361] For example, as discussed previously,

[354] Attachment C—List of Significant Changes to FBI Section 702 Program, *supra*. According to FBI, the goal of the audit was to verify that querying was done in compliance with laws, Court-approved procedures, and policies, identify any patterns of noncompliance, and develop recommendations to improve compliance going forward. The 2021 OIA audit examined approximately 2,321 queries of unminimized FISA information, including Section 702, that were conducted over a 12-month period by FBI personnel at various field offices and at FBI Headquarters. According to FBI, the sample of queries was designed to include queries assessed to be at the highest risk of noncompliance. Within this sample size, OIA and DOJ jointly identified 286 noncompliant queries, of which 162 were potentially noncompliant with the FBI querying procedures. DOJ is continuing to investigate whether other queries were noncompliant with the FBI querying procedures, including whether certain queries conducted for evidence of a crime only were subject to the court order requirement in 50 U.S.C. § 1881a(f)(2). OIA's first audit established a baseline against which future audits can be compared but did not result in a final report. In mid-2022, OIA began a second audit of queries of raw FISA information, including Section 702 information. OIA's second audit examined 558 queries conducted over a 12-month period with the goal of evaluating whether FBI's recent query compliance mitigation strategies are resulting in improved query compliance. In May 2023, OIA released its final report on the results of these two audits. OIA's first audit found that 82% of FBI queries of Section 702 datasets were compliant with the query standard; OIA's second audit found that 96% of FBI queries of Section 702 datasets were complaint. Of the 558 queries reviewed in OIA's second audit, 446 queries searched against raw Section 702 collection, in addition to searching raw traditional FISA collection. 64% of the 446 queries of raw Section 702 collection were marked as concerning a U.S. person or presumed U.S. person.

[355] *Id.* FBI's compliance with the Section 702 targeting procedures has previously been audited by FBI INSD.

[356] 25th Joint Assessment, *supra*, at A-14.

[357] This training working group has consulted with NSA and CIA in an effort to benchmark FBI training.

[358] 25th Joint Assessment, *supra*, at A-14.

[359] *E.g.*, FBI FISA Query Training, *supra*.

[360] DOJ OIG Audit, *supra*, at 1-2.

[361] FBI FISA Query Training, *supra*, at 59.

in 2022, FBI began requiring attorney pre-approval of all batch job queries using 100 or more query terms, and senior executive service pre-approval of all sensitive queries.[362] These approvals are usually granted at the field office level, but may be granted by NSCLB, or may require FBI Deputy Director approval.[363]

C. CIA's Internal Section 702 Program

As discussed previously, CIA does not target or collect communications pursuant to Section 702.[364] Like FBI and NSA, CIA personnel may nominate a potential Section 702 target to NSA.[365] If CIA receives unminimized Section 702-acquired communications, either through a nomination or a dual-routing request, CIA must apply its Section 702 minimization and querying procedures to the information.[366]

CIA's Section 702 internal compliance program is jointly run by two agency entities: CIA's FISA & SIGINT Office (CIA FSO) and CIA's Office of General Counsel (CIA OGC).[367] CIA FSO provides granular oversight of the agency's compliance with Section 702; CIA OGC provides specific legal counsel when novel legal questions arise, such as with the Section 702 certification process, or specific targeting, querying, retention, or dissemination decisions.[368]

As part of its role in overseeing the agency's implementation of Section 702, CIA FSO provides day-to-day counsel on operational FISA matters, including ensuring that all Section 702 collection is properly minimized and that agency personnel are properly trained and complying with all minimization and querying requirements.[369] The office also provides strategic direction and policy on the management of Section 702 data, and coordinates with oversight entities, including DOJ and ODNI.[370]

CIA's Section 702 internal compliance program is primarily focused on nominating, minimization, and querying targets. Nominations submitted by an analyst are approved by a

[362] Attachment C—List of Significant Changes to FBI Section 702 Program, *supra*.

[363] *Id.*

[364] 25th Joint Assessment, *supra*, at A-8.

[365] *Id.*

[366] *Id.*

[367] (U) *Id.* at 14.

[368] *Id.* at A-9.

[369] *Id.*

[370] *Id.*

supervisor and CIA FSO prior to export to NSA.[371] In addition, disseminations of Section 702-acquired information require CIA FSO approval, and such disseminations of U.S. person information must also be approved by a CIA attorney.[372] Although it does not require internal review or approval of queries of Section 702-acquired information, the agency employs access controls and advisory services. For example, only authorized personnel who have received Section 702 training and authorizations are granted access to unminimized Section 702-acquired information in CIA systems.[373] Additionally, for guidance, personnel are instructed to consult CIA OGC attorneys who are embedded with operational elements. These attorneys are also responsible for reporting compliance incidents to DOJ and ODNI.[374] Finally, CIA's Office of Privacy and Civil Liberties also reviews and oversees CIA's required FISA transparency reporting information, and compiles CIA's U.S. person masking and unmasking statistics.[375]

D. NCTC's Internal Section 702 Program

Unlike NSA, FBI, and CIA, NCTC neither directly engages in targeting and acquisition, nor does it nominate potential Section 702 targets to NSA.[376] NCTC is authorized, however, to receive dual-routed unminimized Section 702 data pursuant to the international terrorism certification only. NCTC has access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism.[377] NCTC's processing, retention, and dissemination of unminimized Section 702-acquired information is subject to NCTC's Section 702 minimization and querying procedures.[378] Commensurate with the size of its Section 702 operations, NCTC's internal Section 702 compliance program is the smallest of the four agencies, and is managed by NCTC's Compliance and Transparency Group (NCTC Compliance),[379] in coordination with NCTC Legal.[380]

[371] *Id.*

[372] Cent. Intel. Agency Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Feb. 2023).

[373] 25th Joint Assessment, *supra*, at A-9.

[374] *Id.* at A-10.

[375] Cent. Intel. Agency, Supplemental Response to Accuracy Review (Jan. 2023).

[376] 25th Joint Assessment, *supra*, at A-14.

[377] *Id.* at A-10.

[378] *Id.*

[379] NCTC Compliance is within NCTC's Office of Enterprise Services.

[380] 25th Joint Assessment, *supra*, at A-10.

NCTC Compliance provides strategic direction and internal compliance review for data handling and management of Section 702 data.[381] It also administers and implements NCTC Section 702 training; ensures that all unminimized Section 702-acquired information is properly routed, minimized, and disseminated; and assesses whether NCTC personnel are complying with the minimization and querying procedures.[382] In order to ensure compliance with the Section 702 querying and minimization procedures, on a monthly basis NCTC Compliance reviews query logs, covering 100 percent of queries performed against unminimized Section 702-acquired data, and reviews all Section 702 disseminations cables—i.e., cables that notify NSA, CIA, and FBI that NCTC has minimized raw Section 702-acquired information.[383] These reviews, along with spot checks to verify compliance with Section 702 storage rules, also enable NCTC Compliance to identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.[384] Finally, NCTC Compliance coordinates with oversight entities, including DOJ and ODNI, for bimonthly Section 702 compliance reviews.[385]

E. Internal Compliance Incident Reporting

Incidents of noncompliance with the Section 702 targeting, minimization, or querying procedures that are identified by any of these agencies' internal compliance programs (or otherwise self-identified) must be reported to DOJ and ODNI.[386] Because NSA's internal compliance program requires pre-query approvals and auditing, most reported incidents are identified by NSA analysts or by NSA's internal compliance program.[387] By contrast, because FBI's internal compliance program is not as established, most FBI compliance incidents (which are mostly related to querying, not minimization or targeting) are identified by oversight entities.[388] As discussed later in this Report, once a compliance incident is reported, these internal compliance programs are also involved in implementing remedial actions, such as purging, recalling tainted reports, deploying system updates, or retraining of personnel, as required.[389] The internal Section 702 compliance programs of the agencies responsible for Section 702 acquisition are also

[381] *Id.*

[382] *Id.* at 15.

[383] Nat'l Counterterrorism Ctr., NCTC Responses to Questionnaire of August 23, 2022, at 7-10 (Sept. 9, 2022).

[384] 25th Joint Assessment, *supra*, at A-10-A-11.

[385] *Id.* at A-10.

[386] *Id.* at iii-iv.

[387] *Id.* at 8.

[388] *See id.* at 3 (describing that DOJ's field office reviews have been responsible for discovering a significant portion of the FBI minimization and querying incidents).

[389] *Id.* at 46-47 (describing elements of the purge process).

responsible for conducting an annual review of the Section 702 program.[390] These reviews must report the number of disseminations of U.S. person identities made, the number of U.S. person identities that were subsequently unmasked, and the number of Section 702 targets that were subsequently determined to be located in the United States.[391] The reviews must also evaluate whether there is reason to believe that foreign intelligence information is being acquired under Section 702, as well as the adequacy of the minimization procedures and the application of those procedures to Section 702-acquired information.[392]

The Board's investigation has revealed that, for most of these individuals, ensuring compliance with the FISA authorities, including Section 702, is only one of their many responsibilities.

VIII. Oversight

Section 702 is also subject to oversight by various entities external to NSA, FBI, CIA, and NCTC, several of which were mandated by Congress when it first enacted Section 702 in 2008 and again when it reauthorized the program in 2018.[393] DOJ, ODNI, and the FISC have the primary responsibility for overseeing the Intelligence Community's implementation of the program.[394] The various agency Offices of the Inspector General, Government Accountability Office, and PCLOB have also played roles in oversight of surveillance conducted under Section 702. In addition, Congress conducts oversight of surveillance conducted under Section 702. The House and Senate Judiciary Committees serve as the primary committees of jurisdiction for FISA and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence conduct oversight over all Intelligence Community activities.

Section 702 requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to Section 702 and to submit such assessments to the FISC and relevant congressional committees at least once every six months.[395] To fulfill this requirement, a team of oversight personnel from DOJ and ODNI conduct compliance reviews to assess whether the authorities under Section 702 have been implemented in accordance with the

[390] 50 U.S.C. § 1881a(m)(3).

[391] *Id.*

[392] *Id.*

[393] *See id.* § 1881a(m).

[394] *See id.* The Board's investigation has shown that this oversight is primarily focused on constitutional, statutory, and FISC-approved procedural requirements; DOJ, ODNI, and the FISC are not as involved in the implementation of internal agency policies.

[395] *See id.*

Constitution, the statute, and the applicable procedures and guidelines.[396] As discussed below, any compliance incidents discovered during these reviews (or otherwise) are reported by DOJ to Congress, as well as to the FISC,[397] which uses individual and systematic compliance incidents to analyze agency implementation of the procedures and assess the need for programmatic changes.[398]

A. DOJ/ODNI Joint Oversight

DOJ and ODNI work together in complementary yet subtly different ways to oversee the implementation of the Section 702 program in tandem with the agencies' internal oversight programs. In general, PCLOB has observed that DOJ focuses more on legal compliance matters, ODNI focuses more on policy matters, and DOJ and ODNI work together to identify and address overarching trends. DOJ houses a section of approximately thirty attorneys and professional staff who generally focus on oversight of the Intelligence Community's application of FISA authorities, including Section 702. These attorneys are divided into teams that focus on particular agencies and on specific oversight activities. For example, there are individual teams that focus on NSA targeting decisions; NSA post-tasking incidents; FBI targeting and minimization decisions; FBI queries; and CIA and NCTC minimization and querying decisions. Any novel questions of law may also be addressed to a separate legal policy office in DOJ, which provides additional legal analysis. ODNI has several offices that assist with its oversight of the Section 702 program: ODNI's Office of Civil Liberties, Privacy, and Transparency (ODNI CLPT); ODNI's Office of General Counsel (ODNI OGC); and ODNI's Mission Integration Directorate Mission Performance, Analysis, and Collection (MPAC) Division.

1. *DOJ/ODNI Oversight of NSA's Implementation of Section 702*

a. Targeting Reviews

NSA is required to document every targeting decision made under its targeting procedures.[399] The record of each targeting decision, known as a tasking sheet, includes: (a) the specific selector to be tasked; (b) citations to the information that support a conclusion that the target is reasonably believed to be located outside the United States; and (c) a narrative describing the basis for NSA's assessment that the target is expected to possess, is expected to receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign

[396] 25th Joint Assessment, *supra*, at iii-iv.

[397] *See* 50 U.S.C. § 1881f; FISC Rules of Procedure, *supra*, at 5.

[398] *See* FISC Rules of Procedure, *supra*, at 5.

[399] *See* 25th Joint Assessment, *supra*, at A-6-A-7.

territory authorized for targeting.[400]

NSA provides all of these tasking sheets electronically to DOJ and ODNI. DOJ performs a post-tasking review of every tasking sheet provided by NSA, and ODNI reviews a portion of these sheets.[401] DOJ, and as applicable, in consultation with ODNI, determines whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information to ascertain the basis for NSA's foreignness determinations and foreign intelligence purposes.[402] In addition, DOJ, and as applicable, in consultation with ODNI, reviews whether the tasking was in overall compliance with the statutory limitations, such as the prohibition against reverse targeting.[403] After its review, DOJ sends NSA a list of questions compiled by its personnel, and any requests for additional information.[404] For tasking sheets that DOJ assesses meet the standards and provide sufficient information based on the sheet itself, no further supporting documentation is required.[405]

Bi-monthly, DOJ and ODNI staff engage virtually and in person with staff from NSA's Compliance Group, NSA OGC, and other NSA personnel as required.[406] DOJ, ODNI, and NSA work together to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement.[407] DOJ and ODNI may also seek additional information from FBI and CIA regarding selectors they have nominated.[408] If needed, the agencies continue to discuss certain taskings after these reviews, or identify them as tasking errors.[409] The results of each DOJ/ODNI bimonthly review are required by statute to be provided to the House and Senate Judiciary and Intelligence congressional committees.[410] Historically, these bimonthly reviews have determined that approximately 99 percent of all NSA taskings met the requirements of the NSA targeting procedures.[411]

---

[400] *Id.* at A-6.

[401] *Id.* at 8.

[402] *Id.*

[403] *Id.*

[404] *Id.*

[405] *Id.*

[406] *Id.* at 9. However, DOJ and ODNI engage with NSA on a continual basis regarding compliance matters.

[407] *Id.*

[408] *Id.*

[409] *Id.*

[410] *Id.*

[411] *Id.* at 45.

b. Minimization Reviews

At those same bimonthly reviews, DOJ and ODNI also review NSA's compliance with its minimization procedures.[412] NSA sends DOJ and ODNI all reports disseminating Section 702-acquired U.S. person information. DOJ currently reviews all disseminated reports containing U.S. person information and ODNI reviews a sample.[413] DOJ and ODNI also review a sample of other reports containing Section 702-acquired information that do not include U.S. person information, as well as a sample of reports NSA has shared with certain foreign government partners.[414]

c. Querying Reviews

NSA's Section 702 querying procedures provide that prior to using any U.S. person identifiers as terms to query and select Section 702-acquired data, NSA personnel must provide a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information.[415] DOJ and ODNI also review these statements bimonthly. When querying Section 702-acquired metadata with a U.S. person query term, NSA personnel must document a justification for performing that query showing that it meets the query standard, and in case of sensitive queries, as discussed above, must request pre-approval.[416] When querying Section 702-acquired content with a U.S. person query term, NSA personnel must first provide a justification for why the query would be reasonably likely to return foreign intelligence information, and that justification must be approved by NSA OGC before the employee can perform the query.[417] DOJ performs a post-query review of all NSA queries of Section 702-acquired metadata using a U.S. person query term, including of the statement of facts.[418] For NSA queries of Section 702-acquired content, DOJ reviews the supporting documentation, including applicable FISC orders, and NSA OGC's approval of U.S. person query terms.[419]

[412] *Id.* at 9.

[413] *Id.*

[414] *Id.*

[415] *Id.* NSA did not have Section 702 querying procedures until 2018; previously, NSA's Section 702 query rules were contained in its minimization procedures.

[416] *Id.*

[417] *Id.* NSA's Section 702 querying procedures provide that NSA may approve the use of a U.S. person identifier to query Section 702-acquired content for no longer than a period of one year and that such approvals may be renewed for periods up to one year.

[418] *Id.*

[419] *Id.*

2. *DOJ/ODNI Oversight of FBI's Implementation of Section 702*

a. Targeting Reviews

FBI processes requests for information from the other Intelligence Community agencies.[420] In doing so, FBI TDI personnel work through a checklist to ensure each request is consistent with the FBI targeting procedures.[421] In particular, this involves conducting checks for information relevant to the Designated Account to ensure it is not used by a U.S. person or someone located in the United States.[422]

At least every sixty days, DOJ and ODNI personnel conduct a targeting compliance review at FBI headquarters.[423] DOJ and ODNI personnel review the targeting checklists compiled by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.[424] Typically, these are in-person monthly reviews of every request that returned results in FBI systems.[425] During the coronavirus pandemic, DOJ conducted these reviews remotely every sixty days, and reviewed a sample of these packets.[426]

Separately, DOJ and ODNI also review the original source documentation underlying FBI nominations for the Section 702 program as needed.[427]

b. Minimization Reviews

DOJ performs quarterly reviews at FBI headquarters of FBI's compliance with its minimization procedures.[428] DOJ reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing U.S. person information.[429] DOJ also reviews all disseminations by the relevant FBI headquarters unit of Section 702-acquired information concerning U.S. persons.[430] DOJ and ODNI also perform minimization reviews at

[420] *Id.* at 10.

[421] *Id.*

[422] *Id.*

[423] *Id.* at 11.

[424] *Id.*

[425] *Id.*

[426] *Id.*

[427] *Id.* at 12.

[428] *Id.*

[429] *Id.*

[430] *Id.*

FBI field offices throughout the year.[431] At these reviews, DOJ reviews a sample of retention decisions made by FBI personnel in connection with investigations involving Section 702-acquired information and a sample of disseminations of Section 702-acquired information concerning U.S. persons.[432] Typically, NSD conducts minimization reviews in person at approximately 25 to 30 FBI field offices annually.[433] DOJ's minimization reviews were suspended entirely from March 2020 to February 2021. In February 2021, NSD resumed field office reviews and in June 2022, DOJ resumed in-person minimization reviews of Section 702 information routed to FBI at selected FBI field offices.[434] In addition, DOJ and ODNI currently conduct an annual process review.

c. Querying Reviews

FBI's querying procedures require that, when querying Section 702-aquired information with a U.S. person or presumed U.S. person query term, before FBI personnel may access the results of that query they must first provide a written statement of the specific factual basis to believe that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime.[435] Unlike NSA's querying procedures, FBI querying procedures do not require personnel to provide a written statement of facts before querying or accessing the results from queries of Section 702-acquired metadata, or noncontents, with a U.S. person query term.[436]

Historically, DOJ and ODNI reviewed a sample of FBI's queries of unminimized FISA-acquired information, including Section 702-acquired information.[437] Unlike reviews of NSA querying, DOJ and ODNI review both U.S. person queries and other queries. In 2021, DOJ restarted its query reviews, which had been suspended since the start of the coronavirus pandemic, and increased the resources it dedicated to those reviews. As discussed previously, based on incidents reported to the FISC that were discovered during DOJ query reviews, the FISC issued an Order in September 2021 expressing concern over the "widespread violations of the querying

[431] *Id.*

[432] *Id.* at 11.

[433] For each field office review, DOJ evaluates Section 702 information routed to FBI during the review period selected (i.e., generally the time since DOJ's last review of that field office).

[434] U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 1 June 2021—30 November 2021, at 42 (Mar. 2023) [hereinafter 27th Joint Assessment]; 26th Joint Assessment, *supra*; U.S. Dep't of Just., Responses to Written Questions Submitted by PCLOB and Directed to NSD, at 10 (Sept. 2022).

[435] 25th Joint Assessment, *supra*, at A-15.

[436] *Id.* at 9. *Compare* 2021 NSA Querying Procedures, *supra*, *with* 2021 FBI Querying Procedures, *supra*.

[437] 25th Joint Assessment, *supra*, at 12.

standard by the FBI."[438] Currently, DOJ reviews a subset of FBI field offices annually, and generally reviews a 90-day snapshot of queries conducted by personnel in the relevant office in two FBI systems that contain unminimized FISA-acquired information.[439] During these reviews, DOJ personnel seek to determine whether each query met the query standard and whether queries were properly labeled as to U.S. person status.[440] To evaluate compliance with Section 702(f)(2), they also assess whether any U.S. person queries were conducted in Section 702 data solely for the purpose of returning evidence of a crime.[441] If such a query were conducted, DOJ personnel seek additional information as to whether FBI personnel received and reviewed Section 702-acquired information and whether the query was conducted at the predicated investigation stage. If so, DOJ identifies whether FBI sought and obtained an order from the FISC pursuant to Section 702(f)(2).[442]

3. *DOJ/ODNI Oversight of CIA's Implementation of Section 702*

a. Targeting Reviews

Partially because CIA does not conduct Section 702 targeting or acquisition, oversight of the agency's implementation of Section 702 is more limited than that of NSA and FBI.[443] DOJ and ODNI may, however, review the original source documentation underlying CIA nominations for the Section 702 program as part of the targeting reviews conducted at NSA, as described above.[444]

[438] (U) U.S. Dep't of Just. Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (April 18, 2023).

[439] (U) Fed. Bureau of Investigation Briefing for Priv. and C.L. Oversight Bd. Staff (July 29, 2022). These 90-day snapshots are usually of a period several months before the audit, and FBI assists DOJ by compiling the query logs in advance of the review. FBI personnel (below the CDC level) are not told until after the snapshot review period that an audit will be conducted.

[440] 25th Joint Assessment, *supra*, at 12.

[441] DOJ review of FBI evidence of a crime only queries also occurs outside the FBI field office reviews. As a matter of course, when FBI personnel label a query as seeking evidence of a crime only, FBI attorneys are notified and often consult with DOJ regarding those queries.

[442] *See* 25th Joint Assessment, *supra*, at A-15. As discussed previously, if it is determined that a query of Section 702-acquired information using a U.S. person query term was conducted for purposes of acquiring evidence of a crime information only, it must be included in quarterly reports to the FISC. If such a query were performed in connection with a predicated criminal investigation that does not relate to national security and the analyst reviewed the results of the query prior to obtaining a Section 702(f)(2)(A) order from the FISC, DOJ would report those instances as compliance incidents to the FISC.

[443] Id. at 13.

[444] *Id.* at 14.

b. Minimization Reviews

DOJ and ODNI also conduct bimonthly minimization reviews at CIA. Prior to the coronavirus pandemic, DOJ and ODNI reviewed all of CIA's written justifications for marking U.S. person information for long-term retention and transfer outside of the restricted FISA repository, and DOJ and ODNI also reviewed a sample of the underlying communications marked for retention and transfer in person. Since the onset of the coronavirus pandemic, DOJ has continued to review all of these justifications, but asks follow-up questions via email instead of reviewing a sample of the underlying communications in person. ODNI reviews a sample of these justifications.[445] These oversight personnel also review all disseminations of Section 702-acquired U.S. person information.[446]

c. Querying Reviews

Like NSA, CIA's querying procedures require that, when querying Section 702-acquired content using a U.S. person query term, CIA personnel must provide a written statement of the specific factual basis to believe that the query will be reasonably likely to retrieve foreign intelligence information. However, unlike NSA, CIA's procedures do not require prior approval of U.S. person query terms by CIA's OGC before they may be used to conduct content queries. Bimonthly, DOJ reviews all of CIA's written foreign intelligence justifications for U.S. person queries of Section 702-acquired content.[447] ODNI reviews a sample.[448]

4. *DOJ/ODNI Oversight of NCTC's Implementation of Section 702*

a. Targeting Reviews

NCTC neither engages in targeting or acquisition nor nominates potential Section 702 targets to NSA.[449] DOJ and ODNI, therefore, do not conduct separate targeting reviews at NCTC.[450]

b. Minimization Reviews

Bimonthly, DOJ reviews all NCTC justifications for minimization and retention of Section 702-acquired communications, irrespective of whether they contain U.S. person information, and

[445] *Id.*

[446] *Id.*

[447] *Id.*

[448] *Id.*

[449] *Id.* at 15.

[450] *Id.*

ODNI reviews a sample.[451] DOJ also reviews the content of Section 702-acquired communications containing U.S. person information that have been marked for minimization and retention.[452] DOJ also reviews all disseminations of Section 702-acquired U.S. person information and ODNI reviews a sample.

c. Querying Reviews

Like NSA and CIA, NCTC's querying procedures require that, when querying Section 702-acquired content and noncontent using a U.S. person query term, NCTC personnel must first provide a written statement of the specific factual basis to believe that the query was reasonably likely to retrieve foreign intelligence information.[453] However, unlike NSA, NCTC's procedures do not require prior approval by ODNI OGC attorneys supporting NCTC of U.S. person query terms before they may be used to conduct content queries. Bimonthly, DOJ reviews all of NCTC's written foreign intelligence justifications irrespective of whether the query contains U.S. person query terms, and ODNI reviews a sample.[454]

5. *Incident Investigation, Reporting, and Related Activities*

Whether compliance incidents are initially discovered pursuant to a DOJ/ODNI review, an internal agency compliance review, or by self-reporting, Section 702's statutory language and the FISC's own rules of procedure require DOJ to report compliance incidents by relevant elements of the Intelligence Community or ECSPs to Congress and the FISC.[455] Pursuant to the FISC Rules of Procedure, all compliance incidents must be reported to the FISC without undue delay in a Rule 13(b) notice and/or in a quarterly report.[456] Rule 13(b) states that such reports must include a description of the incident of noncompliance, the facts and circumstances related to the incident, any modifications that will be made in how the government is using the authority in light of the incident, and a description of how the government will handle any information obtained as a result of the incident.[457] Separately, the Attorney General and DNI must conduct semiannual assessments regarding the agencies' compliance with their targeting procedures, minimization

[451] *Id.*

[452] *Id.*

[453] 2021 NCTC Querying Procedures, *supra*, at 3-4.

[454] 26th Joint Assessment, *supra*, at 16-17.

[455] *See* 50 U.S.C. § 1881f(b)(1)(G); FISC Rules of Procedure, *supra*, at 5.

[456] 26th Joint Assessment, *supra*, at iii-iv; FISC Rules of Procedure, *supra*, at 5. A notice is usually required when the incident involves a U.S. person, a person located in the United States, multiple authorities, or a systemic issue.

[457] FISC Rules of Procedure, *supra*, at 5.

procedures, querying procedures, and the Attorney General Guidelines.[458] This semiannual joint assessment must be provided to Congress and the FISC.[459] As of December 2022, 24 of the semiannual joint assessments have been partially declassified and are publicly available.[460]

To meet these various reporting obligations, a team of DOJ and ODNI personnel review incident reports, request additional information, and, when necessary, further investigate potential incidents of noncompliance.[461] These inquiries and investigations entail frequent interaction with counterparts in the internal agency compliance programs discussed above.[462] In addition to resolving individual compliance matters, the DOJ/ODNI teams periodically coordinate with representatives from NSA, FBI, CIA, and NCTC to discuss, among other things, compliance trends and incidents that affect multiple agencies.[463] Some of the results of DOJ's and ODNI's compliance investigations and reports are discussed in the next section.

B. FISC Oversight

The FISC's primary role in Section 702 is to review the Section 702 certifications and corresponding targeting, minimization, and querying procedures to ensure they meet the requirements of the statute and the Fourth Amendment.[464] As described in detail above, however, the FISC has held that this review of the Section 702 certifications and related documents must be made in light of the actual manner in which the government has implemented (or plans to implement) the Section 702 authorities.[465] In addition to filings made by the government to the FISC in support of the certifications, the FISC's determinations are informed by DOJ's reports of all identified incidents of noncompliance with the procedures, the Attorney General and DNI's semiannual joint assessment regarding compliance with the procedures, the annual reports of agency heads authorized to acquire foreign intelligence information under Section 702, and any reports by the Inspectors General.[466] In reviewing the certifications, the FISC may also order the government to respond to questions regarding the conduct of the Section 702 program and may

[458] 50 U.S.C. § 1881a(m)(1).

[459] *Id.*

[460] *See IC on the Record Database*, *supra.*

[461] 26th Joint Assessment, *supra,* at iii-iv.

[462] *Id.*

[463] *Id.* at 9-17.

[464] 50 U.S.C. § 1881a(j)(2)-(3).

[465] *See* Apr. 21, 2022 FISC Opinion and Order, *supra,* at 67.

[466] *See* 50 U.S.C. § 1881a(m)(1)-(3); FISC Rules of Procedure, *supra,* at 5.

hold hearings in order to take sworn testimony from government witnesses.[467] As noted above, when considering the certifications, the FISC shall appoint amicus curiae to review any novel or significant interpretations of law unless the FISC issues a finding that such an appointment would be inappropriate. The FISC has appointed an amicus in its review of several Section 702 certifications since Congress created the amicus role in 2015. FISA also provides that the FISC "may appoint an individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit and individual or organization leave to file an amicus curiae brief."[468]

The FISC's oversight role is not limited to the renewal of Section 702 certifications. The government's obligation to report incidents of noncompliance under the FISC's rules is independent of whether any Section 702 certification is currently pending before the Court.[469] In a 2013 letter to the then-Senate Judiciary Committee Chairman, the then-presiding judge of the FISC stated that with respect to all FISA compliance matters, including incidents of noncompliance with the Section 702 procedures, the Court may seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issue orders to the government to cease an action that the Court assesses to be noncompliant.[470]

C. Inspector General Reports

Section 702 also authorizes Inspectors General of agencies that acquire data pursuant to Section 702 to conduct reviews of the Section 702 program.[471] The Inspectors General are authorized to evaluate the agencies' compliance with the targeting procedures, minimization procedures, querying procedures, and Attorney General Guidelines.[472] Any such reviews are required to contain an accounting of the number of disseminated reports containing U.S. person identities, the number of instances in which those identities were unmasked, and the number of

[467] FISC Rules of Procedure, *supra*, at 1, 6; *see* Letter from Presiding Judge Reggie B. Walton, Foreign Intel. Surveillance Ct., to Senator Patrick Leahy, Chairman, S. Comm. on the Judiciary, at 4-6 (July 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Leahy-11-2013.pdf [hereinafter Judge Walton Letter] (describing government submissions related to Section 702 certifications and the types of additional information sought from the government by the FISC); Bates October 2011 Opinion, *supra*, at 7-10 (describing examples of filings and hearings).

[468] 50 U.S.C. § 1803(i)(2)(B).

[469] FISC Rules of Procedure, *supra*, at 5.

[470] Judge Walton Letter, *supra*, at 10-11.

[471] 50 U.S.C. § 1881a(m)(2).

[472] *Id.*

targets that were subsequently determined to be located in the United States.[473] The results of these reviews must be provided to the Attorney General, the DNI, the FISC, and Congress.[474] The NSA, CIA, and DOJ Inspectors General have conducted reviews under this provision.[475]

For example, in the most recent NSA Office of the Inspector General (OIG review of NSA's implementation of Section 702, NSA OIG identified numerous violations and areas in need of improvement related to the use of U.S. person query terms and made thirteen recommendations to address them.[476] NSA management agreed with all thirteen recommendations and either completed or planned remedial measures to the satisfaction of NSA OIG.

Two issues relate directly to the Board's examination of U.S. person queries. First, NSA OIG found that NSA analysts had conducted numerous U.S. person queries against Section 702 collection with selectors that had not been approved by NSA OGC or whose authorization had expired.[477] NSA OIG recommended that NSA fully deploy an automated system to notify analysts of potential noncompliance with procedures.[478]

Second, NSA OIG found that thirty-five U.S. person selectors that were on a "defeat list," which is intended to stop selectors from being run against NSA databases, were still approved for querying, and this fact should have been reported to the FISC.[479] NSA determined that the selectors had not been cross-checked with the defeat list for technological reasons related to a previous notification to the FISC, and only twelve had actually been used in queries. NSA subsequently reported the incidents per NSA OIG's recommendation.

D. Congressional Oversight

[473] *Id.*

[474] *Id.*

[475] *See* Cent. Intel. Agency, Off. of the Inspector Gen., CIA's Foreign Intelligence Surveillance Act (FISA) 702 Program (2017); U.S. Dep't of Just., Off. of the Inspector Gen., A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (Re-released with some previously redacted information unredacted) (2012); Nat'l. Sec. Agency, Off. of the Inspector Gen., Final Report of the Audit on the FISA Amendments Act §702 Detasking Requirements (2010). In the most recent review provided to the Board, the NSA Office of Inspector General's report to Congress dated September 29, 2021, the NSA OIG made thirteen recommendations to assist NSA in addressing issues related to the use of U.S. person terms to query Section 702 data. NSA management agreed with all thirteen recommendations and either completed or planned remedial measures to the satisfaction of the OIG.

[476] Nat'l Sec. Agency, Off. of the Inspector Gen., Semiannual Report to Congress—1 April to 30 September 2021, at 6 (2023) [hereinafter NSA OIG Report].

[477] *See id.* at 5-6.

[478] *Id.* at 34.

[479] *Id.*

Four congressional committees conduct oversight over the government's implementation of Section 702: the Senate Select Committee on Intelligence; the Senate Committee on the Judiciary; the House Permanent Select Committee on Intelligence; and the House Committee on the Judiciary. When Congress initially authorized the Section 702 program, it did so with sunset provisions, which allows amendments to the program to be discussed through a reauthorization process.[480] Most recently, Congress reauthorized Section 702 for six years beginning on January 19, 2018, and the program is set to expire at the end of 2023, unless Congress reauthorizes it again.[481]

Section 702 mandates congressional oversight, including requiring that the Attorney General provide these four committees with a semiannual report describing several aspects of the Section 702 program, including the underlying documents that govern the program.[482] Among other things, this semiannual report must include copies of the reports from any compliance reviews conducted by DOJ or ODNI, a description of any incidents of noncompliance by the Intelligence Community or an ECSP reported to the FISC during the applicable six-month period, any certifications (including targeting, minimization, and querying procedures) submitted during the reporting period, and the redacted directives sent to the ECSPs during the reporting period.[483] The semiannual report must also include a description of the FISC's review of the certifications and copies of any order by the FISC or pleading by the government that contains a significant legal interpretation of Section 702.[484]

The government also provides the four committees with all government filings and FISC orders and opinions related to the Court's consideration of the Section 702 certifications.[485] In addition, the congressional committees receive the classified Attorney General and DNI semiannual joint assessment regarding compliance with the procedures, the annual reports of agency heads that conduct Section 702 acquisition, and any reports by the Inspectors General.[486] Moreover, the agencies may separately (and more promptly) inform the congressional committees

[480] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, § 403(b)(1), 122 Stat. 2439 (2008).

[481] Pub. L. 110-261, § 403(b)(1), 122 Stat. 2474 (2008), *as amended by* Pub. L. 112-238, §2(a)(1), 126 Stat. 1631; Pub. L. 115-118, § 201(a)(1), 132 Stat. 19 (2018).

[482] 50 U.S.C. § 1881f.

[483] *Id.* § 1881f(b)(1).

[484] *Id.* § 1881f(b)(1)(D). Copies of documents related to significant legal interpretations are also produced to Congress pursuant to 50 U.S.C. § 1871.

[485] *Id.* § 1881f.

[486] *Id.* § 1881a(l)(1)-(3).

of substantial compliance incidents.[487] The committees also hold hearings, and committee members and staff receive briefings, regarding the implementation of the Section 702 program.[488]

IX. Compliance Issues

The Section 702 program is a technically complex collection program with detailed rules embodied in the targeting procedures, minimization procedures, querying procedures, the Attorney General's Acquisition Guidelines,[489] directives, and within the statutory language itself. Incidents of noncompliance with these rules have been identified in the course of internal agency compliance review, as well as oversight conducted by DOJ and ODNI. Those incidents of noncompliance included individual errors, system issues, and instances where Intelligence Community personnel did not fully understand the requirements. According to the government, there have been several examples where oversight mechanisms have identified incidents involving improper intent in seeking to circumvent or violate the procedures, related rules, or statutory requirements. The matters identified to PCLOB are:

- One instance in which an FBI linguist had conducted multiple queries in 2015 using the individual's own name, the names of the individual's relatives, and the names of co-workers, and subsequently, in 2017, conducted queries seeking information regarding an individual apparently employed by defense counsel in a non-national security criminal prosecution;[490]
- One instance from 2018 in which an FBI task force officer conducted queries seeking information in connection with a call the individual's family member had received in which the caller made allegations against another family member;[491]
- One instance from 2022 in which two NSA analysts conducted queries seeking information about a non-U.S. person potential tenant of a rental property owned by the

[487] *See, e.g.,* NSA DCLPO Report, *supra,* at 3.

[488] *See, e.g.,* S. Rep. No. 112-174, at 2 (2012).

[489] Pursuant to Section 702(g), the Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978 were adopted by the Attorney General, in consultation with the DNI, in 2008 and revised in 2018.

[490] U.S. Dep't of Just., Notice to the U.S. Foreign Intel. Surveillance Ct.: Final Notice of Compliance Incident Regarding the FBI's Querying of Raw FISA-Acquired Information, Including Information Acquired Pursuant to Section 702 of FISA (Apr. 5, 2019).

[491] U.S. Dep't of Just., Notice to the U.S. Foreign Intel. Surveillance Ct.: Notice of compliance incidents regarding the FBI's querying of raw FISA-acquired information, including information acquired pursuant to Section 702 of FISA (Sept. 4, 2018).

analysts;[492] and

- One instance from 2022 in which an NSA analyst conducted queries on two occasions seeking information about two individuals that the analyst had met through an online dating service.

The FISC has held, most recently in April 2022, that the program as a whole complies with both statutory requirements and those of the Fourth Amendment; however, it has imposed various reporting requirements on the government so that it can continually evaluate the impact of compliance incidents on the lawfulness of the Section 702 program.[493]

A. Types of Compliance Incidents

Compliance incidents are generally grouped by the applicable procedure (targeting, minimization, or querying), but each incident may involve multiple compliance issues.[494] For example, as described below, an incident involving a failure to detask a selector may also include a notification delay. As noted previously in this Report, compliance incidents are generally reported to the FISC by DOJ when discovered by DOJ or the agency, but there may be delays in reporting due to investigating the underlying facts of the matter and assessing whether the incident constituted a reportable compliance incident. Pursuant to Rule 13(b) of the Rules of Procedure for the FISC, the government must provide prompt notice of compliance matters to the Court. By agreement with the FISC, certain lower-priority incidents may be reported in quarterly reports rather than being first reported in individual 13(b) notices.[495] Although queries have accounted for the vast majority of incidents over the last several years, the government reports and collects data related to all categories of incidents.

1. *Targeting Incidents*

Targeting incidents include a range of errors relating to both the improper tasking and the delayed detasking of selectors.

- Tasking incidents: an error in the initial tasking of the selector. Tasking incidents include foreignness determination errors (failure to establish a sufficient basis to assess that the target was a non-U.S. person, located outside the United States), foreign intelligence purpose errors (failure to establish that the target was expected to possess,

[492] U.S. Dep't of Just., Notice to the U.S. Foreign Intel. Surveillance Ct.: Notice of Potential Compliance Incidents Regarding Noncompliant Queries (Nov. 2, 2022).

[493] Apr. 21, 2022 FISC Opinion and Order, *supra,* at 121.

[494] 26th Joint Assessment, *supra,* at 36.

[495] FISC Rules of Procedure, *supra,* at 5; 50 U.S.C. § 1881a(m)(1).

receive, or communicate foreign intelligence authorized for collection in the currently applicable Section 702 certifications), typographical errors when tasking the selector, and tasking a selector to the incorrect provider.[496]

- Detasking incidents, i.e., detasking delays: instances in which the selector was properly tasked, but errors occurred in failing to detask the selector without delay when detasking was required by statute or procedure.[497] Many of the detasking delays have occurred when a properly targeted non-U.S. person either traveled or appeared to have traveled to the United States. In such instances, prompt detasking of selectors used by that target is required. Detasking errors also include incomplete detaskings, i.e., detasking some but not all of the selectors used by a target.

- Overproduction incidents: when attempting to acquire communications associated with a properly tasked selector, data associated with untasked selectors was also provided by the provider.[498]

- Overcollection incidents: Incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection."[499]

- Notification delays: incidents in which notification requirements mandated by the targeting procedures were not satisfied. In general, NSA must provide notice to DOJ and ODNI within five business days of discovering that a selector is being used by a person in the United States or by a U.S. person.[500]

- Documentation incidents: while the targeting rationale or foreignness determination is not deficient, the determination to target a selector was not properly documented.[501]

Although targeting incidents are associated with either the FBI or NSA targeting procedures and are thus attributed to FBI and NSA, the underlying cause of the incident could lie

[496] 26th Joint Assessment, *supra*, at 32.

[497] Id.

[498] *Id.*

[499] *Id.*

[500] *Id.*

[501] *Id.* at 33.

with any of the four agencies.[502] The specific facts of the incident are included in Rule 13(b) notifications or quarterly reports to the FISC and in semiannual reports to Congress and generally indicate the underlying cause of the issue, if known.[503] Both the NSA and FBI targeting incident rates have been consistently below one percent for at least the last five reporting periods.[504] Since the summer of 2019 until 2023, the NSA targeting compliance incident rate, which is calculated by dividing the number of targeting compliance incidents reported to the FISC in a given six-month reporting period by the average number of tasked selectors subject to acquisition at any given time during the reporting period, has ranged from approximately 0.05% to .015%; in other words, a 99.85% compliance rate or better.[505] During the same time period, the FBI targeting compliance incident rate, which is calculated by dividing the number of FBI targeting compliance incidents reported to the FISC during a given six-month reporting period divided by the total number of selectors tasked by FBI for collection during that

Both the NSA and FBI targeting incident rates have been consistently below one percent for at least the last five reporting periods.

[502] For example, if NSA fails to provide FBI with certain required information in connection with a request that FBI task a Designated Account, that could result in NSA causing a violation of the FBI targeting procedures. *See, e.g.*, 27th AG SAR, *supra*, at 98.

[503] *See, e.g., id.*

[504] *See* 26th Joint Assessment, *supra*; 25th Joint Assessment, *supra*; U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 01 December 2019—31 May 2020 (Dec. 2021) [hereinafter 24th Joint Assessment]; U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 01 June 2019—30 November 2019 (Sept. 2021) [hereinafter 23rd Joint Assessment]; U.S. Dep't of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance With Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: 01 December 2018—31 May 2019 (Aug. 2021) [hereinafter 22nd Joint Assessment].

Of the targeting compliance incidents reported in the 26th Joint Assessment, 47.5% were the result of NSA not having a sufficient foreign intelligence purpose for the tasking; 14.6% were the result of insufficient foreignness determinations; 20.1% were typographical errors; 1.4% involved errors in tasking a selector to an incorrect provider; and 14.5% involved a delayed detasking of a target's selectors.

[505] *See* 26th Joint Assessment, *supra*, at 37; *see also* 25th Joint Assessment, *supra*; 24th Joint Assessment, *supra*; 23rd Joint Assessment, *supra*.

reporting period, has ranged between approximately 0.011% and 0.0070%; in other words, a 99.99% compliance rate or better.[506]

2. *Minimization Incidents*

Minimization incidents involve the improper acquisition, retention, use, or dissemination of Section 702 information.[507] Such incidents may involve a systemic failure to properly age off information or improper dissemination of attorney-client communications.[508] Minimization incidents could also include failure to properly mask a U.S. person identity or unmasking a U.S. person identity in a disseminated intelligence report when the identity was not necessary to understand foreign intelligence information or was not evidence of a crime. Standards for when masking is required are set by agency minimization procedures and may be enhanced by agency policy. Reporting on minimization errors has also historically included querying errors, a relic of the days when querying was governed by the minimization procedures.[509] In future reporting, the Intelligence Community has asserted that these metrics will be separated, thus increasing transparency and facilitating easier assessment. That said, the vast majority of the combined minimization and querying incident numbers have been attributable to querying.[510]

3. *Querying Incidents*

Querying incidents occur when the query does not satisfy the query requirements laid out in the respective agency's querying procedures or the analyst failed to obtain proper approvals for the query.[511] For example, a query incident must be reported to the FISC when a query is conducted for an improper purpose, is overly broad, or is not supported by a proper justification. Additionally, as NSA analysts are required to obtain prior approval for all U.S. person query terms from NSA's OGC before conducting a content query, failure to obtain that approval or conducting a query after that approval has expired would be a reportable query incident.[512] FBI is required to obtain a Section 702(f)(2) order to access the contents of communications retrieved from a U.S.

[506] *See* 26th Joint Assessment, *supra*, at 40; *see also* 25th Joint Assessment, *supra*; 24th Joint Assessment, *supra*; 23rd Joint Assessment, *supra*.

[507] 26th Joint Assessment, *supra*, at 33.

[508] *E.g.*, *id.* at 51.

[509] *E.g.*, *id.*

[510] *See*, *e.g.*, *id.* at 3-4.

[511] *Id.* at 33. In addition to meeting the query standard described above, personnel must properly apply certain presumptions when labeling a query as a U.S. person query or otherwise. The 2014 Report did not describe this as a potential query compliance incident type because it was not yet a requirement.

[512] 2021 NSA Querying Procedures, *supra*.

person evidence of a crime only query that is conducted pursuant to a predicated criminal investigation opened by FBI unrelated to national security. Failure to obtain a Section 702(f)(2) order prior to reviewing the contents of communications retrieved pursuant to such a query must be reported to the FISC as a query compliance incident.[513]

Querying incidents have accounted for the largest percentage of compliance incidents over the last several years due primarily to FBI compliance issues. These have included issues related to FBI system configuration, training, and improper application of the query standard.[514] Compliance incidents have also resulted from queries conducted using leads, or "tips."[515] Due to these compliance issues, the government has begun reporting the FBI query compliance incident rate, which is calculated by dividing the number of query compliance incidents reported to the FISC during a given six-month reporting period by the number of queries reviewed by DOJ in connection with the reviews at which those incidents were discovered. The FBI query compliance incident rate has ranged from 0.40% to 36.59% since 2019.[516] High query compliance incident rates have generally been attributable to large noncompliant batch job queries. Periods of low rates of query compliance incidents generally occurred while DOJ personnel were limited in their ability to conduct field office reviews throughout the coronavirus pandemic.[517] DOJ and ODNI assessed that query compliance remained a challenge for FBI during the coronavirus pandemic periods, notwithstanding the low rates.[518]

B. Compliance Incident Reporting

DOJ and ODNI are required to track and report compliance incidents to Congress in periods running from December 1 through May 31 and June 1 through November 30. These incidents are analyzed jointly by DOJ and ODNI to identify compliance trends and potential mitigation strategies. DOJ and ODNI are not required to report specific metrics or trends by law and have not promulgated a uniform standard that requires reporting compliance incidents in specific categories.

Previously, the government calculated an overall compliance incident rate for the Section 702 program by dividing the number of compliance incidents reported to the FISC in a given six-month period by the average number of selectors tasked for collection on any given day during

[513] CY2022 ASTR, *supra*, at 26.

[514] 27th AG SAR, *supra*, at 127.

[515] *See, e.g.*, Apr. 21, 2022 FISC Opinion and Order, *supra.*

[516] 26th Joint Assessment, *supra*, at 3.

[517] *See id.* at 3-4.

[518] *See, e.g., id.* at 4.

that period. The Intelligence Community consistently noted that this calculation was somewhat flawed as it compared two numbers that were not dependent on or necessarily related to one another.[519] At the time of the 2014 PCLOB report, this rate was consistently below one percent.[520] In 2018, however, increased focus on FBI queries led the government to identify a substantial number of query incidents.[521] While reported compliance incidents at CIA and NCTC have remained close to zero, FBI's reported compliance incidents have numbered in the thousands or tens of thousands, depending on the year.[522] The government concluded that the increase in compliance incidents related to queries exacerbated the problem that the prior method of calculating an overall compliance incident rate was misleading, since the number of query incidents is not in any way related to or dependent on the average number of tasked selectors. In 2022, the government suspended reporting this rate noting that it did not provide a useful measure of overall compliance, nor did it provide insight into the overall health of the Section 702 program. The government concluded that the new measurement was more appropriate because too many of the incidents in the numerator of the rate (in particular, minimization and querying errors) did not bear any relation to the targeting activity in the denominator of the rate (the average number of taske selectors during a given period).[523]

While reported compliance incidents at CIA and NCTC have remained close to zero, FBI's reported compliance incidents have numbered in the thousands or tens of thousands, depending on the year.

DOJ and ODNI instead adopted "more tailored compliance metrics aimed at better tracking specific compliance matters."[524] The government currently reports the NSA targeting compliance incident rate, which compares the number of NSA targeting incidents to the average number of tasked selectors, and the FBI query compliance incident rate, which compares the number of query

[519] Id. at 2.

[520] 2014 PCLOB Report, *supra*, at 77.

[521] Prior to 2018, the querying standard was articulated differently, and FBI asserts that DOJ began to identify querying compliance incidents it had not previously identified.

[522] The compliance incidents at CIA and NCTC mostly have involved isolated, individual instances of noncompliance, not systemic issues. *See* 26th Joint Assessment, *supra*, at 62-64. The compliance incidents at NCTC involved, for example, dissemination of unminimized Section 702-acquired information without proper labeling. The compliance incidents at CIA mostly involved, for example, queries that were not reasonably likely to retrieve foreign intelligence information.

[523] *Id.* at 2.

[524] *Id.*

incidents reported to the FISC in a given reporting period to the number of queries reviewed.[525] The NSA targeting compliance incident rate was first reported following a period in which NSA was experiencing higher than prior incident rates. As noted above, for the last several years, however, this incident rate has remained below one percent.[526] The FBI query compliance incident rate has fluctuated widely, in part because oversight was largely suspended earlier in the coronavirus pandemic and reduced query compliance incident rates reported during the coronavirus pandemic may not be reliable indicators of the true state of query compliance during those periods.[527] DOJ resumed FBI field office query reviews in 2021 and expanded to pre-coronavirus pandemic levels in 2022.[528] Once the data has been compiled from more recent reviews, the government will be better able to assess the effectiveness of enhanced training and system updates, though DOJ has continued to report query compliance incidents at almost every field office reviewed.[529]

C. Notable Compliance Trends

In 2022 the government identified numerous incidents of noncompliance with the NSA targeting procedures, the NSA minimization procedures, the NSA querying procedures, and/or the Attorney General's Acquisition Guidelines.[530] The vast majority of the querying incidents involved NSA analysts querying unminimized Section 702-acquired information using U.S. person query terms that had not been approved pursuant to NSA's Section 702 Querying Procedures.[531] The majority of NSA's compliance incidents were discovered by NSA's internal compliance program.

During the same reporting period, the government identified several incidents of noncompliance with the FBI targeting procedures and vast numbers of incidents of noncompliance with the FBI querying procedures.[532] The majority of FBI's compliance incidents were discovered by external overseers, i.e., DOJ and ODNI.[533] The noncompliant queries reported to the FISC during this reporting period were conducted prior to the implementation of several remedial

[525] *Id.* at 3.

[526] *Id.* at 37.

[527] *Id.* at 31.

[528] *Id.* at 13.

[529] 27th Joint Assessment, *supra*, at 30-31.

[530] 27th AG SAR, *supra*, at 2. These incidents covered the reporting period of June to November 2021.

[531] *Id.* at 83.

[532] *Id.* at 2. As noted, the reporting period for these incidents covered June to November, 2021.

[533] *See id*.

measures that were put in place to address the query issues, such as system re-designs, the creation of FBI OIA, and the issuance of new query guidance.[534] In addition, during this reporting period, the number of FBI querying incidents reported to the FISC was heavily impacted by three particular noncompliant batch job queries.[535]

As previously stated, CIA and NCTC do not task selectors but do receive unminimized communications from NSA and FBI.[536] During this same reporting period, DOJ and ODNI identified a few incidents of noncompliance with the CIA minimization or querying procedures and NCTC minimization procedures.[537] Since the majority of compliance incidents are attributable to FBI querying, this section will focus on these types of incidents.[538]

1. *Background on Query Compliance Issues*

As mentioned above, after a series of FBI violations of the query standard, including violations of the Section 702 querying procedures and/or FBI's FISA Title I/III minimization procedures, the FISC issued an order in September 2021, relating to FBI's querying of unminimized information obtained under FISA, and focused on the querying of unminimized collection obtained pursuant to Section 702.[539] The FISC found "[t]he problems relating to FBI querying practices are substantial and persistent."[540] The opinion reviewed a number of reported compliance incidents to illustrate that FBI's failure to apply the querying standard when searching unminimized Section 702-acquired information was more pervasive than the FISC had previously

[534] *Id.* at 97.

[535] *See id.* at 120.

[536] Id.

[537] *Id.* at 92, 132.

[538] *Id.* The numbers discussed herein cannot be viewed with a straight comparison because post-query reviews are done differently at FBI and NSA. DOJ and ODNI visit, virtually or physically, particular FBI field offices and review queries of unminimized FISA collection conducted at that field office during a particular period of time. DOJ and ODNI review both U.S. person queries and non-U.S. person queries that are run against unminimized Section 702-acquired and/or traditional FISA-acquired collection. By comparison, DOJ external overseers review all NSA-approved U.S. person query terms for querying into unminimized Section 702-acquired content and review all queries against Section 702-acquired metadata.

[539] Order in Response to Querying Violations, In re DNI/AG 702(h) Certifications 2020-A, 2020-B, 2020-C, and Predecessor Certifications, Docket Nos. 702(j)-20-01, 702(j)-20-02, 702(j)-20-03, and predecessor dockets, In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under FISA, Docket No. 08-1833, In re FBI Standard Minimization Procedures for Tangible Things Obtained Pursuant to Title V of FISA, Docket No. BR 13-49 (FISA Ct. Sept. 2, 2021) [hereinafter FISC 2021 Querying Violations Order]. The September 2021 Order included incidents where personnel opted-out of querying 702 data but still had query incidents against traditional FISA and BR.

[540] *Id.* at 13.

believed.[541] The FISC acknowledged that, in response to these continued compliance incidents, FBI had implemented several system changes[542] and updated its mandatory Section 702 program training, but found that the changes were insufficient.[543] The FISC ordered the government to update the Court with "a description of steps it is taking or will take to ensure that FBI applies the querying standard in a manner that is consistent with the government's representations to the FISC and the FISC's interpretation of that standard in its opinions."[544]

In April 2022, following a number of filings by the government, the FISC issued an opinion and order discussing the then-pending FBI querying procedures, among other matters, and examined the deficiencies by FBI as they relate to querying practices.[545] The order further discussed the changes FBI had made (as described in the timeline below), and predicted that these changes should, to an extent, help reduce the number of noncompliant queries. The following sections discuss some of the factors that, the Board's investigation has revealed, have contributed to FBI's relatively high query incident rate, as compared with NSA, CIA, and NCTC.

2. *System Design Issues*

As described in previously in this Report, FBI's primary systems that contain Section 702-acquired information were previously designed so that queries automatically opted in to all datasets, including FISA collection.[546] During external audits, DOJ and ODNI identified that a significant percentage of query incidents occurred because personnel did not realize their queries would run against unminimized Section 702 information.[547] For this reason, in June 2021, FBI modified its systems so that the default setting was for queries to not include unminimized FISA Section 702 datasets.[548] The systems now require personnel to affirmatively make a decision

[541] *Id.* at 6.

[542] As discussed throughout this Report, FBI made several system changes between 2020 and 2022, including: configuring its systems to default to not including unminimized FISA-acquired information; counting U.S. person queries; and requiring that personnel provide justifications in order to view the Section 702-acquired information resulting from U.S. person queries.

[543] FISC 2021 Querying Violations Order, *supra,* at 13.

[544] *See id.* at 14.

[545] Apr. 21, 2022 FISC Opinion and Order, *supra*.

[546] *Id.* at 37.

[547] Some of the more significant compliance incidents caused by the opt-out system design involved FBI personnel querying their own name in order to locate work products drafted by them, without realizing the query term would run in Section 702-acquired information.

[548] Apr. 21, 2022 FISC Opinion and Order, *supra,* at 37.

whether to query FISA Section 702 datasets or not.[549] In addition, FBI personnel may no longer rely on a pre-populated justification for their query and must always provide a written justification for their query before they may access the results of a query that involves a U.S. person query term.[550]

Another type of system design issue is that FBI systems do not readily track certain types of information, and personnel are not required to perform pre-query due diligence. For example, compliance incidents have resulted from an analyst in one field office querying Section 702-acquired information using a U.S. person query term in response to a lead from another field office, unaware that the other field office had opened a predicated criminal investigation on the same matter.[551] Because FBI personnel are currently not required to perform pre-query due diligence and there is no central tracking system to notify personnel across offices, personnel are generally unaware of predicated criminal investigations opened by other field offices.

3. *Batch Job Queries*

As described above, if performed incorrectly, batch job queries can lead to large-scale compliance incidents.[552] Although batch job queries involve multiple queries using query terms that are run pursuant to the same justification, that same justification must apply to each individual term.[553] In some historical incidents, FBI personnel have been unable to articulate a proper justification, or why a particular query term is likely to be found in Section 702-acquired information, and this issue has applied to thousands of terms, resulting in a large-scale compliance incident.[554]

For example, following a 2018 audit at an FBI field office, DOJ discovered that FBI personnel conducted batch job queries totaling over 6,800 queries of the Social Security numbers of all individuals who had obtained a particular employment-related certification.[555] According to the FBI analyst who conducted the queries, they were conducted in order to see whether any of

[549] *Id.* at 38.

[550] FBI FISA Systems Briefing, *supra.*

[551] Intel. Cmty. Briefing for Priv. and C.L. Oversight Bd. Staff (Apr. 27, 2023).

[552] *See* 27th AG SAR, *supra*.

[553] CY2021 ASTR, *supra*, at 20.

[554] In addition, since an entire batch job query must be labeled as a U.S. person query or a non-U.S. person query, entire batch job queries can be identified as noncompliant with the Section 702 querying procedures if the presumptions regarding U.S. person query terms were incorrectly applied.

[555] U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions Under Section 702 of the Foreign Intelligence Surveillance Act, at 131 (Sept. 2018) [hereinafter 20th AG SAR].

these individuals had any connections to terrorists or suspected terrorists.[556] DOJ concluded that these batch job queries, which resulted in thousands of noncompliant U.S. person queries lacking a proper justification, were conducted in the absence of any reason to believe the Social Security numbers would likely be found in Section 702-acquired information.[557] Following a 2021 audit at another FBI field office, DOJ discovered that an FBI analyst conducted three related batch job queries consisting of over 23,000 separate queries relating to the U.S. Capitol breach on January 6, 2021.[558] DOJ concluded that the FBI analyst that conducted the queries did not have any indications of foreign intelligence related to the query terms, and thus the queries lacked a proper justification.

In addition, following another 2018 FBI field office audit, DOJ discovered that FBI personnel had conducted batch job queries totaling over 1,600 queries of information—such as name, date of birth, passport number, telephone number, and email address—relating to all individuals who had flown through an airport during a particular date range and who were either traveling to or returning from a foreign country.[559] According to the FBI task force officer who conducted the queries, they were conducted in order to determine whether any of the individuals posed a national security threat, regardless of whether FBI was aware of information indicating that a particular individual posed such a threat.[560] These batch job queries, which resulted in over a thousand noncompliant U.S. person queries lacking a proper justification, were conducted in the absence of any reason to believe the query terms would likely be found in Section 702-acquired information.[561]

4. *Vetting Queries Performed by FBI*

FBI queries performed for vetting purposes are also commonly found to be noncompliant with the Section 702 querying procedures.[562] As described above, FBI vetting queries are usually conducted to help determine whether an individual should be granted access to information or government spaces, should be used as a source, or should be granted certain status.[563] Such queries

[556] *Id.* at 131.

[557] *Id.*

[558] 27th AG SAR, *supra*, at 125.

[559] 20th AG SAR, *supra*, at 125-26.

[560] *Id.*

[561] *Id.*

[562] 27th AG SAR, *supra*, at 104-19.

[563] *See id.*

may lack a proper justification under the current querying procedures if they either are not intended to or are not reasonably likely to return foreign intelligence information or evidence of a crime.[564]

For example, following a 2021 audit at an FBI field office, DOJ discovered that FBI personnel had queried the names and other identifiers of individuals who were scheduled to visit a government facility.[565] These vetting queries, which involved multiple batch job queries of noncompliant U.S. person queries lacking a proper justification, were conducted in the absence of any reason to believe the query terms would likely be found in Section 702-acquired information.[566]

In addition, following another FBI field office audit in 2018, DOJ discovered that FBI personnel had queried the names and dates of birth of individuals who were registered competitors an athletic event.[567] According to the FBI analyst who performed the queries, these types of queries were conducted as part of a routine event safety check in order to determine whether any of the individuals posed a national security or terrorism threat, regardless of whether FBI was aware of any such threat.[568] These vetting queries, which resulted in almost two thousand noncompliant U.S. person queries lacking a proper justification, were conducted in the absence of any reason to believe the query terms would likely be found in Section 702-acquired information.[569]

As mentioned above, FBI personnel may conduct source development vetting queries to determine the reliability of sources or to further investigate entities of interest.[570] These queries may result in compliance incidents, however, if they lack a proper justification. For example, after an FBI field office audit in 2020, DOJ discovered that an FBI analyst ran a batch job query including approximately 27 queries using the name of a company and the names of individuals who worked at the company to identify any derogatory information which would assist FBI in determining whether to develop these individuals as potential sources.[571] NSD assessed that queries conducted "under a mere suspicion that cyber criminals use [certain tools] in furtherance

[564] *See id.*

[565] 26th AG SAR, *supra,* at 98-99.

[566] Id.

[567] 21st AG SAR, *supra,* at 151-52.

[568] *Id.*

[569] *Id.*

[570] *See generally* Fed. Bureau of Investigation, DOJ/FBI Guidance for Queries of Raw FISA-acquired Information (June 18, 2018).

[571] 27th AG SAR, *supra,* at 106.

of criminal activity, both foreign and domestic, are not reasonably likely to retrieve foreign intelligence information or evidence of a crime."[572]

5. *Queries Related to Civil Unrest and Criminal Activities*

At least one of the government incident reports also contain a category for "Queries of Individuals Arrested in Connection with Civil Unrest and Protests."[573] Although these two categories are conceptually quite different, both raise concerns about running queries where there is no reason to believe that the information is likely to be found in data collected under Section 702. The government has identified a significant number of noncompliant queries where government personnel have conducted queries related to instances of civil unrest and protests.[574] In 2021, the government conducted hundreds of noncompliant queries concerning individuals arrested in connection with civil unrest and protests.[575] These queries often lack a proper justification, as an individual's participation in a protest or criminal act, in and of itself, does not give sufficient cause to believe that the query term is likely to be found in Section 702-acquired information, which is collected for foreign intelligence purposes.[576]

…[F]ollowing external oversight reviews at FBI field offices, DOJ discovered a number of queries of the names of individuals involved with the January 6, 2021, breach of the U.S. Capitol, or who were arrested in connection with the Black Lives Matter protests, absent sufficient cause to believe the individual query terms would be in Section 702-acquired information.

For example, following external oversight reviews at FBI field offices, DOJ discovered a number of queries of the names of individuals involved with the January 6, 2021, breach of the U.S. Capitol, or who were arrested in connection with the Black Lives Matter protests, absent sufficient cause to believe the individual query terms would be in Section 702-acquired information.[577] In one incident, FBI personnel between June 3 and June 5, 2020, conducted 141

[572] *Id.; see* FISC 2021 Querying Violations Order, *supra*, at 9.

[573] 27th AG SAR, *supra*, at 102.

[574] *See id.*

[575] *See id.* at 102, 108, 113, 124.

[576] *See id.* at 102.

[577] *Id.* at 102, 124.

queries of identifiers "associated with individuals arrested by the D.C. Metropolitan Police Department, the U.S. Secret Service, or the U.S. Park Police" in connection with the protests following the death of George Floyd.[578] At the time of the queries, FBI personnel had no information connecting the individuals or the conduct to information that would be contained in FBI's Section 702-acquired information.[579] In the reporting period covering November 2020 to December 2021, non-compliant queries related to civil unrest numbered in the tens of thousands.[580]

The government has also reported a number of queries concerning individuals involved in domestic drug and gang investigations, human trafficking investigations, and others, absent sufficient cause to believe the query terms would be in Section 702-acquired information.[581]

6. *Queries that Misidentified the U.S. Person Status of the Query Term*

As described previously in this Report, all Intelligence Community agencies are required to keep a record of each U.S. person query term used to query unminimized Section 702 information.[582] The Section 702 querying procedures currently require that all agencies' systems "include a technical procedure whereby a record is kept of each United States person query term used for a query."[583] This requirement was included as part of the 2018 Reauthorization Act.[584] All agencies must rely on presumptions when they do not know the U.S. person status of a subject of a query, and these presumptions are necessarily based on incomplete information. At NSA, however, when the U.S. person status of the subject of a query is unknown, analysts perform additional research by searching minimized FISA and non-FISA datasets.[585] At FBI, there is no requirement to conduct additional research to determine the U.S. person status of a particular query subject, so FBI personnel are allowed to rely on the various presumptions.[586]

For example, there were two large batch job queries using contacts associated with a former counterterrorism target. These batch job queries were labeled as containing exclusively non-U.S.

[578] *Id.* at 102.

[579] *Id.* at 102-03.

[580] *Id.*at 125

[581] *E.g.*, *id.* at 115, 125.

[582] *E.g.*, 2021 NSA Querying Procedures, *supra*, at 4; 2021 NCTC Querying Procedures, *supra*, at 3; 2021 FBI Querying Procedures, *supra*, at 4; 2021 CIA Querying Procedures, *supra*, at 3.

[583] *E.g.*, 2021 NSA Querying Procedures, *supra*, at 4; 2021 NCTC Querying Procedures, *supra*, at 3; 2021 FBI Querying Procedures, *supra*, at 4; 2021 CIA Querying Procedures, *supra*, at 3.

[584] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 4 (2018).

[585] Nat'l Sec. Agency, Email Response to Priv. and C.L. Oversight Bd. Staff (Aug. 16, 2023).

[586] 2021 FBI Querying Procedures, *supra*, at 3.

person query terms.[587] During an FBI field office review, DOJ discovered that 33,931 of the 68,183 query terms were correctly categorized as non-U.S. person query terms, but the remaining 34,252 queries in the batch job query should have been labeled as U.S. person query terms.[588] Additionally, there were three batch job queries related to individuals who had been the targets of cyber-attacks by foreign threat actors. These batch job queries were labeled as containing exclusively non-U.S. person query terms. During an FBI field office review, it was discovered that 8,217 of the 22,531 query terms included in the batch job queries should have been categorized as U.S. person query terms, and would have been so categorized separately.[589]

7. *Other Queries*

DOJ's Semiannual Report also includes certain query incidents identified as "Other Noncompliant Queries," that are generally not covered by the above-mentioned compliance categories.[590] These incidents range from linguists incorrectly conducting queries in FBI's database using their own name[591] to "routine search[es] for derogatory information" using the name of a confidential human source.[592]

8. *Queries Conducted at the FBI Pre-Assessment or Assessment Stage*

As discussed above, FBI engages in investigative activity (a) prior to assessments; (b) during assessments, and (c) during predicated investigations.[593] FBI may conduct database checks, including querying unminimized Section 702-acquired information, at all investigative stages.[594] However, DOJ field office reviews have identified many examples of queries of Section 702-acquired information conducted prior to an assessment or during an assessment that failed to meet the justification standard.[595] For example, following audits at FBI field offices, DOJ has reported queries relating to individuals who contacted FBI to report suspicious behavior, i.e., Guardian leads.[596] These queries may be meant to aid FBI personnel in evaluating an individual's credibility,

[587] 27th AG SAR, *supra,* at 122.

[588] Id.

[589] Id. at 127.

[590] *E.g., id.* at 105, 112, 119.

[591] *Id.* at 105.

[592] *Id.* at 112.

[593] *See* FBI DIOG, *supra,* at 5-1-7-13.

[594] *Id.* at 5-1.

[595] FBI FISA Systems Briefing, *supra*.

[596] 27th AG SAR, *supra,* at 113, 119.

but can lack any reason to believe the query term would be in Section 702-acquired information.[597] Similar types of improper queries have been found relating to the names of individuals suspected of any potentially suspicious behavior, such as individuals listed in Financial Suspicious Activity Reports (SARs), which are automated notifications FBI receives from the U.S. Department of the Treasury when a financial transaction meets certain criteria.[598]

9. *Evidence of a Crime Only Queries*

As noted in Section IV of the FBI Querying Procedures, FBI may query Section 702-acquired information for both foreign intelligence information and/or evidence of a crime.[599] In order for a query to be conducted for the purpose of finding foreign intelligence information, it must have a foreign intelligence nexus. For queries seeking evidence of a crime only, if FBI personnel would like to view the contents that result from such a query including a U.S. person query term, the query must be reported to the FISC quarterly. Further, if the query is in connection with a predicated criminal investigation opened by FBI that does not relate to the national security of the United States, FBI personnel must obtain a Section 702(f)(2) order from the FISC before reviewing the contents of communications retrieved by such a query.[600] However, as noted above, FBI has never sought such an order, although there were at least four identified instances in 2021 in which FBI personnel conducted such queries and accessed the results in violation of this requirement.[601]

In the September 2021 order issued by the FISC, the FISC noted that the reporting indicated that evidence of crime only queries are an infinitesimal percentage of FBI queries of unminimized Section 702 information.[602] Specifically, from March to May 2021, "none of those queries were

[597] *Id.* at 113, 119.

[598] *Id.* at 129.

[599] 2021 FBI Querying Procedures, *supra*, at 3-4.

[600] According to the government, whether a predicated criminal investigation relates to the national security of the United States for purposes of Section 702(f)(2) requires a case-by-case determination. The further removed a predicated criminal investigation is from a suspected crime involving a threat to national security, the greater the likelihood that a query seeking to retrieve only evidence of a crime run in connection with such investigation would require a separate order from the FISC. Government's Submission in Response to the Court's Questions Regarding FBI Queries, at 20, *In re DNI/AG 702(h) Certification 2021-A and its Predecessor Certifications*, Docket No. 702(j)-21-01 and predecessor dockets, *In re DNI/AG 702(h) Certification 2021-B and its Predecessor Certifications*, Docket No. 702(j)-21-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2021-C and its Predecessor Certifications*, Docket No. 702(j)-21-03 and predecessor dockets (FISA Ct. Jan. 19, 2022) [hereinafter 2021 Government's Submission in Response to the Court's Questions Regarding FBI Queries].

[601] CY2021 ASTR, *supra*, at 22.

[602] FISC 2021 Querying Violations Order, *supra*, at 12.

conducted for an evidence of crime only purpose."[603] The FISC questioned the credibility of this metric and suggested that FBI is under-reporting the queries.[604] The Court assessed that the number of evidence of a crime only queries reported to the Court are likely to lack credibility so long as DOJ and FBI "lack a shared, reasonable understanding . . . of the parameters of 702(f)(2) and the reporting requirements regarding evidence-of crime-only queries."[605]

Subsequently, the government submitted its response to the Court's order in which it explained that, because FBI personnel are only required to document a query justification when attempting to access the unminimized contents of Section 702-acquired data retrieved in response to a U.S. person query, the number of queries in which FBI users provide documented justifications indicating that the purpose of the query was only to retrieve evidence of crime does not represent all U.S. person queries of Section 702-acquired data conducted by FBI for the purpose of retrieving only evidence of a crime.[606] If FBI personnel conduct a U.S. person query for an evidence of a crime only purpose and no Section 702-acquired information is returned or such information is returned but FBI personnel do not access the content, no evidence of a crime-only justification is recorded.[607]

Through various filings, the government has provided its interpretation of the query standard that has been accepted by the FISC regarding when a query is conducted for evidence of a crime only and when a query is in connection with a predicated criminal investigation that does not relate to the national security of the United States.[608] To help ensure FBI is adequately capturing evidence of a crime only queries, FBI recently reconfigured its systems to no longer default to labeling queries as being conducted for purposes of retrieving foreign intelligence information. Before reviewing the contents retrieved by a query of Section 702-acquired information, FBI personnel must now affirmatively indicate whether a query is being conducted to retrieve (a) foreign intelligence information, or (b) evidence of a crime only.[609]

10. *Sensitive Query Terms*

[603] *Id.* In the September 2021 order, the FISC referenced FBI's assertion that, out of over two million queries, none were performed for evidence of a crime only purposes.

[604] *Id.* at 13.

[605] *Id.* at 14.

[606] 2021 Government's Submission in Response to the Court's Questions Regarding FBI Queries, *supra*, at 27-28.

[607] *Id.*

[608] Id.

[609] *Id.* at 32-33.

As described above, sensitive query terms can have a greater potential for abuse.[610] FBI sensitive query policy covers persons such as elected officials, members of the media, members of academia, and religious figures.[611] NSA's sensitive query policy covers professions and organizations deemed integral to the exercise of First Amendment protected rights and the protections of democratic political system.[612] For example, following oversight reviews at FBI field offices, DOJ reported that queries of individual members of Congress were conducted for the following reasons: to evaluate whether any criminal or national security threat existed toward him/her; to follow up on information regarding threats of planned civil unrest;[613] or to assess foreign influence threats to the 2020 election.[614] In each of these examples, DOJ and ODNI found that the queries lacked a sufficient justification to explain why the query terms would be reasonably likely to return foreign intelligence information or evidence of a crime from Section 702-acquired information, and therefore these queries violated the query standard.[615]

D. Compliance Issue Mitigation Measures

Between 2020 and 2022, in response to the notable compliance issues with FBI's querying of raw Section 702-acquired information, FBI made significant changes to its internal compliance structure and functions, especially as they pertain to queries. Some of these changes were in response to directives issued by the FISC[616] or DOJ,[617] while others were implemented as a matter of policy. Although each of these changes has been described in the preceding sections of this Report, the Board understands that whether and to what extent these changes will have an impact remains to be seen. Further, in Part 4 of this Report, the Board discusses the extent to which, as a

[610] Preventative measures, such as requiring internal pre-query approval, have reduced the likelihood of such abuse.

[611] FBI Sensitive Query Guidance, *supra*, at 7.

[612] NSA Training, USP Queries, *supra*, at 10.

[613] In this instance, the FBI personnel was unaware the subject of the query was a member of Congress. 27th AG SAR, *supra*, at 127.

[614] Id. at 127-28.

[615] *Id.*

[616] FISC 2021 Querying Violations Order, *supra*.

[617] Memorandum from Merrick Garland, Att'y Gen., to the Deputy Att'y Gen. et al., "Further Augmenting the Internal Compliance Functions of the Federal Bureau of Investigation" (April 22, 2021) (directing FBI to submit a detailed work plan regarding its implementation of Attorney General Barr's memorandum, and to set specific, measurable goals and to create performance metrics to reduce FISA compliance error rates and establish a timeline for completing specified program audits); "Augmenting the Internal Compliance Functions of the Federal Bureau of Investigation," *supra* (directing FBI to establish OIA and undertake a variety of auditing, assessment, compliance, and oversight measures applicable to its national security authorities).

policy matter, these changes are sufficient to address the privacy and civil liberties risks posed by current query practices.

The following are some of the measures FBI implemented in the last few years to facilitate compliance with the FISA, and thus Section 702, querying requirements:

- Establishment of FBI Office of Internal Auditing: FBI established OIA in 2020 in order to develop multiple auditing programs in connection with FBI's national security activities.[618] As discussed above, FBI OIA has conducted two audits of queries conducted by FBI personnel.[619]

- Elimination of Pre-Populated Common Justifications for U.S. Person Query Terms: In 2021, FBI modified its systems containing unminimized Section 702 information to eliminate pre-populated common justifications for U.S. person queries, so that personnel record a case-specific justification for a query using a U.S. person query term before accessing any content retrieved by such a query from unminimized Section 702-acquired information.[620] These case-specific justifications are subject to review and audit by DOJ as part of its regular oversight reviews.

- Requiring FBI Personnel to "Opt In" to Query Unminimized Section 702 Information: In summer 2021, FBI changed the default settings in the databases where it stores unminimized Section 702-acquired information so that FBI personnel need to affirmatively "opt in" to querying unminimized Section 702 information.[621]

- Ensuring Heightened Approvals on Batch Job FISA Queries: Also in summer 2021, FBI instituted a policy requiring FBI personnel to obtain attorney approval prior to conducting a "batch job" query involving 100 or more query terms.[622] In summer 2023,

[618] 27th AG SAR, *supra*, at 115.

[619] Attachment C—List of Significant Changes to FBI Section 702 Program, *supra*, at 4.

[620] June 2023 Joint Statement to Senate Judiciary, *supra* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

[621] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation). This system change was designed to address the large number of inadvertent queries of Section 702 information in which FBI agents and analysts did not realize their queries would run against such collection. Historically, users' queries automatically queried unminimized FISA collection, including Section 702 information, in these databases if they had been authorized to access Section 702 information unless they elected to opt out of having their query run against unminimized FISA collection.

[622] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation). The FBI attorney pre-approval requirement was designed to ensure that there was additional review of situations where one incorrect decision could have a greater privacy impact due to the large number of query terms.

FBI announced plans to begin requiring attorney approval for batch job queries of any size.

- Supplemental Guidance and Mandatory Training on Query Standards: In November 2021, DOJ sent comprehensive querying guidance to FBI.[623] FBI provided this guidance to all FBI personnel with access to unminimized FISA-acquired information, including Section 702-acquired information. In December 2021, FBI instituted new mandatory training on that guidance. This query training was expanded and updated at the end of 2022, and is now required annually for all FBI personnel with access to unminimized FISA-acquired information.[624] In addition, the text of FBI's Section 702 querying procedures was revised to more clearly spell out the query standard to FBI personnel.

- New Restrictions and Oversight of Sensitive Queries: In March 2022, FBI instituted a new policy requiring enhanced pre-approval requirements for certain "sensitive" queries, such as those involving elected officials, members of the news media, members of academia, or religious figures.[625] Under the new policy, FBI's Deputy Director needs to personally approve certain queries before they can be conducted.[626] This measure was designed to ensure that there was additional review at a leadership level of certain queries that reflect particular investigative sensitivities.[627]

[623] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation). All FBI personnel with access to unminimized FISA information are required to complete the training or lose access to FISA systems. The guidance and mandatory training directly address misunderstandings about the rules applicable to queries of unminimized FISA information and instruct personnel on how to apply the query rules.

[624] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation). All FBI personnel with access to unminimized FISA information are required to complete the training or lose access to FISA systems. The guidance and mandatory training directly address misunderstandings about the rules applicable to queries of unminimized FISA information and instruct personnel on how to apply the query rules.

[625] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

[626] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

[627] *Id.* (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

PART 4: POLICY ANALYSIS

In the Board's 2014 Report, the Board included a "Policy Analysis" section that analyzed both the value and privacy implications of the Section 702 program, as well as a Legal Analysis section.[1] The Board assessed the advantages and unique capabilities of Section 702, its contributions to counterterrorism, and its contributions to other foreign intelligence efforts, concluding that the program was highly valuable. It also reviewed the privacy and civil liberties implications of the Section 702 program, finding that the program posed privacy concerns.

With this updated review, the Board concludes that Section 702 remains highly valuable to protect national security, and that it creates serious privacy and civil liberties risks.[2] To assess the overall impact of the Section 702 program, these privacy and civil liberties risks must be measured against the value that the Section 702 program provides. The Board believes that the privacy and civil liberties risks posed by Section 702 can be reduced while preserving the program's value in protecting Americans' national security.

I. Value of the Section 702 Program

The Board assesses that the Section 702 program has been highly valuable in protecting the United States from a wide range of foreign threats, including terrorist attacks in the United States and abroad, cyber-attacks on U.S. critical infrastructure, and both conventional and cyber threats posed by the People's Republic of China (PRC), Russia, Iran, and the Democratic People's Republic of Korea (DPRK).[3] Information collected under Section 702 informs national decision-makers; provides insight into foreign adversaries' organizational goals, strategies, and objectives; and can identify the capabilities of hostile actors.

Furthermore, Section 702 collection has become more valuable in certain key respects relative to other sources of intelligence. For example, the reduced U.S. military footprint in numerous regions of the globe has increased the need to find new means of gathering information. In addition, the IC has evolved its use of Section 702-acquired information to operate in conjunction with foreign intelligence collection under other authorities.

[1] Notably, the 2014 Board's recommendations were explicitly framed as policy recommendations.

[2] The Board recognizes that a preliminary question when assessing any surveillance program involves whether the collection program is legally authorized. The Board's 2014 report contained a legal analysis section, which included a statutory analysis, constitutional analysis, and analysis of treatment of non-U.S. persons. For this 2023 Report, however, the Board has chosen not to include a legal analysis section. As in 2014, the Board presents a policy analysis followed by a series of policy recommendations.

[3] Off. of the Dir. of Nat'l Intel., Annual Threat Assessment of the U.S. Intelligence Community, at 4 (2023).

The following section describes Section 702's value in both quantitative and qualitative terms, based on information including statistics on the use of information acquired from Section 702 collection in intelligence reporting, descriptions of the unique features of Section 702 that differentiate it from other intelligence collection methods, and examples of intelligence operations in which Section 702-acquired information provided unique value.

A. Value to National Decision-Makers

The Section 702 program is part of a complex intelligence enterprise that assists decision-makers up to and including the President in responding to the most pressing threats facing the United States. A useful indicator of the program's value is the information it provides to policy-makers. At the highest level, that information is provided in the President's Daily Brief (PDB), a classified summary of intelligence and analysis on key national security issues produced daily for the President and key administration officials. The PDB is coordinated and delivered by ODNI with contributions by NSA and other IC elements.[4] It includes reports from the most sensitive intelligence sources and presents the IC's best insights on national security threats. According to the NSA, in 2022, information "sourced to" Section 702 supported 59 percent of articles in the PDB.[5] Other reports containing Section 702-acquired data are widely disseminated to officials with a need to know at relevant departments and agencies. From December 2020 through May 2021, NSA, FBI, NCTC, and CIA distributed tens of thousands of reports based on minimized Section 702-acquired intelligence.[6] According to NSA, the value of Section 702 outweighs its cost, since in 2022, nearly 20 percent of all NSA intelligence reporting relied entirely or in part on Section 702-acquired data,[7] whereas the unique costs of the program account for less than 4 percent of NSA's collection budget.[8] The Board did not receive estimates for the cost of paying providers compelled to provide assistance under Section 702, or for supporting costs such as targeting, analysis, or reporting of this collection at NSA or any other agency involved in the FISA Section 702 program.

[4] *See* Off. of the Dir. of Nat'l Intel., *What is the PDB?*, https://intelligence.gov/publics-daily-brief/presidents-daily-brief (last visited July 31, 2023).

[5] Off. of the Dir. of Nat'l Intel. et al., Section 702 of the Foreign Intelligence Surveillance Act, at 4, 8 (2023).

[6] Off. of the Dir. of Nat'l Intel., PCLOB's Questions Submitted to ODNI on 28 September 2022, ODNI's Responses dated 20 December 2022, at 1 (Dec. 20, 2022). Minimized Section 702 information includes U.S. person information that is "masked," as described in Part 3.

[7] Nat'l Sec. Agency, Responses to PCLOB Request Numbers 18, 20, 24 (dated August 31, 2022), at 5 (Jan. 25, 2023) [hereinafter Responses to PCLOB Request Numbers 18, 20, 24].

[8] Priv. and C.L. Oversight Bd., *Public Forum on Foreign Intelligence Surveillance Act (FISA) Section 702*, at 19 (Jan. 12, 2023) [hereinafter PCLOB Public Forum] (keynote speech by General Paul M. Nakasone, Nat'l Sec. Agency). Section 702 is part of an NSA budget, which collectively delivers Section 702 upstream and downstream collection, as well as Title I FISA. NSA has pointed out, however, that this portion of the budget does not include supporting costs such as targeting, analysis, or reporting of this collection at NSA or any other agency involved in the FISA Section 702 program.

According to the U.S. Department of State (DOS), DOS relies on Section 702-acquired information in carrying out its diplomatic mission. For example, a DOS official reported that Section 702 information "enabled U.S. diplomats to demarche a Middle Eastern country over its efforts to monitor and track dissidents abroad… helped expose efforts by foreign powers, including the PRC, to coerce nations to oppose international responses to human rights violations… [and] allowed the State Department and other agencies to notify partners and allies about illicit North Korean activities."[9]

B. Unique Capabilities

Section 702's value is based in part on the program's unique capabilities to collect intelligence. As the Board explained in 2014, Section 702 offers certain advantages over Executive Order 12333 (E.O. 12333) with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. E.O. 12333 collection, by contrast, may not be as secure, complete, or reliable as collection from platforms maintained by U.S. service providers. Additionally, Section 702 is able to enhance, or in some instances when necessary, replace other forms of collection.

In some regions of the world communications infrastructure is limited, which impairs the government's ability to collect signals intelligence under other authorities. Intelligence collection regarding these regions would be greatly impaired without the Section 702 program.[10] In other parts of the world where current on-the-ground U.S. capability is sparse or significantly diminished, Section 702 capabilities are particularly important.[11] Because it involves the use of U.S.-based companies' communications infrastructure, Section 702 gives U.S. intelligence agencies the advantage of collecting with the assistance of sophisticated, technologically advanced communications providers.

Section 702 also has national security advantages over traditional FISA collection under Title I of the statute due to its agility, stemming from the lower legal standards and lack of individualized review by the FISC. Section 702 allows the government to begin monitoring new non-U.S. person targets abroad more quickly, because it does not require FISC review of targeting decisions. Rapidly monitoring new targets allows the government to keep pace with the tradecraft of terrorists and foreign adversaries, who often switch modes of communication to maintain anonymity,

[9] Ctr. for. Strategic and Int'l Studies, *U.S. Diplomacy and Section 702: A Conversation with Assistant Secretary of State Brett Holmgren* (May 30, 2023) (statement of Brett Holmgren, Assistant Sec'y of State, U.S. Dep't of State, Bureau of Intel. and Rsch.).

[10] Off. of the Dir. of Nat'l Intel., *FISA Section 702 Reauthorization* (June 1, 2022).

[11] *Hearing on Annual Worldwide Threats: Hearing Before the H. Permanent Select Comm. on Intel*., 177th Cong. 77 (2022) (statement of Christopher A. Wray, Dir., Fed. Bureau of Investigation).

circumvent surveillance, or evade capture.[12] A senior FBI operations official stated that the agility afforded by Section 702 is "particularly important in a technology environment where foreign threat actors can move to new communications accounts and infrastructure in a matter of hours, if not minutes."[13]

C. Operational Value

In order to evaluate the operational value of Section 702, the Board has compared threats facing the United States with contributions of Section 702-acquired information in countering those threats. Section 702 provides value to the U.S. national security apparatus in a wide variety of direct foreign threats to U.S. lives and property. Indeed, as those threats have evolved over time, the program's value has extended beyond its original focus on counterterrorism and now encompasses broader strategic and defensive goals as well.

The most authoritative source for unclassified information about threats to U.S. national security is the Annual Threat Assessment (ATA) of the U.S. Intelligence Community, an annual unclassified report that was most recently released on February 6, 2023.[14] In its threat assessment, the IC identified two categories of "critical strategic challenges" for the United States: (1) "great powers, rising regional powers, as well as an evolving array of non-state actors" who are vying "for dominance in the global order," including Russia, the PRC, Iran, and the DPRK;[15] and (2) "shared global challenges" that are "converging as the planet emerges from the COVID-19 pandemic… creating unprecedented vulnerabilities."[16]

As of mid-September 2022, almost 22 percent of NSA reporting on terrorism was sourced in whole or in part to Section 702.[17]

From an operational standpoint, the Section 702 program enables the U.S. government to identify individual threat actors and their networks; find elusive targets; and obtain a uniquely refined and detailed view of their individual targets. Additionally, Section 702 capabilities provide information to facilitate other intelligence collection, while protecting sensitive sources and methods. Information obtained through FISA Section 702 collection has enabled the government to discern both the large scale strategies and small scale decision-making of terrorist organizations and other foreign adversaries.

Certain selected declassified examples are described below in accordance with the categories of threats to which they relate, including counterterrorism, great powers, and regional

[12] PCLOB Public Forum, *supra*, at 89.

[13] *Id.* (remarks by Mike Herrington, Senior Operations Advisor, Fed. Bureau of Investigation).

[14] Annual Threat Assessment, *supra*.

[15] *Id.* at 4.

[16] *Id.*

[17] Responses to PCLOB Request Numbers 18, 20, 24, *supra*, at 5.

powers. Additional examples and further discussion are contained in the Classified Annex to this report (Annex C).

1. *Contributions to Counterterrorism*

As described in Part 1 of this Report, the Section 702 program was started in response to the terrorist attacks of September 11, 2001 as a means to identify foreign terrorists and their networks, including those with connections inside the United States. While foreign-directed terrorism inside the United States has diminished since that time, it remains a "persistent and increasingly diverse threat."[18]

From an operational standpoint, the Section 702 program enables the U.S. government to identify individual threat actors and their networks; find elusive targets; and obtain a uniquely refined and detailed view of their individual targets… [This] has enabled the government to discern both the large scale strategies and small scale decision-making of terrorist organizations and other foreign adversaries.

As the Board stated in 2014, the Section 702 program has proven valuable in a number of ways to the government's efforts to combat these foreign threats. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown foreign terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown foreign terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

After more than 15 years of operation, the Section 702 program continues to provide the United States with intelligence that has been critical to discovering and disrupting foreign terrorist plots. Foreign terrorist organizations use a number of practices to obscure their membership and activities. Section 702 collection is used to monitor known foreign terrorists, suspected terrorists, and those in contact with them to enable the government to identify previously unknown individuals and their associates. Moreover and similar to situations involving other signals intelligence collected and stored in a database, a U.S. intelligence analyst investigating foreign terrorism can follow up on a new or existing lead by querying a database of already-collected Section 702 information. The information collected from Section 702 has enabled the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics.

[18] Annual Threat Assessment, *supra*, at 31.

Section 702 collection also provides a uniquely refined and detailed view of individual targets that can help the intelligence agencies to find them, which can be particularly important when members of a terrorist group may be spread all over the world. Members of a terrorist network might freely discuss their current or intended whereabouts in their communications. The flexibility of Section 702 collection further enables the government to effectively maintain coverage on specific individuals if they attempt to switch their modes of communication.

Section 702-acquired information has been combined or used in operations that led to the disruption of a foreign terrorist plot or to the death of terrorist leaders, as described in the following examples:

- Section 702 provided the IC access to critical information that assisted the United States in finding Ayman al-Zawahiri, Osama bin Laden's successor as leader of al-Qa'ida. This information, supplemented by other surveillance, was briefed to the President in order to secure his approval for a missile strike to kill Zawahiri in July 2022.[19]

- In 2020, Section 702-acquired information allowed analysts to identify members of a terrorist cell that was planning an attack on a U.S. facility in a Middle Eastern country. Analysts were able to monitor the group's communications through Section 702 information.[20] As U.S. intelligence-gathering focused on this plot, Section 702 was a critical, unique collection method in gathering information for the government because of the terrorists' travel through multiple countries.[21] The U.S. government, working with allies in the region, was able to disrupt the attack.

- Section 702 informed planning for the February 2022 U.S. military operation that resulted in the death in Syria of Hajji 'Abdallah, the leader of ISIS. Section 702 collection on Hajji 'Abdallah contributed to the U.S. assessment of the ISIS leader's presence in Syria. This information provided military planners and senior policy-makers confidence in their decision to send U.S. troops on the mission.[22]

2. *Contributions to Strategic Competition with Major Powers*

As discussed above, the Section 702 program is not aimed exclusively at preventing terrorism but also serves other foreign intelligence and foreign policy goals. The importance of the program to those goals has increased since 2014, as nation-state adversaries such as the PRC and Russia have taken increasingly hostile positions toward the United States. The ATA

[19] Intel. Cmty. Telephone Briefing for Priv. and C.L. Oversight Bd. Staff (Mar. 16, 2023) [hereinafter IC Briefing March 16, 2023].

[20] *Id.*

[21] Off. of the Dir. of Nat'l Intel., Briefing: FISA Section 702 Reauthorization (June 1, 2022) [hereinafter ODNI Briefing on FISA Section 702 Reauthorization].

[22] *Id.*

underscored that "the era of nation-state competition and conflict has not been relegated to the past but instead has emerged as a defining characteristic of the current era."[23]

The PRC, in particular, has engaged in wide-ranging efforts to extend its influence and reduce that of the United States, especially in the developing world. The ATA describes these efforts as Beijing "project[ing] power globally while offsetting perceived U.S. military superiority."[24] Section 702 has made direct contributions to countering these efforts. For example, Section 702-acquired information has enabled the United States to gain insights into the PRC's efforts to monitor, track, and persecute Chinese nationals believed to be dissidents.[25]

Similarly, Section 702-acquired information has proved integral in attempts to counter Russian aggression. The ATA assesses that "Russia's military action against Ukraine demonstrates that it remains … intent on using whatever tools are needed to try to reestablish a perceived sphere of influence..."[26] Section 702 is used by the IC and the policy-makers it supports to respond to Russian efforts across sectors.[27]

Section 702 has been particularly valuable in gathering intelligence regarding Russia's invasion of Ukraine. On an operational level, Deputy Attorney General Lisa Monaco testified to Congress that Section 702 helped the government uncover gruesome atrocities in Ukraine—including the murder of noncombatants and the forced relocation of children from occupied areas to Russia—and that Section 702 information and other information "has helped us as a country and as a national security community galvanize accountability efforts regarding Ukraine by allowing us to confidently and accurately speak with the international community about atrocities."[28]

Likewise, Section 702 has been valuable in combatting threats from other foreign adversaries. For example, Section 702-acquired information has supported the FBI's investigation of Iranian state-supported hackers' efforts to spear-phish a wide variety of U.S. victims. U.S. person queries of FISA Section 702 holdings allowed the FBI to determine that the hackers were in the process of gathering information on one of the possible victims, a former head of a Federal

[23] Annual Threat Assessment, *supra*, at 4.

[24] *Id*. at 7.

[25] Email from Off. of the Dir. of Nat'l Intel. to Priv. and C.L. Oversight Bd. Staff (June 13, 2023).

[26] Annual Threat Assessment, *supra*, at 4.

[27] IC Briefing March 16, 2023, *supra*.

[28] Holding Russian Kleptocrats and Human Rights Violators Accountable for Their Crimes Against Ukraine: Hearing Before the S. Comm. on the Judiciary, 118th Cong. (2023) (statement of Lisa O. Monaco, Deputy Att'y Gen., U.S. Dep't Of Just.).

Department. With this information, the government was able to notify and warn the potential victim, and provide defensive advice to stay ahead of the threat.[29]

3. *Contributions to Defending Against Cyber-Attacks*

As part of their efforts to counter U.S. influence, degrade U.S. technological superiority, and find weaknesses in the U.S. homeland, our adversaries use cyberwarfare capabilities and proxies to attack U.S. digital and physical infrastructure. Section 702 collection has facilitated U.S. efforts to counter a variety of cyber threats.

- For example, in 2022, Section 702 allowed the FBI to discover that state-supported hackers had infiltrated computer systems on utilities in several locations in the U.S.[30] The FBI was able to warn the systems' operators, help them expel the hackers from their systems, and monitor other infrastructure for further victims.[31]

- In addition, in a high profile example, Section 702 played an important role in the U.S. government's response to the cyber attack involving Colonial Pipeline in 2021. Using FISA Section 702, the Intelligence Community acquired information that verified the identity of the hacker, as well as information that enabled U.S. government efforts to recover the majority of the ransom.

4. *Contributions to Slowing Proliferation of Weapons and Theft of Advanced Technologies*

"Transnational threats interact in a complex system along with more traditional threats such as strategic competition, often reinforcing each other and creating compounding and cascading risks to U.S. national security."[32] The proliferation of weapons of mass destruction and the theft of advanced technologies with military applications exemplify this complexity as they relate to Russia, Iran, and other nation-states. The Section 702 program has helped the United States better understand this complex system and take actions to protect U.S. national security interests in response.

- Section 702-acquired information allowed the FBI to disrupt a foreign state actor's operation and prevent it from gaining access to sensitive technology that is used around the world. Specifically, a NATO ally informed the United States it was investigating a spy who was attempting to recruit individuals who could gain access to U.S. companies, leading to the United States and the ally jointly investigating the spy. Using

[29] Fed. Bureau of Investigation, Additional U.S. Person Query Examples, at 2 (Apr. 7, 2023) [hereinafter FBI Additional U.S. Person Query Examples].

[30] IC Briefing March 16, 2023, *supra*.

[31] *Id.*

[32] Annual Threat Assessment, *supra*, at 26.

information collected under its Section 702 authority, the United States was able to confirm connections between the spy and the company that was developing the technology. The United States warned the company and provided Section 702-acquired information to the allied country, which that country was not otherwise able to obtain.[33]

- In another case, CIA relied on Section 702-acquired information, including conducting U.S. person queries, to support U.S. efforts to prevent an adversary from purchasing dozens of items from the United States that were essential to the development of advanced technical capabilities.[34]

- Finally, after receiving intelligence from another agency that a U.S. person was in contact with intelligence officers from a particular threat country, the FBI queried that U.S. person's identifiers against the FBI's Section 702 collection. The queries returned results from collection on intelligence officers of a different threat country. Those results confirmed that the U.S. person had been in contact with officers from the first threat country. The FBI subsequently investigated, determined the U.S. person to be unwitting of the illicit activities of the intelligence officers, and interviewed the U.S. person, obtaining important intelligence on a hostile foreign state's attempts to acquire sensitive information relating to proliferation of weapons of mass destruction."[35]

D. Value of Upstream Collection

As discussed in Part 3, upstream acquisition occurs with the compelled assistance of providers that control the telecommunications "backbone" over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies. Unlike in 2014, upstream collection no longer includes the acquisition of "abouts" communications (communications in which the selector of a targeted person is contained within the communication but the targeted person is not necessarily a participant in the communication). NSA changed how it conducts upstream collection to ensure that it collects only those communications that are directly "to" or "from" a foreign intelligence target. The changes NSA instituted in 2017 were designed to retain the upstream collection providing the greatest value to national security while reducing the likelihood that NSA would acquire communications of U.S. persons or others who are not in direct contact with a foreign intelligence target. The potential for the acquisition of "multi-communication transactions" (MCTs) (an Internet transaction that

[33] Off. of the Dir. of Nat'l Intel., Briefing: FISA Section 702, Protecting the Nation (Sept. 21, 2022).

[34] Intel. Cmty. Briefing for Priv. and C.L. Oversight Bd. (Mar. 15, 2023).

[35] FBI Additional Query Examples, *supra*.

contains more than one discrete communication within it) still exists, but these MCTs consist solely of communications to or from a target overseas.[36]

Because of these changes, along with additional pre-tasking research and analysis, upstream collection is significantly more focused to acquire only target communications.

Upstream collection remains valuable for several reasons. First, upstream collection offers access to targets' communications where they use non-U.S. ECSPs.[37] For example, downstream collection cannot work against targets using non-U.S. email providers. The U.S. government cannot serve foreign providers with Section 702 directives or compel them to produce target communications.[38] However, so long as a target's communications transit U.S. backbone facilities, they may be acquired through upstream collection.

Second, upstream collection allows the IC to expand the range of material gathered against one target. Because the individual taskings are sent to telecommunications backbone providers rather than individual service providers, many types of communications can potentially be collected with a single directive to a single provider.[39]

E. Value of U.S. Person Queries

As described in Part 3, intelligence agencies use queries of Section 702 data, including U.S. person queries, as an investigative and intelligence tool that permits an agency to efficiently assess whether it possesses relevant foreign intelligence information (or for FBI, also evidence of a crime) in its Section 702-acquired information.[40] FBI personnel rely on queries as a preliminary step designed to return focused information. They help personnel "connect the dots"—that is,

[36] *See* Priv. and C.L. Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 39-40 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%20%2014%202022%201548.pdf [hereinafter 2014 PCLOB Report] (describing how MCTs can be collected even when the transactions only involve communications to or from the target).

[37] *See id.* at 35.

[38] *See id.* (explaining that upstream enables collection with the compelled assistance of providers that control the telecommunications backbone, occurs "in the flow of communications between communication service providers," and includes collection of communications where the targeted person interacts with "foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive.").

[39] *Id.* at 35 n.123 (citing to the statement of Rajesh De, Gen. Couns., Nat'l Sec. Agency ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

[40] As of February 2023, FBI received data from only 3.2% of all IC Section 702 targets. Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2022, at 22 (Apr. 2023) [hereinafter CY2022 ASTR].

uncover plots, identify bad actors, and recognize links between foreign intelligence targets and U.S. persons.[41]

U.S. person queries are central to how FBI utilizes its Section 702 authorities. Intelligence agencies may conduct queries initially to verify or follow up on lead information, to determine whether a lead merits opening an investigation, and to advance ongoing investigations.[42] U.S. person queries can be used to uncover links between U.S. persons and foreign intelligence threat actors.

The vast majority of FBI's U.S. person queries of Section 702 information that are conducted return no results. For example, in 2022, FBI personnel accessed content returned by a U.S. person query for only 1.58% of such queries.[43] The government argues the return of no results is a value in itself, as it allows personnel to rule out certain leads. The FBI in particular struggled to provide the Board with affirmative examples of the unique value of U.S. person queries of Section 702 information in criminal investigations, and to date, the government has been unable to identify a single criminal prosecution arising from U.S. person queries.

The vast majority of FBI's U.S. person queries of Section 702 information that are conducted return no results. For example, in 2022, FBI personnel accessed content returned by a U.S. person query for only 1.58% of such queries.

The strongest examples of the value of U.S. person queries provided to the Board involve so-called "victim queries," or what the government now refers to as "defensive queries."[44] In particular, the government has identified instances in which U.S. person queries provided a means to investigate whether hostile cyber actors have compromised individuals' or organizations' electronic communications and to enable the agency to focus its outreach to the potential victims. In addition, these searches can allow the government to investigate whether a particular U.S. person may be a potential victim of a hostile foreign actor.

[41] In analyzing the intelligence and systemic failures that facilitated the September 11, 2001 attack, the 9/11 Commission assessed that "[t]he U.S. government has access to a vast amount of information . . . [b]ut the U.S. government has a weak system for processing and using what it has." THOMAS H. KEAN & HAMILTON H. LEE, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS ON THE UNITED STATES, at 416-17 (2004) [hereinafter 9/11 Commission Report]. The Commission thus concluded that "the importance of integrated, all-course analysis cannot be overstated. Without it, it is not possible to connect the dots." *Id.* at 408.

[42] Off. of the Dir. of Nat'l Intel., *Section 702 Overview*, at 10, dni.gov/files/icotr/Section702-Basics-Infographic.pdf (last visited July 31, 2023).

[43] Intel. Cmty. Briefing for Priv. and C.L. Oversight Bd. Staff (May 2023).

[44] PCLOB Public Forum, supra; see Charlie Savage, FBI Feared Lawmaker Was Target of Foreign Intelligence Operation, N.Y. TIMES (Apr. 13, 2023).

In many instances, the government has been able to contact potential victims to warn them of intrusions or possible attacks, to obtain from them their online account identifiers (such as their email addresses), and to work with these individuals to disrupt or mitigate the hostile action.

For example, the FBI used U.S. person queries against Section 702-acquired information to identify the extent of a foreign government's transnational repression activities, which included kidnapping and assassination plots. The timely identification of the foreign government's plans and intentions in Section 702-acquired information contributed to the FBI's ability to warn the victims and disrupt the plots.

F. Value of Batch Queries

So-called "batch queries"—queries through which FBI personnel search Section 702 information with hundreds or thousands of query terms at once—allow analysts to process larger sets of identifiers with greater speed when the terms in the batch share a common query justification. Batch queries may arise when, for example, an intelligence agency acquires a terrorist's phone and hundreds of contacts are contained in that phone. Investigators and analysts may seek to search each and every known contact in the Section 702 database to determine more information regarding how those contacts are connected to the target and whether any of those contacts are connected to other terrorist associates, either in the United States or abroad. The batch query allows the investigator or analyst to run a single query using all of the contact information, rather than running hundreds of separate queries on individual contacts.

Importantly, the batch query tool also enables analysts to detect connections among the query terms. As demonstrated in the example of a batch query in Part 3, running query terms as a batch may reveal otherwise unknown connections between the query terms themselves, such as whether multiple email addresses "hit" against information acquired in the same investigation or similar types of investigations (e.g., multiple email addresses "hit" against information collected in more than one counterterrorism investigation). Running batch query terms in various combinations can also identify connections between those terms or individuals, for example by showing that several contacts on the list are communicating with each other, providing important intelligence information about networks. The Board did not review whether there could be less intrusive methods to batch queries that would reveal interconnections among query terms within the Section 702 databases.

G. Efficacy

In its 2014 Report, the Board stated that counterterrorism surveillance programs "can serve a variety of functions" and that the efficacy of such programs is "difficult to assess."[45] The Board explained that "[b]ecause the nature of counterterrorism efforts can vary, measures of success may

[45] 2014 PCLOB Report, *supra*, at 148.

vary as well," and consequently "the number of 'plots thwarted' in this way is only one measure of success." This is especially true because "individual counterterrorism programs are not typically used in isolation; rather, these programs can support and mutually reinforce one another." Accordingly, the Board recommended that "the government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs."[46] The Board explained that in the absence of such measures, "policy-makers and courts cannot effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties it may cause."[47]

In response to the Board's recommendation, ODNI in 2016 published a four-page report entitled "Process for Assessing the Efficacy of Intelligence Programs," in which it stated that the IC "uses a range of processes to assess efficacy and value" and that "[it] believe[s] that together, these processes address the concerns that underlie the Section 702 Report's recommendation." Those methods were to (a) ensure that the IC abides by the National Intelligence Priorities Framework and that policy-makers validate each priority with respect to the anticipated intelligence value from collection; (b) refine processes for selecting SIGINT targets in response to intelligence priorities to ensure that SIGINT concerns were considered alongside other risks and benefits; and (c) assess IC reporting by providing ODNI monthly reports to policy-makers summarizing the quality and relevance of the IC's reporting against priorities.[48] In the Board's view, the 2016 report falls short of identifying a method that accurately and succinctly articulates the degree to which Section 702 has advanced the government's counterterrorism and other national security goals, and the IC has not developed a comprehensive methodology since that time.[49] The Board regrets that, as Section 702 is being considered by Congress for reauthorization, the IC has not produced a methodology to convey properly the impact of Section 702 and its value relative to other surveillance authorities.

II. Privacy and Civil Liberties Implications

This 2023 Report builds on the analysis of privacy and civil liberties risks outlined in the 2014 Report, and updates that analysis as needed based on new information or new uses or practices authorized by Section 702. The Board finds that Section 702 poses significant privacy and civil liberties risks, most notably from U.S. person queries and batch queries. Significant privacy and civil liberties risks also include the scope of permissible targeting, NSA's new approach to upstream collection, a new sensitive collection technique that presented novel and

[46] *Id.*

[47] *Id.*

[48] Off. of the Dir. of Nat'l Intel., Processes for Assessing the Efficacy and Value of Intelligence Programs, at 1-2 (Feb. 9, 2016).

[49] Priv. and C.L. Oversight Bd., Recommendations Assessment Report, at 23-24 (2022).

significant legal issues approved by the FISC in 2022, how data is initially ingested into government repositories, incidental collection, and inadvertent collection.

Since 2014, public attention both in the United States and internationally has focused on concerns about the privacy and civil liberties implications of government surveillance programs. This has related to both commercial and government access to private communications and other electronic information, and the interconnection between the two. This interconnection is relevant in the context of Section 702, which involves the U.S. government's access to private communications from, and with the compelled assistance of, U.S. electronic communication service providers. The analysis that follows covers the key issues identified during the Board's review, to the extent practical given the breadth and complexity of the program and the constraint of protecting classified material.

A. Targeting and Collection

1. *Scope of Permissible Targeting*

As an initial matter, the definition of "foreign intelligence information" that may be collected under FISA is very broad. Thus, although Section 702 permits the government to acquire only information within the scope of one of the topics or certifications approved by the FISC, the statute technically could authorize far more extensive collection. This includes any "information that relates to" the ability of the United States to protect against a variety of national security threats and harms, and also information related to "the conduct of the foreign affairs of the United States."[50]

The government has not sought to use Section 702 to collect information extending to the outer bounds of the FISA definition of foreign intelligence information, and authorized collection has been limited to the specific certifications approved by the FISC. Moreover, the Executive Branch has adopted further limitations through E.O. 14086 on Enhancing Safeguards for United States Signals Intelligence Activities. As discussed in Part 2 above, this executive order, issued in October 2022, narrows the breadth of information the intelligence community is authorized to collect by limiting the use of signals intelligence to twelve specific categories.[51] The Board agrees that the purposes authorized under the three Section 702 certifications fit within the twelve legitimate objectives, and these limitations should help ensure that the government will not conduct surveillance to the full scope of the FISA definition of foreign intelligence information.[52]

2. *Targeting Individuals*

[50] 50 U.S.C. § 1801(e).

[51] Exec. Order No. 14,086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

[52] *Id.*

The Board finds that Section 702's targeting presents a number of privacy risks and harms by authorizing surveillance of a large number of targets, providing only programmatic review of a surveillance program, allowing extensive incidental collection, and causing inadvertent collection. The FISC reviews and approves targeting procedures to minimize the risks of improper surveillance, but there is no individualized judicial review of targeting decisions.

First, signals intelligence authorized by Section 702 results in an extremely large amount of collection.[53] Surveillance of individuals in any form invariably risks intruding on privacy and civil liberties. In CY2022, the Section 702 program targeted approximately 246,073 non-U.S. persons located abroad,[54] which represents a 276% increase since CY2013. The surge in Section 702 targeting in recent years increases the privacy and civil liberties risks, both for actual targets and for those whose information has been incidentally or inadvertently collected. It also increases the privacy harms when those targets' non-public communications are non-consensually screened, analyzed, retained, used, and disseminated by the government. While Section 702 relies upon individual targeting decisions by analysts, the government is able to acquire and store substantial amounts of data—including incidentally collected U.S. person information—that goes beyond what the government could collect under other authorities such as Title I of FISA, because the standards for targeting under Section 702 are by design less rigorous than those governing surveillance targeting persons within the United States. Though the Board recognizes that Section 702 is not "bulk" collection, the program lacks individualized and particularized judicial review of targeting decisions, posing risks that targeting can be overbroad or unjustified. These risks are increasing as the target numbers and their associated selectors continue to grow.

In CY2022, the Section 702 program targeted approximately 246,073 non-U.S. persons located abroad, which represents a 276% increase since CY2013. The surge in Section 702 targeting in recent years increases the privacy and civil liberties risks, both for actual targets and for those whose information has been incidentally or inadvertently collected.

In some instances, persons targeted under Section 702 could instead be targeted under other legal authorities, such as Title I of FISA, which requires the government to demonstrate to the FISC probable cause to believe that the person is an agent of a foreign power. As discussed above,

[53] As noted below, as of calendar year 2022, there were 246,073 persons targeted under Section 702. *See* CY2022 ASTR, *supra*, at 18. Further, as described in the factual narrative of this report, as of 2021, NSA acquired approximately 85.3 million transactions a year in upstream collection, which represents a small percentage of the overall collection under Section 702.

[54] *Id.*

such individualized judicial review under Title I provides greater safeguards for privacy and civil liberties. However, as also described above, Section 702 allows the government to target persons who do not qualify as agents of a foreign power, such as international cyber actors who attack non-U.S. victims, and who are expected to communicate foreign intelligence information.

Thus, while more privacy protective legal authorities like Title I of FISA may be available to the government in many cases, Section 702 enables the government to target a broader array of persons, which also increases the risks of privacy and civil liberties harms. Conversely, in some circumstances, the government may be able to use E.O. 12333[55] or, for certain metadata, National Security Letters, to obtain information similar to that collected under Section 702. Although the Board makes a series of policy recommendations to improve the privacy safeguards under Section 702, it is worth emphasizing that Section 702 provides stronger privacy safeguards than either E.O. 12333 or National Security Letters.

In addition, after reviewing individual tasking sheets, the Board has identified instances in which analysts' written foreign intelligence justifications lack sufficient detail. Although the tasking sheets reviewed by the Board included documentation to demonstrate that targets were reasonably believed to be non-U.S. persons located outside the United States, the documentation of the foreign intelligence purpose for the targeting was not similarly thorough or sufficiently detailed. The tasking sheets stated the foreign intelligence purpose but did not describe or document why the particular target was expected to possess or communicate such information. For example, tasking sheets stated that the target was a member of a particular terrorist group without documenting the basis for this conclusion.[56]

Even if the targeting remains highly accurate, so long as the general upward trend in the number of targets continues and the IC increasingly relies upon Section 702 in the coming years, the privacy risks related to collection will also continue to increase.

Second, Section 702 is a form of programmatic surveillance, in that the FISC approves the program's agency-specific procedures. Programmatic surveillance presents inherent privacy risks because it does not require independent individualized judicial scrutiny at any point in the surveillance program. This means the Court does not scrutunize the selectors or potential individual targets to ensure that targeting is appropriate and meets the foreignness and foreign intelligence purpose requirements.

These standards permit targeting based upon the reasonable belief that a target may possess, receive, or communicate foreign intelligence information and is a non-U.S. person located

[55] The Board has previously reviewed surveillance authorized by E.O. 12333. *See* Priv. and C.L. Oversight Bd., Executive Order 12333 (2021); *see also* Priv. and C.L. Oversight Bd., Additional Unclassified Statement by Board Member Travis LeBlanc (2021).

[56] *E.g.,* U.S. Dep't of Just., Nat'l Sec. Div., Tasking Sheet 4 (Dec. 16, 2022); U.S. Dep't of Just., Tasking Sheet 9 (Dec. 16, 2022).

outside the United States, which, combined with the amount and breadth of information collected under Section 702, creates a significant privacy risk. Targets need not act at the behest of a foreign power. They also don't have to violate U.S. law, or engage in any activities hostile to the United States. For example, the low standards permit the government to target a relative of a terrorist because that relative could have some knowledge of the terrorist's whereabouts. By contrast, in the criminal or traditional FISA context within the United States, the government must establish, based on probable cause, that targets are engaged in clandestine activities, certain criminal actions, or foreign intelligence activities as agents of a foreign power. Under those standards, analysts must obtain and the FISC must approve individualized orders demonstrating that the target is an agent of a foreign power and is engaging in espionage, terrorism, or sabotage, or other foreign intelligence or counterintelligence activities.

It is worth noting, however, that Section 702 limits targeting based on a number of factors to minimize the risks of improper surveillance and to ensure that intrusions upon privacy and civil liberties are taken into account. First, as a threshold matter, a target must be reasonably believed to be a non-U.S. person located outside of the United States.[57] NSA notes that it does not define "reasonable belief" as a "51% to 49% 'foreignness' test."[58] Targets must be expected to possess, receive, or communicate foreign intelligence information within a defined category certified by the Attorney General and the DNI according to priorities established by the President and such categories must be approved for collection by the FISC. Further, in addition to the purpose limitations described above, E.O. 14086 includes provisions originally implemented in Presidential Policy Directive 28 (PPD-28) to protect the privacy interests of non-U.S. persons, such as a prohibition against targeting to suppress free expression or to disadvantage persons on the basis of ethnicity, race, or gender.

Additional privacy issues associated with targeting in downstream collection are discussed in the Annex C to this Report.

3. *Upstream Collection*

Upstream collection involves collecting a target's communications as they transit the Internet backbone, with the compelled assistance of backbone providers, rather than from U.S.-based providers of specific services such as email. The precise roles of NSA personnel and of the

[57] For instance, this can be someone who may possess information "with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States." *See* 50 U.S.C. § 1801(e)(2)(B). The range of foreign intelligence that the government may seek under Section 702 is limited by the certifications approved by the FISC.

[58] Nat'l Sec. Agency, NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, at 4 (2014), https://media.defense.gov/2021/Aug/18/2002833876/-1/-1/0/NSA_REPORT_ON_SECTION_702_PROGRAM.PDF ("Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. this is not a 51% to 49% 'foreignness' test.").

backbone providers compelled to assist with upstream collection, and the nature and types of filtering performed by each, remain classified.

As discussed above, in 2017, NSA suspended upstream "abouts" collection, which involved the collection of communications that were neither to nor from a selector, but instead contained the selector. Since then, NSA has changed its approach to upstream in an effort to ensure that only communications that are actually to or from a target are collected.[59] These changes have substantially reduced the privacy risks stemming from upstream collection under Section 702. The privacy risks from incidental and inadvertent collection remain. In addition, the architecture of upstream collection and the location of collection raise unique privacy issues distinct from other aspects of the Section 702 program.

These issues include risks posed by the possible resumption of "abouts" collection, the screening of a broad set of communications as part of the upstream acquisition process, [60] and the IC's new approach to identifying communications to be acquired in upstream. NSA's compliance regime as well as its software serves to mitigate some, but not all of the harms that result from this new approach to upstream implemented since 2017. However, NSA's new approach to upstream collection results in fewer privacy risks than under the prior approach to upstream that included "abouts" collection.

Even during the first step of the collection in the upstream process, in which raw Internet traffic transiting the Internet backbone is screened for the presence of selectors, privacy harms can occur. Upstream collection does involve limiting the extent of backbone traffic that is subject to screening.[61] Yet, even when traffic is not collected, and even if the screening is automated, the act of screening communications constitutes a serious privacy intrusion. Some civil liberties groups and scholars have contended that this initial screen to determine the presence of selectors itself constitutes a search under the Fourth Amendment.[62]

More specifically, upstream collection requires a more intrusive process than downstream collection to determine whether communications to be collected are those of a target. In

[59] Memorandum Opinion and Order, at 43-67, In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications, Docket No. 702(j)-23-01 and predecessor dockets, In re DNI/AG 702(h) Certification 2023-B and its Predecessor Certifications, Docket No. 702(j)-23-02 and predecessor dockets, In re DNI/AG 702(h) Certification 2023-C and its Predecessor Certifications, Docket No. 702(j)-23-03 and predecessor dockets (FISA Ct. Apr. 11, 2023); see also Off. of the Dir. of Nat'l Intel., IC on the Record Database, https://www.intelligence.gov/ic-on-the-record-database (last visited July 31, 2023).

[60] 2014 PCLOB Report, *supra*, at 37 ("To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases.").

[61] See id.

[62] Although courts have not reached the merits of these claims, Fourth Amendment challenges have been brought in multiple cases. *See, e.g., Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 202, 209-10 (4th Cir. May 23, 2017);

downstream collection, ECSPs produce information associated with a tasked selector. By contrast, in upstream collection, a broader set of potential traffic of interest is screened, which is an inherently more intrusive process. NSA's current approach to upstream is designed to ensure that only communications that are to or from targets are ingested into government databases. However, the process for identifying those communications to be collected involves screening a broader set of traffic transiting the Internet backbone, which necessarily includes communications that are not to or from targets and that will not be ingested into government databases. In addition, although the end of "abouts" collection and the new approach to upstream collection have reduced the likelihood of incidental and inadvertent collection of U.S. person information, that risk remains. Even without "abouts" collection, when compared with downstream there is a higher potential of inadvertent collection, both of purely domestic communications (as the collection takes place at facilities in the United States) and of foreign communications that are neither to nor from a target.

Further, while NSA's filtering techniques for use in upstream collection have improved since the Board's prior review of Section 702, such filtering is still imperfect. In particular, there remains the risk that despite current filtering techniques, upstream collection will lead to government data stores that may contain information that does not constitute foreign intelligence information.

a. Potential to Restart "Abouts" Collection

The Board is unaware of any government interest in, or plans to, restart "abouts" collection. However, as described above, upstream collection previously included "abouts" collection, a practice that raised significant privacy and civil liberties concerns. In collecting communications that were not necessarily to nor from a target, "abouts" collection increased the risk that NSA would collect both wholly domestic communications and "communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications."[63] For these reasons, NSA suspended "abouts" collection in 2017, constituting a key privacy improvement for the program. When Congress reauthorized Section 702 in January 2018, the legislation ended "abouts" collection, but also included a provision allowing the government to restart this collection if it first obtained approval from the FISC and provided notice to Congress.[64] If the NSA were to resume "abouts" collection, the unique privacy risks stemming from such collection could reappear.

In the 2018 FISC opinion approving the government's Section 702 certifications, the court discussed the implications of the "abouts" statutory language and held that the prohibition applies

Order Denying Plaintiffs' Motion for Partial Summary Judgment and Granting Defendants' Motion for Partial Summary Judgment, *Jewel v. Nat'l Sec. Agency*, 2015 WL 545925, *2 (N.D.Cal. Feb. 10, 2015).

[63] 2014 PCLOB Report, *supra*, at 121.

[64] Pub. L. 115-118, 132 Stat. 3, 12 § 103(b).

to downstream collection as well.[65] The court "identified issues concerning the potential applicability of the abouts limitation to some information within the proposed scope of acquisition under the 2018 Certifications" and appointed amici to address whether certain forms of acquisition conducted under the 2018 Certifications involved acquisition of "abouts" communications and thereby fell within the ambit of the FISA Amendments Reauthorization Act.[66]

The declassified FISC opinion provides minimal information as lengthy redactions make it impossible to understand a potential privacy risk related to data collection or the novel and significant legal issue. The declassified opinion conveys that "the government and amici disagree as to whether the abouts limitation has any application to downstream collection."[67] It conveys that a category of information collected under downstream acquisition does not implicate the "abouts" limitation; however, the opinion does not specify what category of information is at issue.[68] The court concluded the forms of acquisition conducted under the 2018 Certifications "would be consistent with the limitation."[69]

While the Board is unable to discuss more in an unclassified format, the Board believes that declassification of more information contained within the court opinion would assist the public and policy-makers to fully understand the specific issues related to downstream collection and the "abouts" statutory language.

b. Privacy Risks Relating to the New Approach to Identifying Communications to be Acquired in Upstream

As noted above, following the suspension of "abouts" collection, NSA developed a new approach to identifying communications to be acquired in upstream. Although, as also noted, the privacy risks in upstream have been substantially reduced, this collection continues to raise privacy risks which are further discussed in Annex C of this Report. It is therefore important that NSA continue to conduct regular and periodic evaluation of upstream collection, and especially this aspect of the program. Certain aspects of upstream collection can cast its net widely, and, as such, are potentially at risk of misuse in the future if the government were to revise or lift the internal controls and policies that prevent such usage. To be clear, the Board found no instances of such misuse nor any evidence that NSA is planning or contemplating such use, and NSA maintains multiple levels of internal review, both pre- and post-targeting, to ensure the compliant use of this technique. However, it is important to ensure continued oversight by the FISC over all uses of this

[65] Memorandum Opinion and Order, at 14, 20, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Oct. 18, 2018) [hereinafter 2018 Cert FISC Opinion and Order].

[66] *Id.* at 14.

[67] *Id.* at 15.

[68] *Id.* at 14.

[69] *Id.* at 16.

collection, as well as external oversight and audits to confirm it is used within the scope of current parameters.

4. *New Highly Sensitive Collection Technique*

The FISC's April 2022 Certification decision discussed another novel and significant issue regarding whether to approve the use of a new sensitive collection technique. Following briefing, including by the amicus, the FISC approved this new technique.[70] Annex C to this Report outlines the use of this technique. As discussed in that annex, this new collection method involves new privacy risks, although the government has taken steps to mitigate those risks. To date, the new collection technique has only been approved for use in very narrow circumstances. If it were used in widespread fashion, it could become extraordinarily intrusive.

5. *Incidental Collection*

Any time Section 702 collection obtains communications between a non-target and a target, the non-target's communication is considered "incidentally collected." For example, when a person targeted for surveillance communicates over the Internet with someone else and the communications are collected, that other person's communications with the target are said to have been "incidentally" acquired. Thus, although Section 702 targets can only be non-U.S. persons, through incidental collection the government acquires a substantial amount of U.S. persons' communications as well. The IC uses the term "incidental" because such collection is not accidental or inadvertent—rather, it is an anticipated collateral result of monitoring a target.[71]

While the term may make this collection sound insignificant, and we do not yet know the scope of incidental collection, it should not be understood as occurring infrequently or as an inconsequential part of the Section 702 program. Further, the scope of Section 702 collection as a whole is extensive. As noted above, as of 2021, NSA acquired approximately 85.3 million Internet transactions a year in upstream collection, which constitutes a small percentage of NSA's Section 702 collection.

Identifying a connection between a target and a U.S. person or person located in the United States can be critical to preventing attacks on U.S. soil, countering other threats to the homeland, or protecting the safety and security of the individual in communication with the target. At the same time, individuals in contact with a target may be unwitting participants or even potential victims. Further, since Section 702 requires that targets be reasonably likely to possess, receive,

[70] Memorandum Opinion and Order, at 120-21, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) [hereinafter Apr. 21, 2022 FISC Opinion and Order].

[71] *See* Priv. and C.L. Oversight Bd., *Transcript of Hearing on Government Surveillance Programs*, at 71 (Mar. 19, 2014), https://documents.pclob.gov/prod/Documents/EventsAndPress/d974abd8-af20-4c8c-8a61-13f4b71ee1ac/20140319-Transcript.pdf [hereinafter PCLOB March 2014 Hearing Transcript] (statement of Robert Litt, former Gen. Couns., Off. of the Dir. of Nat'l Intel.).

and/or communicate foreign intelligence information, and not that the targets themselves be suspected of plotting to harm the United States, individuals in communication with targets may be far removed from terrorism or other threats. Nonetheless, once collected, subject to certain restrictions, U.S. person information may be queried, analyzed, disseminated in intelligence reports, retained, and used as evidence against them in criminal proceedings.[72] Such collection can also be used to initiate targeted surveillance of the individual under alternate legal authorities, or it may be shared with domestic and foreign law enforcement and intelligence partners.

Moreover, through incidental collection, the government can acquire a substantial amount of highly sensitive information about someone who is not a target. By collecting the contents of communications, even though the U.S. persons are not the target, surveillance conducted under Section 702 acquires information that involves private content in which the U.S. persons have an expectation of privacy. This includes text and audio communications generated by the user. The collected material can therefore be highly personal and sensitive, capturing exchanges with loved ones, friends, medical providers, academic advisors, lawyers, or religious leaders, for example. This material can also provide great insight into an individual's whereabouts, both in a given moment and in patterns over time. Further, the knowledge that the government can gather this sort of content can have a chilling effect on speech.[73]

As the Board explained in its 2014 Report on Section 702, from a privacy and civil liberties perspective, incidental collection under Section 702 differs in at least two significant ways from incidental collection that occurs in the course of a criminal wiretap or the traditional FISA process.[74] First, Section 702 allows the government to target a much broader range of people. As noted, collection is not limited to suspected terrorists or others engaged in nefarious activities. Second, Section 702 targeting decisions lack the checks that are part of traditional FISA or criminal electronic surveillance. Namely, because only persons who lack recognized Fourth Amendment rights may be targeted under Section 702, the statute does not require a judge to review and approve individual targets.

a. Scope of Incidental Collection

There is currently no data or transparency identifying the magnitude of incidental collection of U.S. person information. The term "incidental" suggests that it is a small amount, but the government has not provided any actual metrics or estimates. Since the enactment of

[72] *See also* 50 U.S.C. § 1806(c) (describing rules for usage of FISA information in court and administrative proceedings); 50 U.S.C. § 1881e(a) (describing rules for use of Section 702-acquired information as evidence in criminal proceedings where the information concerns a U.S. person).

[73] *See* Leonard Downie Jr. & Sara Rafsky, *The Obama Administration and the Press: Leak investigations and surveillance in post-9/11 America*, COMM. TO PROTECT JOURNALISTS (Oct. 10, 2013), https://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911/.

[74] 2014 PCLOB Report, *supra*, at 115-16.

Section 702, the Intelligence Community has stated that it cannot provide metrics to show the magnitude of incidentally collected U.S. person information. NSA has explained that it is often difficult to determine from a communication the nationality of its participants and that the large volume of collection under Section 702 would make it infeasible to conduct such review and analysis for every communication acquired.[75] Although the Board recommended in the 2014 PCLOB Report that NSA publish several metrics to "provide insight about the extent to which the NSA acquires and utilizes" incidental collection of U.S. person information under Section 702, the NSA has asserted that it is "infeasible" to provide a meaningful estimate of the volume of this collection.[76]

There is currently no data or transparency identifying the magnitude of incidental collection of U.S. person information. The term "incidental" suggests that it is a small amount, but the government has not provided any actual metrics or estimates.

Rigorous and reproducible best estimates or even approximate figures would provide critical transparency in this space. Such insight would promote understanding of the impact Section 702 has on the privacy and civil liberties of U.S. persons. Section 702's minimization procedures are the primary protection for incidentally collected U.S. person information. But without further transparency on the volume of incidental collection, it is difficult to determine whether these safeguards are sufficient. If the magnitude of collection is vast, it would be relevant to the public's understanding of the program and help inform the debate over whether further safeguards are necessary to protect U.S. person information.

b. Incidentally Collected Evidence at Trial

One of the most serious risks to individual civil liberties associated with the incidental collection of U.S. person information is that this classified information collected for intelligence purposes could be used in a criminal prosecution. Although FBI is the only one of the four agencies receiving raw Section 702 collection that has a law enforcement function and FBI generally receives less than 4 percent of the raw information collected under Section 702,[77] the government may use Section 702 information in criminal prosecutions including prosecutions unrelated to the purpose of the original targeting.[78] Under Section 106(c) of FISA, the government

[75] Open Hearing on FISA Legislation: Hearing Before the S. Select Comm. on Intel., 115th Cong. 84 (2017) (statement of Daniel R. Coats, Dir. of Nat'l Intel.).

[76] *See* RECOMMENDATIONS ASSESSMENT REPORT, *supra*, at 21-22; 2014 PCLOB Report, *supra*, at 13.

[77] CY2022 ASTR, *supra*, at 22, 25.

[78] *See* 50 U.S.C. § 1881e(a) (describing rules for use of Section 702-acquired information as evidence in criminal proceedings where the information concerns a U.S. person).

is required to provide notice when it intends to enter into evidence or otherwise use or disclose information obtained or derived from Section 702 in a trial, hearing, or other proceeding against an aggrieved person, namely a person whose communications or activities were subject to electronic surveillance. Pursuant to DOJ guidance, this requirement applies only when the information is relevant to the government's case in chief, or is otherwise detrimental to the defendant (e.g., used in rebutting the defendant's testimony; used at sentencing).[79] As noted in Part 3, the government has provided such notice in just nine criminal prosecutions. The government does not provide notice to criminal defendants when it relies on Section 702 information at earlier stages of a criminal investigation if it does not specifically intend to rely on that evidence or other evidence derived from Section 702 acquisitions at trial.

…[I]n multiple cases, rather than providing notice to criminal defendants of Section 702-derived information, the government has instead sought to develop evidence through other sources without any reliance on FISA-obtained or -derived information… [A]lthough we have no reason to doubt that the government has complied with its statutory notice obligations… these practices can prevent criminal defendants from learning about or being able to challenge evidence obtained through Section 702.

Further, in multiple cases, rather than providing notice to criminal defendants of Section 702-derived information, the government has instead sought to develop evidence through other sources without any reliance on FISA-obtained or -derived information. The lack of notice regarding use at early stages of investigations as well as the practice of relying on alternative sources of evidence even where Section 702 has been used in an investigation create risks that information derived from FISA may still affect the course of any investigation. Additionally, although we have no reason to doubt that the government has complied with its statutory notice obligations, and we recognize that the government chooses to rely on alternative sources of evidence in contexts beyond Section 702 to avoid disclosing sources and methods, these practices can prevent criminal defendants from learning about or being able to challenge evidence obtained through Section 702.

[79] If, however, the Section 702-derived information would divulge sensitive sources and methods or would otherwise be protected from disclosure, the government may make a motion for a protective order to restrict disclosure of classified information pursuant to the Classified Information Procedures Act. Pub. L. 96-456, Oct. 15, 1980, 94 Stat. 2025, as amended, § 3. [This is done through FISA (50 U.S.C. § 1806(f)) rather than CIPA. The government may file for a protective order if disclosure would harm the national security of the United States.]

c. Attorney-Client Communications

The large amounts of incidental collection may include communications between attorneys and their clients. Indeed, multiple sections of each agency's minimization procedures contain detailed guidance on the handling of attorney-client communications. Critical aspects of that guidance are classified and have not been released to the public. When collected, these attorney-client communications, many of which are privileged and protected from disclosure, are another example of the privacy harms of incidental collection, as these are highly sensitive communications in which communicants are expecting confidentiality.

There is no doubt that attorney-client communications are screened, analyzed, acquired, and then stored in government databases. The Board's review uncovered that agencies handle the communications in different ways, minimization procedures have been violated,[80] and better system design would help mitigate these privacy harms.

Under current procedures, FBI differs from other agencies as to the handling of attorney-client communications. NSA, CIA, and NCTC require the destruction of the communication upon a determination that the communication does not contain foreign intelligence information or evidence of a crime. FBI allows the retention of the communication even if it doesn't contain foreign intelligence information or evidence of a crime, subject to the otherwise applicable retention limits specified in the FBI's procedures.

Agency minimization procedures differ among NSA, FBI, CIA, and NCTC, which do not treat attorney client communications consistently due to varying definitions of the terms "attorney-client communication" and "attorney-client privileged communication." The Board is concerned that such inconsistencies may cause confusion potentially leading to compliance incidents.

Lastly, specific to FBI, prior to charging a suspect with a crime based on Section 702-acquired information FBI personnel are required to establish a taint team to review the Section 702 collection to ensure that it does not contain any attorney-client privileged communications that may prejudice the potential defendant. FBI rules require that FBI personnel not assigned to the case be assigned to the taint team as a guard against conflict of interest issues. However, the Board found that FBI does not have a central tracking mechanism for identifying when individuals are charged with a crime in reliance on Section 702-acquired information, so as a result there can be uncertainty among the 56 FBI field offices about whether a criminal indictment is under consideration. This uncertainty increases the risk of taint teams not being properly established, including inadvertently staffing taint teams with personnel who have a connection to the case under review.

[80] *E.g.,* U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions Under Section 702 of the Foreign Intelligence Surveillance Act (Mar. 2022) [hereinafter 27th SAR].

d. Impact on Particular Racial, Religious, or Ethnic Groups

The implication of incidental collection under Section 702 on particular racial, religious, and ethnic groups remains an open question. Because the government does not tag Section 702-collected information in its databases with nationality or other demographic information, it remains unclear whether incidental collection has a greater impact on members of any such groups, risking their privacy and civil liberties at higher rates. In response to the Board's inquiries as to whether the government has assessed whether and to what extent incidental collection under Section 702 may have had a chilling effect on First Amendment-protected activities or a differential impact on any particular groups, the government responded that it has not made such an assessment, stating it has no reliable way to do so.[81]

Indeed, as a threshold issue, currently the government does not tag Section 702-collected information in its databases even to indicate that the data relates to a U.S. person. Additionally, in cases where the government identifies U.S. person information in Section 702 data, it does not take any steps to seek to identify the demographic background of any U.S. persons. Even if a system were adopted to tag information that relates to a U.S. person when it is identified as such, any government efforts to assess the individual's racial, religious, and ethnic background would raise significant privacy issues.

6. *Inadvertent Collection*

The government may also acquire U.S. person communications inadvertently, meaning the government either did not intend or was not authorized to acquire the data. The Board has not discovered any large-scale implementation problems with targeting or tasking, but inadvertent collection can occur as a result of human error, such as mistyping a selector, or when the government erroneously believes that a potential target is a foreigner or located outside the United States and discovers information to the contrary only after collection begins. Finally, it can occur after tasking when the U.S. person status or location of the target changes, or additional or secondary users of a selector are identified who are in the United States or are United States persons.

Inadvertent collection poses very similar privacy risks to incidental collection. However, agency minimization procedures require purging such collection as soon as the mistake or lack of authorization is identified after investigation and human review.[82] For example, according to

[81] Intel. Cmty., PCLOB questions received December 15, 2022 (Jan. 26, 2023).

[82] The government represents that such purging occurs "without delay." In the Board's understanding, "without delay" has different meanings in different contexts. If there is an indication that a target has traveled to the United States, "without delay" may mean immediate termination of acquisition if the target has already traveled and the travel was confirmed by an analyst. "Without delay" in the context of the identification of indicators of U.S. person status generally allows for time to verify the authenticity or accuracy of the indicators. Historically, DOJ has allowed for 24 hours from the discovery of the indicator to consult with analysts and obtain confirmation of the target's status. NAT'L SEC. AGENCY, EXHIBIT B, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION

NSA's targeting procedures, if NSA discovers that a target who was believed to be a non-U.S. person located outside the United States is in fact a U.S. person or is located inside the United States, it must terminate acquisition "without delay."[83]

Inadvertent collection also poses privacy risks separate from incidental collection, because it involves collection on someone who is not a valid target. This means the government would acquire a far greater percentage of that individual's communications as compared with incidental collection. Such inadvertent collection can occur through either errors by providers or by government analysts. Specifically, inadvertent collection can occur due to provider technical mistakes in responding to a directive, as described in previous Semi-Annual Reports to Congress and reported to the FISC. [84] Such provider errors can be more intrusive because providers have access to a vast scope of communications data. Inadvertent collection also causes privacy harms when caused by an analyst who mistakenly believes a selector is associated with a foreign person but in reality is associated with a U.S. person.

B. U.S. Person Queries

U.S. person queries present some of the most serious privacy and civil liberties harms. U.S. persons are entitled to the protections granted in the Fourth Amendment of the U.S. Constitution. Except in the very limited circumstances covered by Section 702(f)(2) for certain FBI queries,[85] government personnel are not required by Section 702 to make any showing of suspicion that the U.S. person is engaged in any form of wrongdoing prior to using a query term associated with that specific U.S. person. Nor does Section 702 require analysts or agents to seek approval from any judicial authority or other independent entity outside their agency. Rather, in pursuit of an agency's legitimate mission, analysts may use queries to digitally compile the entire body of

WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 8 (2022) [hereinafter 2021 NSA Minimization Procedures].

[83] Nat'l Sec. Agency, Exhibit A, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 8-10 (2022) [hereinafter 2021 NSA Targeting Procedures].

[84] *See* U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act (Sept. 2022) [hereinafter 28th SAR]; 27th SAR, *supra*; U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act (Sept. 2021) [hereinafter 26th SAR]. There were no provider errors in the 29th SAR. *See* U.S. Dep't of Just., Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act (Mar. 2023).

[85] As noted in Part 3 above, Section 702(f)(2) requires the FBI to seek a warrant from the FISC before accessing the results of a U.S. person query when all of the following conditions are met: (a) the query is conducted only seeking evidence of a crime (and is not a dual purpose query that also seeks foreign intelligence information), (b) the query is conducted in connection with a predicated criminal investigation, and (c) the criminal investigation does not relate to national security.

communications that have been incidentally collected under Section 702 involving a particular U.S. person's email address or other identifier. Because there also is no requirement for judicial review before targeting—or at the "front end" of Section 702 surveillance—U.S. person queries are often referred to as "backdoor searches." Further, since 2017, U.S. person queries may be conducted to search through communications acquired by upstream collection, so NSA analysts may search through the entirety of Section 702 data using U.S. person identifiers. In the Board's view, the Section 702 databases contain highly sensitive information due to the breadth and depth of the signals intelligence conducted, as well as the large potential for incidentally collected U.S. person information.

When government personnel search through collected communications seeking information about a particular U.S. person, this creates significant risks to privacy. Americans' communications captured through surveillance can include discussions of political and religious views, personal financial information, mental and physical health information, and other sensitive data. Moreover, while Section 702 targets must be reasonably believed to be non-U.S. persons located outside the United States, the targets themselves do not need to be individuals suspected of any wrongdoing, but must only be people reasonably likely to possess, receive, and/or communicate foreign intelligence information. As a result, ordinary Americans may be in contact with Section 702 targets for business or personal reasons even if the Americans have no connection to, or reason to suspect, any wrongdoing by their foreign contacts and even when the government has no reason to believe the target has violated any U.S. law or engaged in any wrongdoing.

When government personnel search through collected communications seeking information about a particular U.S. person, this creates significant risks to privacy. Americans' communications captured through surveillance can include discussions of political and religious views, personal financial information, mental and physical health information, and other sensitive data.

Americans' private communications also implicate their rights under the First Amendment, including free speech and freedom of association. As described in Part 3, in recent years both NSA and FBI have recognized particular sensitivity in U.S. person queries involving heightened First Amendment interests. Both agencies have implemented policies requiring enhanced review for queries related to sensitive investigative matters, particularly for U.S. persons engaged in particular professions, like journalists and elected officials. These rules help improve protections, but they do not address the First Amendment interests of all Americans, nor do they address the concern that patterns of communication can reveal Americans' associations with others.

Further, searches through Section 702 data seeking information about specific U.S. persons can undercut the rationale for permitting targeting under the program without individualized judicial review: that it is a foreign intelligence collection program focused solely on foreign targets. As the Board stated in its 2014 Report on Section 702:

> Depending on the scope of collection, however, the applicable rules may allow a substantial amount of private information about U.S. persons to be acquired by the government, examined by its personnel, and used in ways that may have a negative impact on those persons. . . . If [the scope of incidental collection is significant], this would raise legitimate concern about whether a collection program that is premised on targeting foreigners located outside the United States without individual judicial orders now acquires substantial information about U.S. persons without the safeguards of individualized court review. Emphasizing again that we have seen no indication of abuse, nor any sign that the government has taken lightly its obligations to establish and adhere to a detailed set of rules governing the program, the collection and examination of U.S. persons' communications represents a privacy intrusion even in the absence of misuse for improper ends.[86]

While the government takes seriously the prohibition against reverse targeting—which bans targeting a person outside the United States as a pretext to target a known person reasonably believed to be located in the United States—its approach to U.S. person queries threatens to undermine that critical safeguard for Americans' privacy rights. Once the government seeks to focus its investigatory attention on a specific U.S. person whose communications have been collected incidentally under Section 702, that process of focusing investigatory attention is analytically equivalent to targeting. Therefore, at the query stage, robust safeguards are needed to protect the individual's privacy and to avoid converting the program into one that focuses on U.S. persons.

NSA's approach to conducting U.S. person queries is the most privacy-protective of the agencies. NSA procedures require that personnel obtain prior approval from the Office of General Counsel for all U.S. person query terms used for queries of Section 702 content. NSA procedures also require personnel to document their justifications in writing prior to using all U.S. person query terms. CIA and NCTC do not require prior approval for U.S. person query terms. However, like NSA, both agencies require analysts to document a justification prior to conducting the query. As noted earlier in this report, as of the summer of 2023, FBI has announced that it will also require personnel to enter a written justification for all U.S. person queries prior to conducting the query.

[86] 2014 PCLOB Report, *supra*, at 133.

Except in the very limited circumstances described above for FBI, no independent judicial review is required for U.S. person query terms used by any of the four agencies participating in the Section 702 program.[87]

Although all U.S. person queries by the IC present privacy and civil liberties risks, the FBI's querying procedures and practices pose the most significant threats to Americans' privacy. First, as has been well documented, FBI personnel have continued to engage in practices that violate existing querying procedures and guidance, leading to numerous compliance violations and admonitions from the FISC.[88] Many of these violations are outlined in Part 3 of this Report. The extent of compliance violations are concerning, as they demonstrate a failure to follow the existing rules. Additionally, the high volume of U.S. person queries exacerbates the potential for abuse. The Board recognizes and welcomes the fact that the FBI has recently implemented several reforms designed to improve compliance, but these changes have not been sufficient to protect privacy and civil liberties.[89]

Particularly troubling is that the FBI has never once submitted an application to the FISC pursuant to Section 702(f)(2), despite many documented cases over the past five years (since the requirement was enacted) in which the warrant requirement actually applied. Section 702(f)(2) requires a warrant to view the results from a U.S. person query conducted only for evidence of a crime purposes in connection with a predicated investigation into a non-national security crime. However, even after FBI corrected its systems to avoid inadvertent viewing of the results of such queries,[90] and even after three years had passed following enactment of this statutory requirement,

[87] As described above, Section 702(f)(2) requires FBI to seek a warrant from the FISC before accessing the results of U.S. person queries in very narrow circumstances.

[88] In 2018, the FISC stated that FBI conducting tens of thousands of unjustified queries represented an arbitrary invasion of individual privacy. The FISC noted that compliance with provisions restricting the use and dissemination of the results of queries "mitigates the intrusion on U.S. persons' privacy resulting from unjustified queries, either by limiting the scope of information acquired and therefore subject to querying or limiting the further use or disclosure of U.S.-person information returned by queries." 2018 Cert FISC Opinion and Order, *supra*, at 89-91. In September 2021, the FISC reiterated its concerns over FBI's procedural compliance challenges, noting that failure to correct "substantial and persistent" compliance issues "call[s] into question the continued validity [of the procedures], as well as the ability of a FISC judge to find the FBI's Section 702 procedures, as implemented, to be consistent with statutory and Fourth Amendment requirements." The FISC directed FBI to take several steps designed to enhance compliance and transparency. Order in Response to Querying Violations, at 13, *In re DNI/AG 702(h) Certifications 2020-A, 2020-B, 2020-C, and Predecessor Certifications*, Docket Nos. 702(j)-20-01, 702(j)-20-02, 702(j)-20-03, and predecessor dockets, *In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under FISA*, Docket No. 08-1833, *In re FBI Standard Minimization Procedures for Tangible Things Obtained Pursuant to Title V of FISA*, Docket No. BR 13-49 (FISA Ct. Sept. 2, 2021).

[89] In response to the September 2021 FISC order and earlier FISC commentary concerning FBI compliance incidents, FBI revised its Section 702 querying procedures and portions of the minimization procedures that govern queries of other FISA datasets; revised training and issued query-specific training; altered default settings, prompts, and documentation requirements in its systems; and implemented new attorney review and approval requirements for batch jobs and sensitive queries. DOJ NSD also issued updated guidance on the query standard.

[90] Initially, FBI violated this requirement for numerous queries due to a flaw in its system design that enabled agents to view query results through a preview panel. *See* OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL

there were six documented instances over the course of 2021 and 2022 in which such a court order was required but FBI personnel failed to seek a warrant before viewing the results of U.S. person queries.[91] Thus, as of August 2023, the FBI has never obtained a Section 702(f)(2) order.

Section 702 of FISA	*(In Calendar Years)*				
	2018	2019	2020	2021	2022
Number of reports to FISC, as required by Court orders, of FBI personnel accessing specified Section 702-acquired content returned by specified queries not designed to find and extract foreign intelligence information	**5**	**91**	**1**	**5**	**1**
Number of FISC orders obtained pursuant to Section 702(f)(2) to review the results of a query that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence	**0**	**0**	**0**	**0**	**0**

Figure 4

Second, FBI's querying practices pose greater threats to privacy because the FBI, as the United States' domestic law enforcement agency, has the ability and the mission to investigate and prosecute Americans for crimes. When an American faces the prospect of criminal investigation and prosecution, their privacy interests are at their highest. Since, as noted, Americans' sensitive communications are incidentally collected under Section 702 even when individuals have no reason to believe that they are in contact with wrongdoers, robust guardrails are needed to protect privacy rights in circumstances where the government seeks to search through those communications. However, when the Board inquired, the government responded that it does not track how many times it has used Section 702 information that was identified through a U.S. person query as part of a criminal investigation or prosecution, and the government was unable to identify any instance in which this has occurred. Thus, U.S. persons have been unable to challenge the use of evidence in criminal proceedings that was identified through U.S. person queries.[92]

TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR CY2020, at 20-21 (2021) [hereinafter CY2020 ASTR].

[91] As of the 2020 certification of the Section 702 program, the FISC noted that the government had asserted that, based upon mandatory FISA training, FBI personnel "should be aware" of the requirement to obtain an order from the FISC for such queries subject to Section 702(f)(2), and yet the FBI has not complied with this requirement. Memorandum Opinion and Order, at 48, *In re DNI/AG 702(h) Certification 2020-A and its Predecessor Certifications*, Docket No. 702(j)-20-01 and predecessor dockets, *In re DNI/AG 702(h) Certification 2020-B and its Predecessor Certifications*, Docket No. 702(j)-20-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2020-C and its Predecessor Certifications*, Docket No. 702(j)-20-03 and predecessor dockets (FISA Ct. Nov. 18, 2020).

[92] See, e.g., United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021).

Moreover, it is important that the rules for U.S. person queries should not enable law enforcement to rely on this practice to convert a foreign intelligence collection authority into a domestic law enforcement tool, and thereby evade otherwise applicable privacy safeguards. This concern is most heightened in the case of evidence of a crime only U.S. person queries, which are U.S. person queries that are conducted without any foreign intelligence purpose because the crimes are unrelated to national security. In such circumstances, there is a greater risk that the foreign intelligence purpose of Section 702 can be subverted.

FBI does not track how many evidence of a crime queries it runs annually. It only tracks and reports the number of such queries in which results are both returned and accessed and that are defined as "queries" in the FBI Querying Procedures. In 2022, approximately 1.58% of all FBI U.S. person queries resulted in an FBI user accessing content information returned by the query.[93] Of these queries in 2022 that resulted in a hit and where the results were accessed by FBI, there were sixteen conducted for evidence of a crime only. In 2021, there were thirteen such queries, and in 2020, there was one.[94] During the same years, FBI opened zero criminal investigations of U.S. persons who were not considered a threat to national security based in whole or in part on Section 702 information.[95] In fact, since at least 2017, FBI has not opened any criminal investigations of U.S. persons who were not considered a threat to national security based at least in part on Section 702 information.[96]

These facts suggest that FBI may not need the authority to run U.S. person queries for evidence of a crime only purposes. However, rather than completely precluding FBI from accessing Section 702 data in such situations, we believe that the better course is to raise the standards for conducting U.S. person queries to ensure sufficient protection for Americans' privacy rights.

---

[93] Intel. Cmty. Briefing for Priv. and C.L. Oversight Bd. Staff (May 2023), *supra*. In 2021, approximately 0.23% of all FBI U.S. person queries resulted in an FBI user accessing content information returned by the query.

[94] These queries include the five in 2021 and the additional query in 2022 that should have required FBI to seek a warrant from the FISC under Section 702(f)(2) in order to view the query results. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2022, at 27 (2023) [hereinafter CY2022 ASTR]; CY2020 ASTR, *supra*, at 21.

[95] CY2022 ASTR, *supra*, at 28.

[96] *See* Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year CY2021 (2022) [hereinafter CY2021 ASTR]; CY2020 ASTR, *supra*; Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year CY2019 (2020) [hereinafter CY2019 ASTR]; Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year CY2018 (2019) [hereinafter CY2018 ASTR]; Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year CY2017 (2018) [hereinafter CY2017 ASTR].

In addition and as noted when analyzing the value of the FBI's use of U.S. person queries, there was little justification provided to the Board on the relative value of the close to 5 million searches conducted by the FBI from 2019 to 2022. In the most recent Annual Statistical Transparency Report, the FBI lowered its searches by 94 percent, and the Board has seen little evidence by the FBI that it now lacks certain information or is unable to find relevant information at any stages of an investigation. The FBI identified few cases in which a U.S. person query provided unique value in demonstrating a previously unknown connection between the U.S. person and another Section 702 target or otherwise advancing a criminal investigation. In addition, the number of searches occurring is still substantial. This is especially so as compared to other IC components. In calendar year 2022, whereas FBI used 119,383 unique U.S. person query terms, NSA, NCTC, and CIA combined used a total of 4,684 U.S. person terms.[97]

In recent years, both NSA and FBI have recognized particular sensitivity in U.S. person queries involving heightened First Amendment interests. As described in Part 3, NSA and FBI have each implemented policies requiring enhanced review for queries related to U.S. persons engaged in particular professions. These new policies are welcome, but are not sufficient to address the threats posed by U.S. person queries.

1. *Assessment and Pre-Assessment Queries*

As discussed in Part 3, FBI routinely searches Section 702 data at the pre-assessment and assessment stages of FBI investigations. Agents conduct searches at those stages to learn more about a given person or identifier that comes across their desk. This may explain why so many FBI searches do not provide actionable intelligence to FBI analysts. As also described above, thousands of searches were improper extending to community leaders, repair-people, and even political figures and their staff.

Searches performed before an investigation even begins create one of the greatest threats to privacy and civil liberties. According to FBI's Domestic Investigations and Operations Guide, assessments do not require factual predication, but do require an authorized purpose and clearly defined objectives.[98] The pre-assessment stage requires neither.[99] Although Section 702 queries must still meet the query standard, the low thresholds applicable at the pre-assessment stage increase the risk that an individual's private communications will be compiled despite the lack of any basis to suspect the individual of wrongdoing. Further, even though the communications identified through a database query have already been collected, compiling all of a specific individual's communications contained in the database and surfacing them for review by an agent constitutes a privacy invasion that requires more sufficient justification than is currently provided.

[97] CY2022 ASTR, *supra*, at 20, 24.

[98] Fed. Bureau of Investigation, Domestic Investigations and Operations Guide, at 5-1 (2021) [hereinafter FBI DIOG].

[99] *Id.* at 5-2.

2. *Queries Related to First Amendment Activities*

In addition to the privacy risks discussed above, searches conducted by FBI analysts related to social advocacy and non-violent civil protests also pose significant threats to civil liberties, because protest activity is covered by the First Amendment.[100] FBI conducted thousands of searches concerning people who were arrested in connection with social advocacy and protests around the country. As noted in Part 3, in 2021, the government conducted hundreds of noncompliant queries concerning individuals arrested in connection with civil unrest and protests.[101] In one example, FBI personnel in Washington, DC conducted 141 queries of identifiers associated with activists who were arrested in connection with protesting the murder of George Floyd in Washington, DC between June 3 and June 5, 2020, despite the lack of any reason to believe there would be information on these individuals in Section 702 databases.[102] Thus, the FBI analysts lacked a proper justification for searching the activists' identifier.

Although the examples above concern queries that were recognized as compliance incidents, it is important to emphasize that searches related to political protests strike at the heart of conduct protected by the First Amendment and raise the specter of improper politically motivated searches. Thus, while it is critical to protect the privacy of all individuals, it is even more important to ensure robust guardrails when searches also threaten the right to free expression and create risks of improper targeting of individuals based on their political views. FBI's new procedures for approval of Sensitive Queries represent an important step toward directly addressing these threats to protected expressive activity. However, these procedures are not sufficient to fully safeguard First Amendment activities.

3. *Other Problematic Queries and their Privacy Harms*

Other queries conducted by FBI also create severe privacy harms. As noted in Part 3, FBI queried community leaders and religious leaders, as well as everyday Americans who came into an FBI field office to provide a tip.[103] The fact that FBI received the information and immediately used a known U.S. person identifier to search the Section 702 database either to verify or refute the information despite the lack of any apparent connection to foreign intelligence presents a significant privacy harm. The behavior indicates that FBI has treated Section 702 databases essentially as a search engine for routine use. Further compounding the issue, these noncompliant

[100] While the newest 29th Semi-Annual Report (SAR) to Congress does not present the categories of compliance incidents, the government categorized compliance incidents in previous SARs.

[101] *See* 27th SAR, *supra*, at 102, 108, 113, 124.

[102] *Id.* at 102.

[103] In some instances, the "tip" included individuals who were identified in a shopping center's parking lot with multiple containers of home cleaning products. *See* Memorandum Opinion and Order, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) [hereinafter Apr. 21, 2022 FISC Opinion and Order]. Unfortunately, some of the specific examples remain classified.

searches are only able to be uncovered through manual auditing of the FISA databases at local field offices. FBI's routine use of queries to search a specialized foreign intelligence database is especially problematic due to the fact that FBI uses the database for pre-assessment and assessment actions.

In the Board's view, such routine querying of 702 information based on even an uncorroborated tip demonstrates another key privacy threat posed by U.S. person queries.

4. *Victim Queries*

The government has described situations in which U.S. person queries are used to identify potential victims of planned attacks, including cyber-attacks. Such instances have been at the forefront of the government's advocacy in favor of the need for U.S. person queries. In many instances it is not initially apparent whether the U.S. person is a witting or unwitting participant, and the government has used U.S. person queries to help make this determination. In some of the examples provided to the Board, the government likely would have been able to obtain the consent of the U.S. persons to run queries using their identifiers.

The government now describes such searches as "defensive queries," but in most cases they still raise the same privacy risks as other queries for information about specific Americans. Current rules do not provide any victim-based exception to query standards. It may, however, be appropriate to develop different rules for situations in which the government obtains actual consent from the person whose identifier the government seeks to query. As discussed above, there have been examples where the FBI has actually reached out to potential victims to voluntarily inform them of potential threats, and asked those potential victims to provide their email addresses and other selectors so that agents could conduct queries to assess whether the individuals were the subject of a planned attack. The Board is not aware of any instance in which the potential victim declined to provide the requested selector information to the FBI. When the government obtains actual consent from a potential victim, including providing their contact information as selectors, this can ensure that the person understands and is willing to cede some of their privacy in order to gain relevant information or protection.

C. Multi-Term Query Actions, Batch Job Queries

As described in Part 3, FBI systems allow users to conduct a single query action that encompasses multiple query terms. In such query actions, the analyst inputs a single justification that applies to all query terms. The FBI now refers to these searches as "Batch Job Queries." Such batch job queries have been conducted for as many as 1.9 million query terms, as in the cyber-attack example described in Part 3. Other agencies in the Intelligence Community refer to these types of searches as "multi-term query actions."

As discussed previously, FBI's query guidance for conducting batch job queries requires that "each and every identifier queried must independently satisfy the querying standard by having

an authorized purpose, an appropriate design, and a proper justification."[104] However, FBI personnel are permitted to use the same justification for all query terms, and there is no requirement that agents separately record an explanation for why each term is considered to meet the standard. For example, imagine FBI personnel obtain a known terrorist's cell phone. FBI may seek to conduct a batch job query using all email addresses in the contacts list of that cellphone, under the single rationale that all the emails were in that contacts list. The FBI does not assess every single discriminant used when running batch queries. Tellingly, the FISC previously referred to these queries as "bulk searches."[105]

In 2021, following a series of large-scale batch job query compliance incidents, FBI implemented an attorney review requirement for batch job queries with 100 or more query terms. In June 2023, FBI updated this rule to require attorney review for all batch job queries.[106] The attorney approval requirement for batch job queries is not specific to U.S. person queries. However, agents are still not required to document separately that each and every query term independently meets the query standard.

Batch queries present yet another privacy and civil liberties harm in the context of the Section 702 program. The rules allowing a single broad justification for hundreds or thousands of query terms can cause serious privacy harms. First, this can normalize agents' and analysts' use of broad and imprecise justifications beyond the batch context. Second, such search justifications are ripe for returning a disproportionate amount of irrelevant information.

[104] Fed. Bureau of Investigation, FBI FISA Query Guidance, at 6 (March 17, 2022).

[105] See Memorandum Opinion and Order, at 25, In re DNI/AG 702(h) Certification 2020-A and its Predecessor Certifications, Docket No. 702(j)-20-01 and predecessor dockets, In re DNI/AG 702(h) Certification 2020-B and its Predecessor Certifications, Docket No. 702(j)-20-02 and predecessor dockets, In re DNI/AG 702(h) Certification 2020-C and its Predecessor Certifications, Docket No. 702(j)-20-03 and predecessor dockets (FISA Ct. Nov. 18, 2020). The government has since changed its terminology. The term "bulk" is also a term of art; however, two predominant definitions exist. Notably, the National Academies' report on bulk surveillance defined bulk collection as "collection in which a significant portion of the retained data pertains to identifiers that are not targets at the time of collection." The second definition is from Presidential Policy Directive 28, signed by President Obama, in which bulk was defined as the collection of information "without the use of discriminants."

[106] Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary, 118th Cong. 11 (2023) [hereinafter June 2023 Joint Statement to Senate Judiciary] (statement of Paul Abbate, Deputy Dir., Fed. Bureau of Investigation).

Most concerning, without a specific and individualized assessment for each discriminant it is not possible to ensure that the query standard is actually being met and only searches reasonably believed to return evidence of a crime or foreign intelligence are performed. For example, as noted above, current rules permit FBI to use a batch query where all the identifiers were found in the contact list of a known terrorist. FBI is able to input a single justification for all such identifiers because there is no requirement that FBI personnel demonstrate why querying identifiers for each of those contacts is likely to retrieve foreign intelligence information or evidence of a crime. However, these contacts may include people with no connection to such information or evidence.

Batch queries present yet another privacy and civil liberty harm in the context of the Section 702 program… without a specific and individualized assessment for each discriminant it is not possible to ensure that the query standard is actually being met and only searches reasonably believed to return evidence of a crime or foreign intelligence are performed.

While the government asserts that batch queries do not constitute bulk searches, it would be helpful for the government to conduct a legal analysis examining how the practice of batch queries complies with the terms of E.O. 14086 and its requirements for necessity and proportionality. The Board recognizes that the specific requirements of Section 2(c) of the Executive Order regarding queries of bulk collection do not apply to Section 702. However, Section 2(a) of the Executive Order requires that all signals intelligence activities must be necessary and proportionate to a validated intelligence priority. As the government moves forward with implementation of this new executive order, such a legal analysis will help the government to ensure that batch queries comply with these requirements, and to identify whether the standards for queries involving terms associated with non-U.S. persons need to be updated.

D. Exceptions and Exemptions to the Querying Procedures

Congress narrowly defined "queries" and set out requirements for "querying procedures" in the statute; however, the querying procedures across all agencies exempt certain actions from the definition of "queries." They also contain exceptions that permit conducting other types of queries without following otherwise applicable rules. These exemptions and exceptions undercut the statutory rule. Privacy risks exist because such actions do not have to comply with the standards in the querying procedures.

The exemptions and exceptions present civil liberties concerns by further narrowing the definitions provided by Congress, and thereby excluding those exempted activities and queries from statutory reporting requirements. For example, the number of queries is necessarily much larger than the publicly reported numbers because the various querying procedures' definitions of

"query" exempt actions conducted for "user activity monitoring" or exempt a user's actions subsequent to conducting a query to sort the results of the query.[107] The various querying procedures also except entire categories of searches from the procedures, including queries conducted for purposes of training, to comply with court orders, and to enable congressional oversight.[108]

These exemptions and exceptions are not appropriately defined to ensure they effectively mitigate or even reduce privacy risks. For example, all agencies' exceptions include that "notwithstanding" the query standard or the creation and maintenance of querying records, "nothing in these procedures shall prohibit" the lawful oversight functions of DOJ, ODNI, or the applicable Offices of the Inspector General (OIG), prohibit the agency from providing the assistance necessary for DOJ, ODNI, or OIG to perform their lawful oversight functions, or prohibit the agency from conducting the queries. In the context of the FBI, the exceptions also include complying with Freedom of Information Act or Privacy Act requirements.[109] This means querying of U.S. and non-U.S. persons identifiers and the likely retrieval of information that was not reasonably believed to contain foreign intelligence information—a significant privacy risk. Congress required querying procedures to improve the protection of U.S. person data; however, the exemptions and exceptions in agencies' querying procedures undermine this safeguard. Although it may be appropriate to designate certain circumstances under which queries should be subject to different standards, Congress should consider and determine what circumstances justify such departures.

The exceptions to the querying procedures also lack sufficient detail to provide adequate guidance to those performing the queries. Four out of six of NSA's exceptions are one sentence long.[110]

E. Privacy Risks from Retention and Dissemination

It is a fundamental principle of data privacy that the longer data is retained, the greater the privacy risks. This stems from such threats as the risk of data breach or other improper access to data, the risk that data will be improperly used for purposes beyond the authorized purpose for collection, and the risk that information will be shared more broadly than authorized.

As described earlier, under Section 702, most data may be retained for five years, unless it has been reviewed and determined to constitute foreign intelligence information or evidence of a

[107] Nat'l Sec. Agency, Exhibit H, Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 2 (2021) [hereinafter 2021 NSA Querying Procedures].

[108] See, e.g., id.

[109] 5 U.S.C. § 552a.

[110] 2021 NSA Querying Procedures, *supra*, at 5.

crime. However, each agency has its own procedures containing notable variations, and the standard retention periods for Section 702 data are not limited to the previously publicized five-year retention period. In particular, in many circumstances FBI is permitted to retain data for up to ten years, or, with additional controls, for up to fifteen years. Such lengthy retention periods substantially increase privacy risks.

Dissemination of Section702-acquired information throughout the intelligence community and to foreign, state, local, and tribal partners creates risks to privacy and civil liberties as well, especially due to the ease with which the government can share substantial amounts of information. Between September 2021 and August 2022, FBI disseminated 3,527 reports containing Section 702-acquired U.S. person information.[111]

As described in the Facts Section, data identified as foreign intelligence information or, in certain cases, evidence of a crime, may be disseminated to other recipients for a number of specifically enumerated purposes. These purposes include sharing with private entities and individuals to assist in the mitigation or prevention of computer intrusions or attacks,[112] and with private entities and individuals when FBI determines the information is capable of providing assistance in mitigating or preventing serious economic harm or serious physical harm to life or property.[113]

At FBI, the standard for such disseminations containing U.S. person information is whether the FISA-acquired information concerning U.S. persons reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime being disseminated for a law enforcement purpose. When a U.S. person's information is disseminated, the identity of the person is generally deleted and a replaced with a generic term or symbol so that the information cannot be reasonably connected with an identifiable U.S. person.[114] By contrast with FBI, in certain circumstances NSA may disseminate the information to the recipient with the U.S. person's identity revealed,[115] otherwise known as "unmasking."

The sharing of U.S. person information with state, local and tribal governments for foreign intelligence purposes is governed by the FISA definition of foreign intelligence information.[116]

---

[111] Fed. Bureau of Investigation, Supplemental Response to Accuracy Review (Jan. 2023).

[112] Fed. Bureau of Investigation, Exhibit D, Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 47 (2021) [hereinafter 2021 FBI Minimization Procedures].

[113] *Id.*

[114] 2021 NSA Minimization Procedures, *supra*, at 14.

[115] *Id.* at 15.

[116] 50 U.S.C. § 1801.

The first part of that definition presents a high bar as it concerns information related to hostile acts of a foreign power or agent of a foreign power, sabotage, international terrorism, and clandestine intelligence activities. These specific descriptions mitigate against overcollection and oversharing. However, the second clause of the foreign intelligence information definition allows for broad sharing of information because it includes sharing U.S. person information that reasonably appears to be necessary to the national defense or the security of the United States or the conduct of the foreign affairs of the United States.

Sharing with private entities raises additional concerns. While there is no doubt that certain exigencies should exist to allow the sharing of Section 702 information, the sharing of U.S. person information with private entities creates heightened privacy risks. In particular, private entities are not subject to the same restrictions as government actors that limit onward sharing. The FBI was unable to provide metrics on the number of disseminations made under the provision of their Minimization Procedures covering dissemination to private entities.[117]

Certain privacy and civil liberties risks and significant privacy harms occur by the sharing of U.S. person information with foreign governments. The United States is unable to exert its own privacy protections on the data once it leaves U.S. data repositories.[118] The United States also has little insight into how that information is used after it is shared. FBI personnel must ensure U.S. person data is protected by its foreign partners.

F. Use, Retention, and Dissemination Privacy Risks to Non-U.S. Persons

In addition to the discussion above regarding targeting that applies directly to non-U.S. persons, many of the privacy and civil liberties risks described throughout the above sections on use, retention, and dissemination of Section 702 information also apply to non-U.S. persons. Indeed, because only selectors reasonably believed to be associated with non-U.S. persons may be targeted for collection under Section 702, the privacy risks for non-U.S. persons are greater than for Americans. The privacy harms are exacerbated by the fact that the scope of "foreign intelligence information" under FISA is very broad and may relate to the United States' "foreign affairs" generally. The harms are further compounded because there is no judicial review of targeting decisions and the government may collect the communications of vast numbers of non-U.S. persons under Section 702.

However, the United States has recognized privacy protections for non-U.S. persons, including through ratification of the International Covenant on Civil and Political Rights (ICCPR), through issuance of PPD-28 in 2014, and most recently, through issuance of E.O. 14086 in October 2022. As noted, E.O. 14086 applies to all collection of signals intelligence, including Section 702.

[117] Response from Fed. Bureau of Investigation to Priv. and C.L. Oversight Bd. (Sept. 2022); 2021 FBI Minimization Procedures, *supra*, at 47.

[118] The Board has not had access to these disseminations to foreign governments.

The executive order explicitly recognizes the principles of necessity and proportionality, long-established in EU law, and provides safeguards for the privacy interests of all persons, regardless of nationality. Specifically, E.O. 14086 provides that U.S. signals intelligence activities may only be conducted where "necessary to advance a validated intelligence priority" and "in a manner that is proportionate the validated intelligence priority."[119]

As described above, the executive order also provides that signals intelligence collection activities may only be conducted in pursuit of one of twelve listed legitimate objectives.[120] As also noted above, the Board agrees that the purposes authorized under the current Section 702 certifications fit within the twelve legitimate objectives, and these limitations should help ensure that the government will not conduct surveillance to the outer bounds of the FISA definition of foreign intelligence information. However, because these limits are contained in an executive order, the FISC will likely not consider that it has jurisdiction to enforce the restriction. Therefore, if in the future the government were to seek to conduct Section 702 surveillance for a purpose outside the scope of these twelve purposes, the FISC would likely not be able to deny the certification for failure to comply with the executive order.

Further, even if targeting is narrowed by the twelve limitations under E.O. 14086, there remain a number of other privacy and civil liberties harms at stake. Many innocent non-U.S. persons will suffer from the same harms of incidental collection as U.S. persons do. As with the communications of any non-target, once that information is collected and in government databases, it can be analyzed, disseminated, retained, queried, used as evidence against them in criminal proceedings, and used to initiate targeted surveillance under alternate legal authorities, or it may be shared with law enforcement and intelligence partners worldwide.[121]

G. Training and Auditing

Training is a necessary facet of any compliance regime. At the beginning of the Board's investigation, the Board found that FBI did not conduct annual refresher trainings for those who had access to Section 702 data. Annual training allows analysts to understand the complicated policies and procedures imposed on Section 702 databases. Without annual refresher training, analysts are likely more prone to engage in compliance incidents, which often directly implicate privacy and civil liberties. Fortunately, the FBI recently added a requirement for annual refresher training.

In addition, a robust system of audit logs and audit reviews is critical to compliance. FBI must perform more routine auditing beyond the current visits to field offices and spot checking

[119] Exec. Order No. 14,086, § 2(a)(ii).

[120] *Id.* § 2(b).

[121] Such uses would be subject to otherwise applicable rules, such as those regarding dissemination and use in criminal proceedings.

queries for compliance. This includes ensuring the lag time between initial audits and the eventual publishing of the analysis of those audits is shorter than two years.[122]

H. Transparency and Operation of the FISC

As noted, in 2015 Congress created the role of FISC amici, and required that the FISC shall appoint an amicus in any case involving a novel or significant interpretation of law. The FISC amicus role has been valuable, but three primary issues have limited the ability of amici to provide robust oversight in the context of FISC consideration of Section 702.

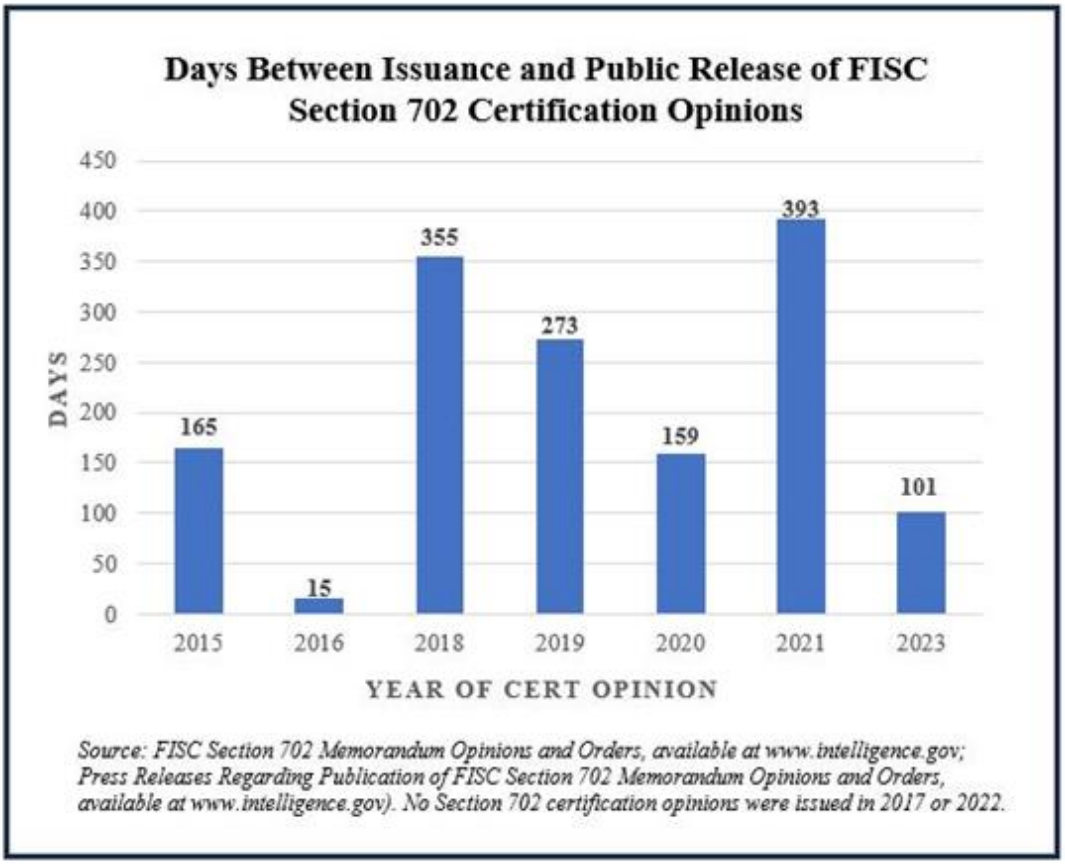


Figure 5

First, although the FISC has appointed amici in connection with its consideration of Section 702 certifications in 2015, 2018, 2021, and 2023, the FISC did not appoint an amicus in connection with the 2016, 2019, or 2020 certifications. Second, amici have experienced difficulty in obtaining access to full information related to the matters in which they have been appointed, including in

[122] For example, the Board was provided a FBI Office of Internal Audit analysis in May 2023; however, the data analyzed in Query Audit 1 covered a twelve-month period between April 1, 2020 and March 31, 2021. The Board was also provided with Query Audit 2 which covered the period July 1, 2021 through March 31, 2022. While the office should be commended for engaging in such analysis, the Board is unable to determine if the data, and the analysis of the data, is still applicable to the 2023 environment.

Section 702 proceedings.[123] Finally, amici have not been able to petition for appeal of adverse decisions, including in a Section 702 certification in which the matter was already being appealed to the FISC-R by the government. Specifically, the government appealed the FISC's decision in the 2018 Certification that FBI was required to count U.S. person queries. While amici did participate in the FISC-R proceedings, the FISC-R did not consider an additional issue that was decided adverse to the amicus below.

Notably, in the PCLOB's Report on Section 215 and the operation of the FISC published in January 2014, the Board recommended that Congress create a "Special Advocate" role that was similar to the amicus role Congress eventually created in 2015. However, the amicus role as created by Congress is weaker than the special advocate position described by the Board in three ways that would have protected against these issues. The Board urged that special advocates participate in matters beyond those involving "novel and significant" issues; that they have full access to information related to matters in which they participate; and that they should be able to petition for appeal of decisions by the FISC and the FISC-R.

In addition, amici have generally been unable to consult each other when one member of the panel has been appointed to participate in a matter.[124] This inability to confer with colleagues who may have direct expertise and who may have litigated relevant matters has served as a barrier to amici fulfilling their responsibilities and it differs markedly from typical legal practice outside the context of the FISC.

Finally, the 2018 Certification and appeal also illustrate an additional issue: the significant delays in releasing court opinions to the public prevent adequate transparency surrounding the FISC. Section 602 of FISA requires that the government must conduct a declassification review of decisions of the FISC and FISC-R that involve a significant interpretation of law, and make those decisions publicly available to the greatest extent practicable. The government did not publicly release the FISC's opinion from the 2018 Certification decision until after it had appealed the decision to the FISC-R, lost again on appeal, and then obtained the remand decision from the FISC. Similarly, the FISC's April 2022 decision certifying the Section 702 program was not publicly released until May 2023. Since Congress required declassification reviews of FISC opinions in 2015, on average it has taken from twelve to eighteen months to release publicly declassified versions of FISC decisions. The public should be able to obtain this information as quickly as is possible while protecting national security. Significant delay and the resulting lack of transparency directly impacts privacy and civil liberties analysis of the Section 702 program.

[123] This conclusion is based upon multiple conversations between PCLOB and some amici.

[124] This conclusion is also based upon conversations between PCLOB and some amici.

III. Conclusion

The Board concludes that although the Section 702 program presents serious risks to, and actual intrusions upon, the privacy and civil liberties of both Americans and non-Americans, the United States is safer with the Section 702 program than without it. Section 702 is valuable in supporting U.S. government efforts to counter foreign threats from actors outside the United States, such as terrorism, weapons proliferation, and cyber threats. At the same time, the risk of overbroad government collection of communications under Section 702 and subsequent government use of that information is very real and can cause harm, at varying degrees. The most serious privacy and civil liberties risks result from U.S. person queries and batch queries, and the government has not demonstrated to us that such queries have nearly as significant value as the Section 702 program overall.

Ultimately, the Board believes that these privacy and civil liberties risks can be reduced while preserving the program's value in protecting Americans' security. The recommendations that follow outline how Congress and the government can reduce these risks.

PART 5: RECOMMENDATIONS

The Board offers the following recommendations, including both recommendations for the enactment of legislation by Congress and recommendations that can be implemented by the government without congressional action. To the extent that any of these recommendations in either category would require additional resources, the Board urges the Administration and Congress to work together to ensure that the necessary funds are authorized and appropriated.

RECOMMENDATION 1:

Congress should codify the twelve legitimate objectives for signals intelligence collection under Executive Order 14086.

In order to clarify current law, prevent overbroad collection, and update the FISC's jurisdiction, the Board recommends that Congress codify the twelve legitimate objectives for signals intelligence collection as laid out in Executive Order 14086 (E.O. 14086). Such codification, by design, should align the definition of foreign intelligence in E.O. 14086 and FISA. It would also allow the FISC to use the standards for foreign intelligence laid out in the Executive Order in FISA-related rulings and court procedures.

The Administration has explained that E.O. 14086 establishes safeguards for U.S. signals intelligence activities, including requiring that such activities be conducted only in pursuit of defined national security objectives. The E.O. is designed to limit the purposes for collection, improving privacy safeguards for all people, regardless of nationality. These provide important privacy and civil liberties protections for signals intelligence collection, including the Section 702 program, and intentionally narrow the grounds upon which the government can otherwise collect under Section 702.

Like all executive orders, E.O. 14086 has the effect of law and remains in force until revoked, canceled, or otherwise considered unlawful. The government understands that the Executive Order is binding and has represented that it is already in compliance with the new limits on surveillance. However, the FISC does not presently have statutory jurisdiction to enforce an executive order and is therefore unable to take it into account when evaluating Section 702 collection practices for legal sufficiency. The Board assesses that the codification described above would provide the necessary clarity in conferring explicit jurisdiction to the FISC to ensure that E.O. 14086 is properly enforced across the judicial branch.

The Board also notes that the twelve specific signals intelligence objectives outlined in E.O. 14086 are crucial to implementing U.S. commitments under the European Union-U.S. Data Privacy Framework and to providing international clarity regarding U.S. law and intelligence collection. The Board assesses that codification of the twelve legitimate objectives for collection would promote the Data Privacy Framework and ensure its longevity. Codifying the twelve

objectives into law and explicitly enabling the FISC to rely on it as an authoritative legal source when evaluating the legality of intelligence collection practices under Section 702 would provide the longer-term certainty the Board deems necessary for full application of privacy and civil liberties rule of law principles to signals intelligence. It also helps bolster public trust in the Intelligence Community's use of Section 702 authorities.

Finally, E.O. 14086 provides that "The President may authorize updates to the list of objectives in light of new national security imperatives…. The Director of National Intelligence shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States." The Board urges that similar language be included in any legislation codifying the objectives. In the event that the President determines that public release of a new objective would pose a risk to national security, the Board recommends ensuring that the FISC as well as relevant congressional committees and members of congressional leadership receive immediate notification at the appropriate levels of classification. This would preserve the executive authority in protecting national security, while ensuring that the FISC has clear, updated jurisdiction in line with the law.

RECOMMENDATION 2:

Congress should codify the prohibition against "abouts" collection by removing NSA's ability to restart it without congressional approval other than in certain exigent circumstances. Any restart of "abouts" collection should apply to only those particular forms of traffic related to the exigency.

Historically, "abouts" collection is among the most privacy-intrusive collection mechanisms used under the Section 702 program, and produced a significant number of compliance incidents involving the acquisition of purely domestic communications. Even when collected accurately, "abouts" collection, by definition, enables the acquisition of communications between non-targeted persons. NSA assessed in 2017 that the compliance risks and difficulty of "abouts" collection outweighed the mission value of such collection.

The current statute allows the government to restart "abouts" collection following approval by the FISC and after providing thirty days' notice to Congress. Due to the significant risks to privacy and civil liberties generated by "abouts" collection, and because there is currently no identified mission need for such collection, the Board recommends that Congress amend the statute to remove the government's ability to restart "abouts" collection, except in certain exigent circumstances as described below.

FISA provides for the government's ability to begin acquisition under Section 702 prior to the FISC authorizing such collection in exigent circumstances. The 2018 Reauthorization Act added a similar provision specific to "abouts" collection that provides a limited ability for the government to restart "abouts" collection following a finding of exigent circumstances. The Board

recommends preserving the government's ability to restart "abouts" collection in exigent circumstances following timely notice to Congress, but also recommends that the government's ability to restart "abouts" collection in exigent circumstances apply narrowly only to communications reasonably likely to contain critical foreign intelligence information that NSA would not otherwise be able to collect without using "abouts" collection.

Specifically, the exigent circumstances provision should permit NSA to conduct "abouts" collection only in upstream and only when NSA has assessed that: (a) it is not technically feasible to limit its collection to communications to or from the target due to the method of communication employed; (b) the target is reasonably likely to use this method to communicate intelligence information important to the national security of the United States; and (c) emergency use of "abouts" collection is necessary to acquire communications to or from the target. NSA has stated that the rationale for "abouts" collection was, in part, that in certain circumstances NSA was not able, at the time of collection, to determine whether the presence of a selector in a communication indicated that it was to or from a target, or that the selector was present only in the body of a communication. NSA was therefore unable to fully mitigate the technical possibility that it might collect communications that were neither to nor from its targets in certain circumstances. The Board recommends that the provision permitting resumption of "abouts" collection under exigent circumstances be tied to this rationale, and be applied only to those types of communications.

Further, the Board recommends that Congress narrow the exigent circumstances exception for "abouts" collection to require that:

- The resumption of "abouts" collection will continue only as long as the exigent circumstances persist but in no case longer than thirty days, unless there is a further finding by the FISC that the exigency persists.
- Only those particular targeting decisions affected by the exigent circumstances will be permitted; that is, "abouts" collection can be used only for those targets and those topics immediately relevant to the exigent circumstances.

Because "abouts" communications are more privacy-intrusive than acquisitions of only to/from communications and historically present a higher risk of inadvertent acquisition of domestic communications as well as compliance incidents, the Board recommends that NSA limit the access to, retention of, and dissemination of all communications acquired using "abouts." This includes tagging such communications as acquired through "abouts," limiting access to a smaller set of NSA analysts, retaining such communications for only two years, and prohibiting the use of U.S. person identifiers to query such communications. Communications acquired through "abouts" collection that are subsequently discovered to be neither to nor from a target should be destroyed as inadvertent collection under the minimization procedures.

The Board recommends that Congress require that in the event NSA engages in "abouts" collection under the exigent circumstances described above, within six months of the resumption of "abouts" collection the government must submit to the FISC a report indicating: (a) the number of communications acquired through "abouts" collection; (b) an estimate of the proportion of such acquired communications that are neither to nor from a targeted selector; (c) an estimate of the number and proportion of any wholly domestic communications acquired; (d) an estimate of the number and proportion of multi-communication transactions acquired; (e) a description of the technical measures taken by NSA to limit acquisition of wholly domestic communications; (f) a description of the technical measures taken by NSA to limit access to, retention of, and dissemination of such acquired communications; and (g) any compliance incidents resulting from such acquired communications.

The Board also notes that, while "abouts" collection previously was employed only by NSA as part of upstream collection, the FISC has interpreted the statutory prohibition as applying to downstream collection as well. The Board recommends that any future "abouts" collection activities continue to be restricted to only upstream collection.

If Congress chooses not to codify the end of "abouts," the Board recommends that the government be required, prior to a decision to restart "abouts" collection, to perform a formal assessment of the value and impact of such a decision. Such an assessment should, at a minimum, include the mission value of the intelligence that would otherwise go uncollected; the available alternative methods for collecting the intelligence; a finding that the technical system for performing "abouts" collection is unlikely to result in the acquisition of purely domestic communications; and the privacy and civil liberties implications of such collection. The Board also encourages the government to engage with the Board in the process of preparing such an assessment. The Board recommends that such an assessment be submitted to the FISC and Congress.

RECOMMENDATION 3:

Congress should require FISC authorization of U.S. person query terms.

As discussed in Part 4 of this Report, querying Section 702 databases for U.S. person information is not merely ancillary to the Section 702 program, but has become a central feature of the program. Whereas Section 702 was initially predicated on a need to obtain foreign intelligence information involving foreigners reasonably believed to be located outside the United States, in the three years spanning January 1, 2020 through December 31, 2022, FBI alone has queried Section 702 databases for U.S. person information nearly 5 million times.

Further, despite Congress enacting Section 702(f)(2) in 2018 requiring FBI to go to the FISC for approval of certain evidence of a crime queries, the government has never sought a FISC order pursuant to (f)(2), even when they should have done so. We are also aware of numerous

other compliance incidents with respect to U.S. person queries—such as querying protesters, a Member of Congress, clergy, and community partners of FBI. The scale of U.S. person queries, the number of compliance issues surrounding U.S. person queries, and the failure of current law and procedures to protect U.S. persons compels the Board to recommend a new approach.

Accordingly, Congress should require FISC review and approval of U.S. person query terms before the government can access the results of any U.S. person query. For the reasons outlined below, this FISC review should be conducted under the current standards of "reasonably likely to retrieve" foreign intelligence or "reasonably likely to retrieve" evidence of a crime. We also recommend that Congress include two exceptions to this FISC approval requirement to account for queries conducted with actual consent for the purpose of identifying communications related to victims and for exigent circumstances.

Currently, without any individualized court approval, government agents can use U.S. person identifiers to query unminimized Section 702 databases for years of a specific American's incidentally collected private communications. This resulting content could produce a detailed look into an individual's private communications, be disseminated across the government, and be used in a criminal prosecution.[1] Such queries may also seek information regarding current and former government officials, federal campaign advisors, attorneys, religious leaders, and journalists, among others. Many Americans may be in frequent correspondence with foreign relatives or business contacts, and such queries could provide the government with extensive private information on these U.S. persons. The government would have needed prior judicial approval to obtain such information if the government had initially targeted the communications of a U.S. person (rather than a foreign person).

Further, in other contexts in which Americans' private communications may be incidentally collected, the government must first obtain an order based on individualized judicial review to approve the target. With Section 702, by contrast, there is no judicial review of targeting decisions.

When NSA, FBI, CIA, and NCTC conduct U.S. person queries seeking foreign intelligence information, we believe the current "reasonably likely to retrieve" foreign intelligence information standard still is appropriate.

FBI is the only agency that conducts U.S. person queries for both foreign intelligence and evidence of a crime purposes. Although FBI's querying procedures and practices pose the most significant risks to Americans' privacy and civil liberties, FBI asserts that a probable cause standard may be too demanding to meet in many circumstances in which FBI would otherwise seek to access the results of a U.S. person query. The most critical safeguard for Americans'

[1] As discussed in this Report, any dissemination would be subject to requirements outlined in the relevant minimization procedures, such as being necessary to understand foreign intelligence information.

privacy rights is to require individualized and particularized judicial review for all U.S. person query terms. It also may be more practicable to apply a consistent standard across all types of queries so that the standard would be the same for foreign intelligence queries, evidence of a crime queries, and "dual purpose" queries expected to return both types of information. The probable cause standard in the foreign intelligence context presents challenges as to how it can be consistently applied in the absence of a criminal law predicate, particularly since Section 702 databases are designed to compile foreign intelligence.

For these reasons, the Board recommends that Congress require FISC review and approval under the current standards of "reasonably likely to retrieve" foreign intelligence or "reasonably likely to retrieve" evidence of a crime in order for the government to access the results of any query using U.S. person query terms.

FBI in particular has urged that requiring prior FISC review of all U.S. person query terms would be unduly burdensome and that the vast majority of FBI U.S. person queries do not return "hits." Providing FISC review prior to the government accessing the results of a U.S. person query will help address this concern, while still providing the critical safeguard of individualized judicial review before any government personnel may review a compilation of the content of communications of any U.S. person.

Therefore, we recommend that prior to seeking FISC approval, government analysts be allowed to search the Section 702 databases without reviewing the results in order to first determine whether there is a hit on a particular U.S. person query term. Congress should allow the government to use internal procedures, under standards at least as rigorous as those in place today,[2] to make such a determination without having to obtain FISC approval. If there is a hit on the U.S. person query term, the government would then need to request FISC approval to retrieve the content of those results. This would allow the government to resolve the common case of "non-hit" searches without needing FISC review.

While our policy recommendation is that Congress adopt the "reasonably likely" standard for all U.S. person queries, the Board would also support a congressional determination that for any U.S. person query designed to retrieve evidence of a crime as at least one purpose of the query, the FISC could apply a higher probable cause standard (while reserving the "reasonably likely" standard for non-evidence of a crime queries).[3] When Americans face the prospect of criminal

[2] For example, NSA currently requires a prior written justification and approval by its Office of General Counsel before conducting a U.S. person query in Section 702-acquired content.

[3] If Congress were to pursue a probable cause standard, Congress could extend the current requirements under Section 702(f)(2)(C) and (D) to all FBI U.S. person queries conducted at least in part to seek evidence of a crime. Section 702(f)(2) would need to be updated to reflect its application to access the results of all U.S. person queries conducted at least in part for evidence of a crime, rather than the current context, which limits the FISC approval requirement to queries conducted in connection with a predicated criminal investigation that does not relate to the national security of the United States.

investigation and prosecution, their privacy and civil liberties interests are at their highest, and such a requirement would maintain parity with the safeguards available under criminal law more generally.

The Board also recommends that Congress include two specific exceptions to the requirement for FISC approval of U.S. person query terms. First, the government has indicated that a substantial portion of its U.S. person queries, at least within FBI, have been related to identifying victims. This has included statements in the Intelligence Community's Annual Statistical Transparency Report for 2021 regarding queries to identify victims of malicious cyber activity and other threats, and remarks by an FBI official at PCLOB's public forum in January 2023 regarding identification of victims in terrorist plots and counterintelligence operations. As such, Congress should provide a consent exception in which the government can access Section 702 communications associated with a U.S. person query with the actual consent of the U.S. person without having to obtain FISC approval.

Second, the government has asserted that a requirement for FISC approval to conduct or review the results of U.S. person queries would create substantial delays that would adversely affect intelligence operations and criminal investigations. To address this concern, Congress should include a provision that makes an exception for exigent circumstances, modeled upon other exigent circumstances provisions in FISA.[4]

The Board also recognizes that the government and the FISC will likely need additional resources to provide the additional documentation and to review applications, respectively. The updated statistics released by FBI showing that system changes adopted in 2021 resulted in a dramatic decline in the number of U.S. person queries suggest that the burden of a prior approval requirement is substantially lessened. Nonetheless, the Board urges that Congress provide additional resources to the government and the FISC, as appropriate to implement this requirement.

RECOMMENDATION 4:

Congress should codify any exemptions from and exceptions to the Section 702 querying procedures in order for such exemptions and exceptions to be implemented.

Each agency's Section 702 querying procedures set forth certain exemptions and exceptions that describe searches that would otherwise meet the query definition but to which the querying procedures do not apply. For example, the querying procedures all include a general emergency exception, which allows agencies to take action in apparent departure from the procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) when it is not feasible to obtain a timely modification from the procedures. The agency

[4] *See* 50 U.S.C. § 1805(e).

must make a record of the action taken—to include any query term(s) used—and report the action taken to DOJ and ODNI, which must promptly inform the FISC of such activity.

The four agencies' querying procedures also include a variety of other exemptions and exceptions. For example, FBI's querying procedures do not apply to queries it determines are necessary to: (a) perform lawful training functions of its personnel; (b) conduct technical maintenance of FBI systems; (c) comply with Freedom of Information Act or Privacy Act requests; (d) comply with a court order or congressional mandate; (e) identify information that must be produced or preserved in connection with a litigation matter; (f) conduct vulnerability or network assessments; or (g) perform lawful oversight functions of FBI's personnel or systems.

The NSA, CIA, and NCTC querying procedures include many of those exceptions, but not all, and include some additional exceptions. NSA's querying procedures include an exception for queries conducted to identify and remove child exploitation material from NSA systems. Neither FBI, CIA, nor NCTC's querying procedures contain a similar provision. Each of these exceptions has the effect of narrowing the scope of what constitutes a U.S. person query subject to the rules outlined in the procedures and requirements for transparency reporting on the number of such queries.

In the 2018 reauthorization of Section 702, Congress added a requirement that the government adopt querying procedures that must be approved by the FISC as part of the annual certification of Section 702. The legislation did not include any explicit authorization for exemptions or exceptions that would permit certain types of queries to be conducted without following the required querying procedures. Setting forth broad exceptions to the querying procedures can create privacy risks when not subject to robust oversight. While the Board agrees that some of these exemptions and exceptions appear reasonable, the Board recommends that Congress codify any exemptions from or exceptions to the querying procedures in order to permit their implementation, ensuring that each category receives robust consideration and oversight. Congress should also consider whether and how any such exemption or exception it codifies should apply to the requirement for FISC approval of U.S. person query terms, as outlined in our Recommendation 3 above. Codification of the exceptions will also require any Intelligence Community requests for new exceptions to go through congressional negotiations rather than only submission to the FISC as part of the annual certification process.

RECOMMENDATION 5:

Congress should require that NSA perform and publish an assessment of the feasibility and value of proposed methodologies for estimating the scope of incidental collection of U.S. person information, including the use of statistical and cryptographic techniques. Congress should establish lawful processes for private providers to assist with the assessment as necessary.

In the 2014 PCLOB Report, the Board recommended that the Intelligence Community make public a series of metrics to provide transparency and "insight about the extent to which NSA acquires and utilizes communications involving U.S. persons and people located in the United States under the Section 702 program." The Intelligence Community implemented two of the five specified metrics, and has made them available through the Annual Statistical Transparency Report but declined to implement the other three. The Intelligence Community has not otherwise estimated the scope of incidental collection of U.S. person information, such as the number of communications incidentally collected, the number of U.S. persons who have had their communications collected, or the number of communications collected under Section 702 that contain U.S. person information. Although NSA initially advised that it would work with Board staff to develop alternative measures to provide insight into the extent of incidental collection,[5] it has declined to do so. In 2017, then-Director of National Intelligence Daniel Coats testified that it was infeasible to prepare a metric that was precise and meaningful without requiring undue analytic effort or overly intrusive analysis that itself would create a privacy risk to U.S. persons. The Intelligence Community maintains this position.

The Board continues to believe that providing additional information regarding the scope of incidental collection of U.S. person information would enable more informed understanding by the public and policymakers. The Board recognizes that no one metric is likely to capture incidental collection fully and accurately, and implementation of this recommendation need not unduly burden NSA or disrupt the work of its analysts. Rather, a set of values, even if approximate, with appropriate caveats and explanations (e.g., which figures are likely to be undercounts or over counts) could facilitate transparency and meaningfully inform the public and policymakers. There have been multiple public proposals for techniques to measure the scope of incidental collection. For example, in the Board's 2022 *Recommendations Assessment Report*, PCLOB staff urged that NSA continue its prior commitment to develop alternate metrics that would provide insight into the scope of incidental collection, such as appropriately designed statistical measurement or an estimate based on cryptographic techniques. For example, some academic researchers have published a proposal for a cryptographically secure method to compute the volume of incidental collection of people reasonably believed to be located in the United States without revealing sensitive information either to the government or to internet service providers.[6] The Board takes no position on which specific approach would be best.

---

[5] PRIV. AND C.L. OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT, at 25-26 (2016), https://documents.pclob.gov/prod/Documents/OversightReport/8ab510df-738f-44b5-a73a-08d1336d544d/Recommendations_Assessment_Report_20160205%20-%20Completed%20508%20-%2010252022.pdf.

[6] ANUNAY KULSHRESTHA & JONATHAN MAYER, ESTIMATING INCIDENTAL COLLECTION IN FOREIGN INTELLIGENCE SURVEILLANCE: LARGE-SCALE MULTIPARTY PRIVATE SET INTERSECTION WITH UNION AND SUM (2022), https://www.usenix.org/system/files/sec22-kulshrestha.pdf.

The Board recommends that Congress require a pilot project at NSA to assess the viability of one or more of the available proposals and others that may be developed and provide the necessary legal authorities to permit service providers to assist as needed. To the extent possible consistent with the need to protect sensitive information, NSA should publish an assessment of the feasibility and value of proposed techniques for estimating incidental collection. Such an assessment should: (a) estimate the time, costs, and resources necessary; (b) evaluate the accuracy of proposed measurements; (c) interpret the estimates; (d) provide appropriate caveats; and (e) describe potential privacy and civil liberties concerns for each evaluated technique. Congress should further require that if NSA determines that one or more of the proposals is both feasible and valuable, it should include an implementation strategy in its assessment, and if NSA determines that none of the proposals would produce information that would be useful to Congress, it must work to develop a viable alternative methodology and report to Congress on its efforts.

RECOMMENDATION 6:

Congress should codify a requirement that the government submit to the FISC a random sample of targeting decisions and supporting written justifications from NSA, FBI, and CIA for *post hoc* judicial review as part of the annual Section 702 recertification process. The sample size and methodology should be approved by the FISC.

The FISC reviews the government's proposed targeting and minimization procedures each time the government seeks approval or re-approval of a certification, typically annually. In the 2014 PCLOB Report on Section 702, the Board recommended that, to assist in the FISC's consideration of the government's periodic Section 702 certification applications, the government should submit with those applications a random sample of targeting decisions (reflected in "tasking" sheets)[7] with supporting documentation. The Board also recommended that the FISC approve the sample size and methodology. As a successor to this 2014 recommendation, the Board now recommends that Congress codify a requirement that the government submit a random sample of targeting decisions from NSA, FBI, and CIA for *post hoc* review as part of the annual Section 702 recertification process. In the Board's two most recent Recommendations Assessment Reports concerning the 2014 PCLOB Report, we note that the government tried to implement this recommendation and the FISC declined to pursue it further. Specifically, since the government sought to implement the recommendation in 2015, the FISC has declined to receive tasking sheets

[7] That recommendation, Recommendation 4 of the 2014 PCLOB Report, also urged that the government should submit a random sample of NSA's and CIA's U.S. person query terms to the FISC. However, the Board considers U.S. person queries in other recommendations in this Report, and this recommendation is specific to targeting decisions.

for review.[8] To ensure implementation of the 2014 recommendation and to clarify the FISC's jurisdiction, the Board recommends that Congress mandate such a requirement.

The Board, as it did in 2014, again assesses that this kind of retrospective information, if submitted to the FISC as part of the annual Section 702 recertification process, would assist the FISC in making an informed review of the government's targeting procedures. Specifically, it would enable the FISC to take a retrospective look at the targets selected and verify that the government's representations during the previous certification approval were accurate. The Board assesses that, if implemented, this recommendation would provide the FISC with additional insight into whether the government is, in fact, satisfying the "foreignness" and "foreign intelligence purpose" requirements, and could signal to the Court what changes to the targeting procedures might be needed, or prompt relevant inquiry by the Court.

RECOMMENDATION 7:

Congress should strengthen the role of the FISC amicus and improve transparency for FISC opinions.

When Congress enacted the USA FREEDOM Act in 2015, it improved the operation and transparency of the FISC, including by creating the role of FISC *amicus curiae* and by requiring a declassification review of every decision by the FISC that involves a significant construction or interpretation of law. Both of these measures have been valuable, but amici have been limited in their ability to assist the Court, including notably in FISC proceedings concerning the annual Section 702 certifications, and there have been lengthy delays in the declassification reviews of FISC opinions. The Board recommends that Congress expand and strengthen the amicus role in order to enhance oversight and bolster public trust in the FISC and, in turn, in the Section 702 program. The Board further recommends that Congress amend the requirement for declassification reviews of FISC opinions to set a time limit for such reviews.

The role of amici is not as robust as the role envisioned in the Board's previously recommended "special advocate" role[9] in three particular ways, all of which have been implicated in the FISC's consideration of Section 702. The Board recommends that Congress amend the FISA amicus provision to address all three issues.

---

[8] *See* PRIV. AND C.L. OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT, at 16-17 (2022), https://documents.pclob.gov/prod/Documents/OversightReport/c29f61be-88e1-47bf-bc76-3d39215a5ceb/2022%20Recommendations%20Assessment%20Report.pdf.

[9] PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, at 187-89 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/cf0ce183-7935-4b06-bb41-007d1f437412/215-Report_on_the_Telephone_Records_Program%20-%20Completed%20508%20-%2011292022.pdf [hereinafter 2014 PCLOB Section 215 Report].

First, the Board urges that Congress expand the types of matters in which the FISC and FISC-R shall appoint amici to participate beyond those involving "novel and significant" issues to explicitly include the annual Section 702 certification process. As discussed in Part 4 of this Report, since Congress created the amicus role in 2015, the FISC has not always appointed an amicus to assist the Court in reviewing Section 702 certifications. In the Board's view, it would be beneficial to ensure amicus participation in this annual process regardless of whether the FISC believes the issues under consideration meet the current statutory standard, which requires appointment of an amicus only when the matter involves a "novel or significant interpretation of the law." Even if there are no novel legal issues in a given year, the breadth of the Section 702 program, ongoing changes in technology, and continuing updates to the government's implementation of the program all counsel in favor of ensuring that the FISC will hear from an amicus when it evaluates recertification of the program and considers whether changes to targeting, minimization, and querying procedures are needed. Therefore, at a minimum, Congress should expand the category of cases requiring amicus participation to include the FISC's annual consideration of Section 702.

A helpful model for Congress to consider in connection with reauthorization of Section 702 comes from recent congressional debate, and the Senate version of the USA FREEDOM Reauthorization Act of 2020 included a provision authorizing amici to participate in cases related to: (a) "significant concerns" regarding First Amendment-protected activities; (b) "sensitive investigative matters;" (c) matters involving a new program or technology or use of technology; and (d) requests for reauthorization of programmatic surveillance such as the annual Section 702 certifications.[10]

Second, the Board recommends that Congress amend the FISA amicus provision to direct that amici should have full access to all the information related to matters in which they participate, providing them with the same information that is available to the government in these matters. In addition, the Board recommends that Congress amend the amicus provision to provide that whenever the FISC or FISC-R appoints an amicus curiae in a matter, that individual may consult with other amici designated on the FISC's approved list regarding any information relevant to the proceeding. As discussed in Part 4, amici currently do not have the ability to consult each other on cases, creating additional challenges to their ability to fulfill their duties, and differing from typical legal practice outside the context of the FISC.

Third, Congress should authorize amici to seek appellate review and petition for appeal of decisions by both the FISC and the FISC-R. Since amici are not parties, they would not be able to appeal as of right, and the FISC-R and the Supreme Court would retain the discretion to accept or deny these petitions. In the Board's January 2014 *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign*

[10] Lee-Leahy Amendment to USA FREEDOM Reauthorization Act of 2020, S.Amdt. 1584 to H.R. 6172 (2020).

Intelligence Surveillance Court, Recommendation 4 outlined two possible pathways for Congress to enable "special advocates" to seek appellate review of decisions by the FISC and the FISC-R.[11] As outlined in that recommendation, Congress could either authorize amici to file petitions for review in the FISC-R and in the Supreme Court, or could authorize amici to make requests to the FISC and to the FISC-R that they certify their opinions for appeal. The Board's report described each option in some detail, and explained that both approaches would be consistent with Article III standing requirements. Specifically, because amici are not parties to the cases in which they appear, the courts would retain the discretion on whether to accept an appeal or to certify a decision for review.

With regard to the declassification reviews of FISC decisions, orders, or opinions involving a significant construction or interpretation of law, the Board recommends that Congress set a time limit for such reviews so that the declassification review and public release of each such decision, order, or opinion must be completed no later than 180 days after the date on which the decision, order, or opinion was issued.

Additionally, the Board recommends that the Director of National Intelligence also conduct a declassification review of FISC filings from amici, and make them publicly available to the greatest extent practicable, as part of the process of declassification review and publication of FISC opinions and orders under FISA Section 602.[12]

RECOMMENDATION 8:

NSA should conduct annual evaluations to ensure continual improvements and modern capabilities are applied to limit the amount of backbone traffic screened and acquired during upstream collection and to document those efforts as part of the annual certification process.

The Board finds that NSA has made considerable progress in limiting the amount and types of traffic that is screened, and has taken additional, significant measures designed to ensure that only communications to or from tasked selectors are collected and retained by NSA. This is of great importance. The changes implemented by NSA since it suspended upstream "abouts" collection in 2017 have improved privacy and civil liberties protections by ensuring a more focused collection.

However, given the extraordinary potential reach of upstream collection, and the common public concerns about the reach and scope of such activities, the Board believes that both NSA and the public would be well served if NSA formalizes, measures, and consistently updates and

[11] 2014 PCLOB Section 215 Report, *supra*, at 187-89.

[12] 50 U.S.C. § 1872.

evaluates such efforts. The Board recommends that NSA regularly assess the effectiveness of such measures and revise or refine them as technology improves and as operational needs change.

To further focus the upstream collection and ensure consistent technological improvement, NSA should take the following steps.

1. NSA should document and formalize measures to:
    a. Screen and collect only traffic likely to contain communications of targeted selectors during upstream acquisition;
    b. Remove traffic that is purely domestic or is neither to nor from a targeted selector; and
    c. Remove traffic not likely to contain foreign intelligence information.
2. On an annual basis, NSA should evaluate the performance of such measures and consider possible additional modifications or improvements to:
    a. Reduce the amount of traffic scanned for the presence of selectors and
    b. Further focus collections to only relevant targeted traffic.
3. NSA should submit a report containing such measures and evaluations to the FISC as part of the annual certification process.
4. NSA should make all such measures and evaluations available to appropriate oversight bodies.

In addition, the government should document and formalize interactions with providers in conducting upstream collection.

RECOMMENDATION 9:

FBI and CIA should strengthen their post-targeting review requirements for foreign intelligence targets and improve their systems to ensure that collection from targets remains appropriate and continues to generate valuable foreign intelligence.

Under the targeting procedures, NSA, FBI, and CIA personnel are required to engage in post-targeting review of Section 702-acquired content. This review is required in order to ensure that targets are appropriate and to assess whether detasking is required on the basis that the target has entered or intends to enter the United States or has gained U.S. person status. The procedures require that this review is conducted "according to analytic and intelligence requirements and priorities," but agency policies generally require that the review occur within five business days of an agency receiving initial collection and every thirty business days thereafter.

NSA systems include features that prompt analysts and facilitate their compliance with the post-targeting review obligations. NSA has developed automated systems that provide a notification when initial collection arrives, along with automated, periodic reminders to meet their review obligations. These notifications remind analysts to review collection from tasked selectors within five business days after the first instance that data is acquired for a particular tasked selector, and at least every 30 days thereafter.[13] NSA's system is also designed to record the fact that the analyst conducted the review.

The Board recommends that if FBI or CIA has primary responsibility for reviewing the Section 702 collection from a selector for which NSA would apply a heightened obligation to review, FBI and CIA personnel should be required to review the collection every ten business days. In addition, the agencies should develop systems that provide standardized prompts reminding an analyst to conduct the review and that record whether the analyst does so, similar to how NSA systems operate.

RECOMMENDATION 10:

The Intelligence Community should establish protocols and update systems to accommodate and require tagging Section 702-acquired information that analysts determine contain U.S. person communicants.

Currently, there is no requirement that Intelligence Community personnel tag or identify any Section 702-acquired communication that they discover includes a known U.S. person communicant. The Board believes that certain proactive measures can be adopted such as data tagging communications when personnel assess they involve U.S. person communicants. These could provide insight into U.S. person communications without unduly burdening or disrupting the work of Intelligence Community personnel or requiring the agencies to further scrutinize the contents of these communications. Such tagging would facilitate application of the rules under the minimization procedures regarding use, retention, and sharing of information concerning U.S. persons.

The Board thus recommends that the Intelligence Community agencies adopt the necessary policy changes and implement the required system modifications to enable and require forward-looking tagging of data assessed to contain collection of U.S. person communications. The Board is not recommending that the Intelligence Community agencies conduct any extra investigation in order to apply this tag; rather, we recommend that if they otherwise determine an individual is a U.S. person in the course of their regular duties, they apply this tag to avoid further duplication of effort. The act of applying a tag to data already assessed by a human to contain U.S. person communications through the regular course of their analytic duties would tag the data to alert other

[13] *See* 2014 PCLOB Report, *supra*, at 48.

analysts that the data contains U.S. person information, enable application of rules related to treatment of U.S. person information, and provide a decision point for data purge to further reduce privacy concerns.

RECOMMENDATION 11:

The Intelligence Community should increase clarity and, where possible, parity regarding agencies' required treatment of Section 702-acquired attorney-client communications. In addition, FBI specifically should centralize tracking of criminal indictments and taint review teams to limit the number of attorney-client communication compliance incidents.

In its review of the agency minimization procedures, the Board found variance in how agency personnel treat attorney-client communications, including how such material was defined, marked (i.e., tagged), flagged for review, disseminated, and purged. For example, if NSA, CIA, or NCTC personnel determine that an attorney-client communication does not contain foreign intelligence information or evidence of a crime, the agency must destroy the communication, irrespective of whether it contains information protected by the attorney-client privilege. If, however, an attorney-client communication does appear to contain foreign intelligence information or evidence of a crime, personnel must bring the communication to the attention of agency attorneys for further handling. Conversely, FBI does not require legal review of all attorney-client communications that appear to contain foreign intelligence information or evidence of a crime, and personnel need not purge attorney-client communications that do not contain foreign intelligence information or evidence of a crime.

The Board recommends that DOJ update the agency minimization procedures to ensure that NSA, FBI, CIA, and NCTC use and define the term "attorney-client communication" consistently, as opposed to "attorney-client privileged communication," and treat attorney-client communications consistently. Although it may be appropriate for FBI to handle the taint team process differently than other agencies given its law enforcement role, the Board further recommends that DOJ work with the Intelligence Community to determine where greater parity may be achieved among the various ways that agencies handle attorney-client communications. Privacy protections could be enhanced through consistent marking and disseminating of such information. The Board understands that purging of attorney-client communications not containing foreign intelligence information or evidence of a crime may not be practicable at FBI due to the agency's discovery obligations. However, the Board recommends that FBI create a means for sequestration of such communications, permitting further access only after attorney review. Such review should permit access only when the attorney-client communication is needed for discovery purposes or is relevant to an ongoing investigation and is foreign intelligence information or evidence of a crime. Finally, Intelligence Community agencies should notify any agency that receives the Section 702 collection if that material contains attorney-client communication.

Separately, under FBI's minimization procedures, as soon as a target is charged with a federal crime, FBI personnel must establish a taint team to review Section 702-acquired information. The taint team reviewers have no role in the prosecution of the criminal matter and ensure that review of the collection does not prejudice the defendant. The Board has found, however, that FBI does not have a central tracking mechanism for criminal indictments, which creates uncertainty among the 56 FBI field offices about whether a Section 702 target has been or is about to be charged with a crime. This uncertainty increases the risk of compliance incidents resulting from taint teams not being established in a timely manner and a potential mishandling of attorney-client communications. The Board recommends that FBI better centralize how it tracks its criminal indictments across field offices to notify agency personnel who may be monitoring a Section 702 target if that target has been charged with a crime.

RECOMMENDATION 12:

FBI, in batch queries, should ensure that each query term that relates to a specific person may be used only if it individually meets the applicable query standard and approval process. In the case of query terms associated with non-U.S. persons, each term should meet standards developed following an assessment in accordance with E.O. 14086's requirement that signals intelligence activities be conducted only as is necessary and proportionate to a valid intelligence priority.

As discussed earlier in this Report, a batch job query runs multiple query terms as part of a single query action. All of the query terms in a batch job query rely on the same justification. These terms may be entirely distinct from one another, such as a series of email addresses, or they may be different combinations of terms or alternate spellings. Query terms may relate to a specific individual, whether a U.S. person or a non-U.S. person.

The use of a single justification for multiple query terms associated with different individuals without individualized assessments increases privacy risks to those individuals. On the other hand, the batch query tool also provides value by enabling analysts to detect connections among individuals associated with the query terms used in batch queries. The Board assesses that it is possible to address these privacy risks while preserving the government's ability to use the batch query tool as a method for detecting these connections.

In June 2021, FBI began requiring users to obtain attorney approval to conduct batch job queries combining 100 or more query terms. As of June 2023, FBI requires every batch job query to be approved by an attorney. This is a helpful improvement, and FBI should continue to include such attorney review. This is consistent with another recommendation in this Report, in which the Board urges that U.S. person query terms must be individually approved by the FISC to improve privacy safeguards for U.S. person queries. Validating each U.S. person query term through implementation of that recommendation would address the privacy risks to U.S. persons.

With regard to query terms associated with non-U.S. persons, the government should ensure that those query terms are validated through standards that comport with E.O. 14086's necessity and proportionality requirements. As noted in Part 4, the Board recognizes that the specific requirements of Section 2(c) of the Executive Order regarding queries of bulk collection do not apply to Section 702, but Section 2(a) of the Executive Order requires that all signals intelligence activities must be necessary and proportionate to a validated intelligence priority. In some historical incidents, FBI personnel have been unable to articulate a proper justification for why a particular query term is likely to be found in Section 702-acquired information. The lack of a proper justification for thousands of queries gives the Board concerns about whether FBI's batch job queries have been conducted in a manner consistent with E.O. 14086's requirement that signals intelligence be conducted only to the extent and in a manner that is necessary and proportionate to a valid intelligence priority.

The new FBI requirement that all batch job queries must be approved by an attorney should help, and all guidance and other relevant materials should be formalized into official documentation. Further, the Board recommends that the government conduct a legal analysis of what query standard should apply to query terms associated with non-U.S. persons to ensure compliance with the necessity and proportionality standards in E.O. 14086. That standard should apply to all queries involving terms associated with non-U.S. persons, including when such terms are used in batch queries.

RECOMMENDATION 13:

The NSA, FBI, CIA, and NCTC querying procedures should be updated to require that personnel, prior to conducting a query in raw Section 702 information, perform due diligence to assess the U.S. persons status of the query subject by searching in minimized FISA and non-FISA datasets.

The Intelligence Community agencies are required to report annually the number of U.S. person query search terms (for queries of unminimized content) and the number of queries conducted (for queries of unminimized non-content information) of raw Section 702 information. In addition, there are certain requirements that apply only to U.S. person queries and not to other types of queries. To facilitate such recordkeeping and determinations as to whether rules regarding U.S. person queries apply, personnel must indicate in agency systems when a query term is reasonably likely to identify one or more specific U.S. persons. When the status of that query term is unknown, agency personnel operate off a series of presumptions set forth in the querying procedures to assess whether an individual is likely a U.S. person. These presumptions, by definition, are applied when personnel are relying upon incomplete information, and as a result they may result in compliance incidents. As a matter of policy, but not under NSA's querying procedures, NSA personnel are required to perform pre-query due diligence in order to make an informed assessment of the U.S. person status of the subject of a query. In particular, the policy

states that analysts should search appropriate databases that may help inform the U.S. person status of the query subject. This does not include open source or all information that may be available to the analyst.

Pre-query due diligence enables NSA personnel to rely on more complete information, and is therefore more likely to result in more accurate assessments regarding the U.S. person status of query subjects. Thus, the Board recommends that, absent exigent circumstances, FBI, CIA, and NCTC require their personnel to perform pre-query due diligence to inform personnel as to the likely U.S. person status of query subjects. As with current NSA policy, this would include searching appropriate databases that may help inform the U.S. person status of the query subject but would not include open source or all information that may be available to the analyst. These due diligence requirements should be incorporated into all four agencies' querying procedures.

RECOMMENDATION 14:

The Intelligence Community should improve its recordkeeping of certain types of queries of raw Section 702-acquired information, including sensitive queries of raw Section 702-acquired information, and, in the case of FBI, evidence of a crime only queries. The number of these queries, along with the number of U.S. person queries, should be published annually in the Annual Statistical Transparency Report (ASTR).

The ASTR is an important mechanism by which the government provides transparency regarding the Intelligence Community's use of FISA and certain other national security authorities. It is through this unclassified report that the public has been made aware of the recent decrease in the number of U.S. person queries of raw Section 702-acquired information. For example, in the most recent ASTR released in April 2023, the Intelligence Community reported that, during calendar year 2022, NSA, CIA, and NCTC used a total of 4,684 U.S. person query terms to search Section 702-acquired information, and FBI used 119,383 unique U.S. person query terms.

The Board finds that publicly providing metrics regarding U.S. person queries brings much-needed transparency to this program. The Board thus recommends that the Intelligence Community agencies update their systems to tag and record certain other types of queries, including sensitive queries, and, in the case of FBI, evidence of a crime only queries.

For agencies that have adopted special procedures for sensitive queries, agency systems should track the number of sensitive queries that have been requested and the number of sensitive queries that have been approved. Annually, the Intelligence Community agencies should publish both numbers in the ASTR.

Separately, based on the Board's review of the design of FBI's querying systems, the Board finds that FBI systems are not accurately capturing when a user is querying Section 702-acquired information for evidence of a crime only. As discussed earlier in this Report, if FBI personnel would like to view the contents that result from a query conducted for evidence of a crime only,

the query must then be reported to the FISC on a quarterly basis. The Board's investigation has found that FBI read this reporting requirement very narrowly, and structured its systems in a way that fails to accurately capture what is likely the vast majority of evidence of a crime only queries. Specifically, FBI personnel only document a query justification when attempting to access the Section 702 contents retrieved by a U.S. person query. Consequently, the number of queries in which FBI users provide documented justifications indicating that the purpose of the query was to retrieve evidence of a crime only represents a small subset of the total number of such queries. In fact, in its September 2021 order, the FISC referenced the government's assertion that, out of over two million queries, none were performed for evidence of a crime only. This led the FISC to question the credibility of this metric and suggested that FBI is under-reporting the queries.

The Board recommends that FBI structure its querying systems so that the systems prompt users to indicate at the *outset* of performing a query whether it is being conducted for evidence of a crime only, regardless whether or not it relates to a likely U.S. person. Making this simple system design change will enable FBI to accurately count when a user is querying Section 702-acquired information for evidence of a crime only. Once FBI is able to implement this system change, the Board recommends that FBI report the number of evidence of a crime only queries, regardless of whether they relate to U.S. persons, annually in the ASTR. Providing meaningful metrics regarding FBI's evidence of a crime only queries will bring much-needed transparency to FBI's use of this foreign intelligence surveillance program for law enforcement purposes.

RECOMMENDATION 15:

FBI should strengthen its internal Section 702 compliance processes and supplement its internal auditing.

The Board recommends that FBI adopt more robust compliance programs and processes, similar to those of NSA, with appropriate budgeting and staff. In reviewing the internal compliance programs of the Intelligence Community agencies, the Board has observed that FBI's internal Section 702 compliance program is not appropriately robust. A number of issues have contributed to FBI's relatively high query compliance incident rate compared to other agencies, including FBI system design issues, and individual errors that resulted in large-scale incidents. However, the Board finds that many of these compliance incidents could have been avoided if FBI had a stronger internal compliance program.

Currently, DOJ's National Security Division is the primary auditor of FBI's Section 702 compliance. The Board recommends that FBI engage in more of its own Section 702 post hoc auditing, permitting DOJ and ODNI to serve as secondary reviewers rather than frontline auditors. The Board notes that, in September 2022, DOJ's Office of the Inspector General reported that the former Assistant Attorney General for the National Security Division also recommended that FBI perform more of its own internal compliance reviews. While the majority of compliance incidents at NSA are discovered internally, the vast majority of FBI's compliance incidents are discovered

by DOJ and ODNI oversight.

As described earlier in this Report, a number of FBI entities participate in FBI's Section 702 internal compliance program, and in 2020, FBI established its Office of Internal Auditing (OIA) to apply auditing processes to FBI's national security activities.

Only a small number of these personnel, however, reported that their primary responsibility was to ensure compliance with various requirements of FISA authorities, including Section 702. Further, FBI OIA has only conducted two audits of queries conducted by FBI personnel, neither of which resulted in a report available for review by the Board.

FBI's internal Section 702 compliance program is especially lacking as compared to that at NSA. NSA employs one employee whose primary responsibility is Section 702 compliance for every 69 personnel with access to Section 702. FBI, on the other hand, only employs one employee whose primary responsibility is Section 702 compliance for every 114 personnel with access to Section 702. FBI would benefit from a well-staffed office at FBI Headquarters with specially trained individuals who can easily be contacted regarding Section 702 compliance-related questions, as well as at least one specially trained employee at every FBI field office.

RECOMMENDATION 16:

DOJ should annually review each FBI field office's compliance with the Section 702 procedures.

The Board's investigation has shown that DOJ's oversight of FBI's compliance with the Section 702 procedures has been important in identifying and working to mitigate FBI's compliance issues. DOJ has been primarily responsible for identifying instances of noncompliance, and has provided in-person and real-time training to FBI personnel and described its findings in notices and reports to the FISC. The FISC uses this information to issue directives, including in its annual certification order. In addition, DOJ leadership has used this information to direct FBI to augment its internal compliance functions, including by directing FBI to establish its Office of Internal Auditing.

Prior to the COVID-19 pandemic, DOJ reviewed 25 to 30 of the 56 FBI field offices annually to evaluate their compliance with the Section 702 minimization and querying procedures. The pandemic interrupted such work. In 2021, DOJ restarted and increased its resources for FBI field office query reviews; in 2022, DOJ resumed remote FBI field office minimization reviews. In 2022, DOJ conducted querying reviews at 28 field offices and headquarters components and minimization reviews at 15 field offices. For querying, DOJ generally reviews a 90-day snapshot of queries of unminimized FISA-acquired information conducted by personnel in the relevant office in two FBI systems. For minimization, DOJ generally reviews a sample of minimization-related examples (i.e., the acquisition, marking, retention, and dissemination of FISA-acquired

information) for all of a field office's FISA investigations with actively tasked Section 702 selectors since the last DOJ review.

The Board finds that additional DOJ reviews of FBI field offices as well as at embassies would help mitigate many of the current FBI compliance issues. According to DOJ, FBI field office reviews are prioritized based on the volume of FISA investigations, and annual reviews of each field office would not be feasible given current resources. This field office prioritization results in some smaller offices undergoing DOJ review only every four years, allowing FBI personnel to go without adequate oversight and real-time training for multiple years. The Board thus recommends that DOJ annually review each FBI field office, and conduct regular reviews at each embassy where FBI personnel use Section 702.

RECOMMENDATION 17:

FBI should explore methods for the use of secure automated review and machine learning to supplement its manual internal auditing of Section 702 compliance.

The Board recommends that FBI better leverage its technological resources—including secure IT automation and machine learning—to more quickly and precisely identify, audit, and address Section 702 compliance issues. FBI should develop the capability quickly to understand trends and patterns in system usage. In 2020, FBI established its Office of Internal Auditing (OIA) to implement auditing processes for FBI's national security activities. Since its founding, OIA has conducted only two audits of the agency's Section 702 queries. Furthermore, based on its final report, those audits were limited in scope. FBI should expand OIA's role in auditing Section 702 compliance by developing and incorporating secure automated review processes, if possible, drawing on machine learning capabilities. The Board has learned that FBI can generate auditable query logs, but it does not conduct data analysis of the logs to assess system-wide compliance. Instead, FBI has historically largely relied on DOJ's manual oversight reviews of FBI queries, which occur at 25 to 30 of the 56 FBI field offices per year. Under current conditions, FBI lacks the fundamental capacity to develop a basic near-real-time sense of which field offices may be experiencing spikes in Section 702 queries, let alone whether improper searches are occurring and at what scale.

The Board assesses that there are opportunities for FBI to supplement its administrative safeguards with stronger technical safeguards. Some potentially feasible options include:

- Tracking patterns of use to identify:
    - Users who have abnormal patterns of use compared to peers, including anomalously large or small degrees of use relative to their mission responsibilities, which could trigger compliance and oversight checks in real time;
    - Sudden changes in an individual user's query patterns; or

- Broader compliance trends that could inform the focus of training, including which FBI field offices exhibit higher rates of noncompliance.

- Automatically reviewing whether analysts are re-using justifications or using boilerplate justifications for multiple U.S. person queries.

RECOMMENDATION 18:

NSA, FBI, CIA, and NCTC should submit to ODNI for annual review all internal and external training provided to personnel regarding the targeting, minimization, and querying procedures. DOJ should also make available securely online all external Section 702 training so that agency personnel can access this material on an as-needed basis. Additionally, Intelligence Community agencies should require supplemental retraining for personnel who have not accessed unminimized Section 702 data in the previous ninety days.

To accompany existing mandatory training, the Board recommends that agencies whose personnel access unminimized Section 702 information submit to ODNI for annual review all training provided to personnel regarding minimization, targeting, and querying procedures. Agencies currently employ different training methods and post-training resources and refreshers. The Board assesses that, if implemented, this recommendation would create a centralized process whereby training modules and materials could be evaluated for best practices and necessary updates. Particularly effective training modules also could be more easily shared among agencies both to increase consistency across the IC and to facilitate agency review and update of training practices.

The Board further recommends that DOJ make available securely online all external Section 702 training that it provides to other agencies so that personnel, particularly those across FBI's field offices, can access this material when needed. Currently, DOJ conducts in-person training of FBI personnel only during onsite field office reviews. Currently, FBI onsite field office reviews reach each office about once every three years. Making Section 702 training available securely online augments existing resources.

The Board also recommends that agencies require refresher training for personnel who seek to access unminimized Section 702 information but who have not accessed such data in the previous ninety days. This training would serve as a mandatory review for personnel of their individual agency's relevant policies and procedures, and would help prevent future compliance incidents.

RECOMMENDATION 19:

The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.

The Board recommends that the government expand upon and improve its efforts to implement Recommendation 10 from the 2014 PCLOB Report. Assessments of the value and efficacy of intelligence collection and counterterrorism programs are necessary elements in evaluating whether such programs are worth their economic and operational costs, as well as the real and potential privacy intrusions and harms that they generate. PCLOB has urged that the Intelligence Community provide such assessments of the programs under PCLOB oversight, including in the 2014 PCLOB Report.

In describing the value of Section 702, the government has historically shared a discrete set of anecdotes (sometimes called "vignettes" or "success stories") that illustrate various use cases or benefits of the program. Additionally, the Intelligence Community has provided top-level statistics on various operational elements of the program, such as targeting and tasking, reporting and dissemination of intelligence, and the use of queries. None of these is sufficient to measure the value and efficacy of the program in its entirety, let alone particular components of the program, operational policies, and applicability of the program against specific threats or focus areas, or similar questions.

An assessment of the program's efficacy helps Congress make informed budgetary and resource determinations. Successfully measuring efficacy within a program can make sure that the Intelligence Community *and* the American public both have confidence that resources are being allocated in the ways that most efficiently and effectively protect the nation with the minimum risk to our nation's values.

Such evaluation is standard and expected practice for government programs. Multiple statutes and executive branch regulations and practices require that executive branch agencies and departments review the performance of their programs and operations, with a focus on measuring the impact of these programs on strategic goals and objectives. The Foundations for Evidence-Based Policymaking Act of 2018 further defines frameworks and requirements of performance and program evaluation. The Office of Management and Budget has provided a number of publications defining terms and setting out requirements for executive agencies in performing their evaluation activities as well.

The Board recommends that the government continue and build upon efforts taken in response to Recommendation 10 from the 2014 PCLOB Report, and develop and implement specific, replicable, and routine assessment methodologies that sufficiently capture and clearly articulate the value and efficacy of the Section 702 program. To the extent possible, the results of these assessments should be published to facilitate transparency and civil society discussions in this space. This also would benefit the Intelligence Community as it makes its case for reauthorization to Congress and the American public. Consistent with the Principles of Intelligence Transparency, unclassified details or high-level summaries of such reports should be published regularly, perhaps included in the Annual Statistical Transparency Reports.

ANNEX A: SEPARATE STATEMENT OF CHAIR SHARON BRADFORD FRANKLIN

I support the Board's report in full, but write separately because I believe that Recommendation 3 should be further strengthened. Specifically, Congress should require that before FBI may access the results of a U.S. person query conducted at least in part to seek evidence of a crime, the government must obtain approval by the FISC under a probable cause standard.

The Board's Policy Analysis outlines both the value of and privacy risks created by conducting U.S. person queries of Section 702 information. As the Board stated, U.S. person queries present some of the most serious privacy and civil liberties harms caused by the Section 702 program. And, though the Board repeatedly pressed the government for cases showing the value of U.S. person queries, FBI in particular had difficulty finding examples of U.S. person queries that had provided unique value in criminal investigations.

The government's difficulty in providing examples of the value of U.S. person queries stands in stark contrast with the government's ability to demonstrate the overall value and importance of the Section 702 program in protecting U.S. national security. For this reason, the claims that requiring FISC approval of U.S. person query terms will damage the Section 702 program and cause grave harm to U.S. national security ring hollow. The government has indeed shown that U.S. person queries can be valuable, and the Board's report does not call for eliminating the practice. Yet, requiring FISC review of U.S. person query terms is necessary to protect Americans' privacy rights and, in my view, would neither cause an end to U.S. person queries nor undermine the overall efficacy of Section 702 in protecting U.S. national security.

The government uses U.S. person queries to search through collected 702 data seeking communications of or about Americans that have been incidentally collected. Incidental collection is a feature of the Section 702 program, not a bug. Importantly, through incidental collection, the government can learn when people inside the United States are on the other end of communications with its Section 702 targets and can seek to assess whether those people in the United States are working with the non-American targets to plot acts of terrorism or otherwise pose threats to the United States.[1] Incidental collection should be distinguished from reverse targeting, which the statute explicitly prohibits and which involves targeting someone outside of the United States as a pretext for acquiring the communications of someone inside the United States. The government takes the prohibition on reverse targeting seriously and has implemented meaningful safeguards to prevent such pretextual targeting. Nonetheless, even though U.S. person queries do not involve targeting another individual as a pretext, they do involve focusing in on a particular U.S. person as the actual subject of interest in a way that raises heightened privacy interests. Thus, at the

[1] The Board's Policy Analysis outlines the privacy risks posed by incidental collection, and Recommendation 5 urges Congress to require NSA to undertake further measures to estimate the scope of such collection.

juncture at which the government seeks to search through collected 702 data seeking information about a particular U.S. person, that investigatory focus is analytically equivalent to the process of targeting, and there is a need for independent judicial review, as we have laid out in Recommendation 3.

Understandably, Congress and members of the public have focused a great deal of attention on FBI's disturbing and continuing compliance violations in conducting U.S. person queries. To its credit, FBI has recently taken a number of steps to improve the design of its query tools and to strengthen policy requirements in an effort to reduce these errors. These changes are welcome and have already led to improvement in FBI's compliance rates, but the persistent pattern of FBI noncompliance over the years dramatically illustrates the need for independent, impartial, and external review. Further, even if FBI were able to improve its performance to the point of 100% compliance with current query standards without judicial review, this would be insufficient to address the privacy threats posed by FBI's U.S. person queries. To fully mitigate these threats, it is necessary to raise the standards in addition to improving compliance.

Implementation of the Board's Recommendation 3 would go a long way toward achieving this goal by requiring the critical safeguard of independent judicial review of U.S. person query terms. But I believe that Congress should also require a probable cause standard for FBI's U.S. person queries conducted at least in part to seek evidence of a crime[2] in order to fully protect Americans' privacy and civil liberties.

Like all of our recommendations in this report, Recommendation 3 is a policy recommendation based on our assessment of the steps needed to mitigate the privacy and civil liberties risks presented by the program. However, when the government runs a search through Section 702 data seeking information on a particular American, the practice raises constitutional concerns as well. As I have argued previously, a search through Section 702 communications data seeking information about a particular American constitutes a search under the Fourth Amendment, and current query standards are insufficient to meet

…[A] search through Section 702 communications data seeking information about a particular American constitutes a search under the Fourth Amendment, and current query standards are insufficient to meet constitutional requirements.

[2] The Factual Narrative section of this report describes "dual purpose" queries, where FBI conducts a query for both foreign intelligence and evidence of a crime purposes. Typically, FBI treats such queries as foreign intelligence queries, but the probable cause standard should apply to all such mixed purpose queries. Indeed, given FBI's law enforcement mission, it is unclear whether *any* FBI queries are conducted *solely* for the purpose of returning foreign intelligence information, without any possibility of using information as evidence of a crime. Thus, a probable cause requirement that applies to all FBI U.S. person queries conducted at least in part seeking evidence of a crime may, as a practical matter, need to apply to all FBI U.S. person queries.

constitutional requirements.[3] I recognize that the FISC has determined that current Section 702 querying procedures comply with the Fourth Amendment,[4] but the U.S. Court of Appeals for the Second Circuit has found that a U.S. person query is a separate Fourth Amendment event that itself must meet the reasonableness test as "a backstop to protect the privacy interests of United States persons and ensure that they are not being improperly targeted."[5] In that case, *United States v. Hasbajrami*, the Second Circuit remanded the question of whether the government's U.S. person queries had complied with the Fourth Amendment.[6]

This difference in interpretation between the FISC and the Second Circuit has not been addressed by other federal appellate courts.[7] Rather, in the few Section 702 cases considered by traditional Article III courts, the government has generally evaded judicial review on the question of whether U.S. person queries comply with the Fourth Amendment.[8] Even where the government has acknowledged conducting U.S. person queries under Section 702, it has asserted during judicial proceedings that the government did not rely on evidence obtained from a query as part of the prosecution.[9]

---

[3] Brief of Amici Curiae David Medine and Sharon Bradford Franklin in Support of Defendant-Appellant and Urging Reversal, *United States v. Muhtorov,* 20 F.4th 558 (10th Cir. 2021) [hereinafter Brief of Amici Curiae in *Muhtorov*].

[4] *See* Memorandum Opinion and Order, at 110, *In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications*, Docket No. 702(j)-23-01, *In re DNI/AG 702(h) Certification 2023-B and its Predecessor Certifications*, Docket No. 702(j)-23-02, *In re DNI/AG 702(h) Certification 2023-C and its Predecessor Certifications*, Docket No. 702(j)-23-03 (FISA Ct. Apr. 11, 2023).

[5] *United States v. Hasbajrami*, 945 F.3d 641, 672 (2d Cir. 2019). Others who have analyzed this issue, including a constitutional scholar, have also argued that U.S. person queries are separate Fourth Amendment events requiring their own justification. *See* Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of crimes*, WASH. PO. (Oct. 20, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-andquerying-the-702-database-for-evidence-of-crimes/.

[6] The district court's decision is still pending.

[7] One federal district court has considered querying of Section 702 information. *United States v. Mohamud*, 2014 WL 2866749 (D. Or. June 24, 2014). While the court in *Mohamud* stated that the query did not constitute a separate search, the court was actually assessing whether U.S. person queries affect the program's overall reasonableness under the Fourth Amendment. On appeal, the Ninth Circuit did not address the specific issue of querying, stating that the case "did not involve the retention and querying of incidentally collected communications. All this case involved was the targeting of a foreign national under § 702, through which Mohamud's email communications were incidentally collected. Confined to the particular facts of this case, we hold that the § 702 acquisition of Mohamud's email communications did not violate the Fourth Amendment." *United States v. Mohamud*, 843 F.3d 420, 438 (9th Cir. 2016).

[8] *See, e.g., Muhtorov*, 20 F.4th at 604-05 (stating that Muhtorov's "argument about post-seizure querying is inapposite because… the trial evidence was not derived from querying a Section 702 database…Querying might raise difficult Fourth Amendment questions that we need not address here.").

[9] *Id.* at 591-92*; see also* Oral Argument (No. 17-2669), *Hasbajrami*. 945 F.3d, at 45:30, https://www.ca2.uscourts.gov/decisions (the government stated that this was "not a criminal case that arose from a so called backdoor query").

In analyzing application of the Fourth Amendment to U.S. person queries, it is important to recognize the difference between searches and seizures.[10] The initial incidental collection of an American's communications under Section 702 constitutes a seizure, and when the government conducts a query into an American's collected Section 702 communications data, that query constitutes a search under the Fourth Amendment and requires independent justification.[11] The Supreme Court drew this distinction in *Riley v. California*, holding that, although the government had lawfully seized the defendants' cell phones incident to their arrest, the government needed a warrant before actually searching those cell phones.[12] There, the Court emphasized that cell phones now hold "the privacies of life"[13] to include information such as "an address, a note, a prescription, a bank statement, a video"[14]—many of the same types of content that can be gathered under Section 702. Thus, contrary to the government's assertions,[15] the Constitution does not permit the government free rein to use lawfully collected information for any lawful purpose. Rather, the Fourth Amendment demands a warrant, or at least some kind of individualized judicial approval, before the government searches through Section 702 data seeking the communications of an American, regardless of the lawfulness of the seizure.

Moreover, in the context of Section 702, the need for individualized judicial review prior to the subsequent search is heightened because, unlike the situation in *Riley*, there is no requirement for a probable cause finding or any individualized judicial review at the front end, prior to seizure of the data. This is because, under Section 702, targets must be non-U.S. persons located outside the United States, and therefore they do not have recognized Fourth Amendment rights. Yet U.S. persons do possess Fourth Amendment rights, and the current query rules that require only internal agency approval for U.S. person queries are insufficient to compensate for the lack of individualized judicial review at the front end of Section 702 collection. This is why these queries are often referred to as "backdoor searches."[16]

Further, under the Fourth Amendment's reasonableness test, the constitutionality of the original 702 collection depends upon the totality of the circumstances,[17] and this totality includes

[10] *See Soldal v. Cook Cnty.*, 506 U.S. 56, 63 (1992)*; see also* Brief of Amici Curiae in *Muhtorov, supra,* at 16-19.

[11] *See Riley v. California*, 573 U.S. 373, 403 (2014)*; see also* Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of crimes, supra*.

[12] *Riley v. California*, 573 U.S. at 403.

[13] *Id.*

[14] *Id.* at 394.

[15] *See, e.g., FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Stuart J. Evans, Deputy Assistant Att'y Gen. for Intel., Nat'l Sec. Div., U.S. Dep't of Just.).

[16] *See, e.g., Fixing FISA, Part II: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (2023) (statement of Elizabeth Goitein, Sr. Dir, Liberty & Nat'l Sec. Program, Brennan Ctr. for Just.).

[17] *See Samson v. California*, 547 U.S. 843 (2006).

the strength of post-collection safeguards for collected data. Since there is no individualized judicial review of any Section 702 target, the back end safeguards must be robust in order to protect the constitutional rights of U.S. persons. The absence of any individualized judicial review of U.S. person query terms thus threatens the overall reasonableness of the program under the Fourth Amendment's totality of the circumstances test.

In PCLOB's 2014 Report on Section 702, the Board considered the reasonableness of the Section 702 program under the Fourth Amendment but chose not to render a judgment on its overall constitutionality. The Board assessed that "the core" of the 702 program "fits within the totality of the circumstances test," but that: "[o]utside of [its] fundamental core, certain aspects of the Section 702 program raise questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness. Such aspects include the scope of the incidental collection of U.S. persons' communications… the use of database queries to search the information collected under the program for the communications of specific U.S. persons, and the possible use of communications acquired under the program for criminal assessments, investigations, or proceedings that have no relationship to foreign intelligence."[18]

The greatest threats to Americans' constitutionally protected rights stem from FBI searches through 702 data seeking information about a particular U.S. person. As discussed in our Policy Analysis, given the possibility of criminal investigation and prosecution, FBI's searches of Americans' communications data for evidence of a crime in a foreign intelligence database present particular risks to privacy and civil liberties, even absent any compliance errors.[19] Further, Section 702 involves collection of communications content, which, as discussed, can include extremely private and revealing information. Due to the sensitive nature of communications content, in other contexts, law enforcement is required to obtain a probable cause warrant before accessing the content of communications.[20]

Consequently, I believe that the Board's Recommendation 3 should be strengthened, and Congress should require that FBI's U.S. person queries of 702 data, when conducted at least in part to seek evidence of crime, are subject to judicial review under the higher probable cause

[18] PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, at 96-97 (2014) [hereinafter PCLOB 2014 Report on 702].

[19] Although the Supreme Court has never addressed the question of whether there is a foreign intelligence exception to the warrant requirement, courts have long recognized that electronic surveillance for the pure purpose of foreign intelligence should be treated differently than domestic law enforcement prosecutions. *See, e.g., United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297 (1972); *see also United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974)(en banc); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973).

[20] *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (holding that a warrant is required for government to obtain at least seven days of cell site location information and citing with approval the opinion of the U.S. Court of Appeals for the Sixth Circuit in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), in which the court held that a warrant is required for law enforcement to obtain the content of communications from a service provider).

…Congress should require that FBI's U.S. person queries of 702 data, when conducted at least in part to seek evidence of crime, are subject to judicial review under the higher probable cause standard.

standard.[21] This would ensure that such queries fully comply with the Fourth Amendment and would be consistent with criminal law in other contexts.[22] I agree with the aspects of Recommendation 3 that are designed to reduce the burden on the government and the FISC, including limiting the requirement for FISC review to instances in which the U.S. person query has resulted in a hit in 702 data and government personnel want to access the results of the query. Although running a U.S. person query does create a privacy intrusion regardless of whether there is a hit, the privacy harm is much greater at the point personnel review the results that are returned when there is a hit.[23] I also agree with the exceptions for exigent circumstances and for searches conducted with actual consent. Congress could require a probable cause standard for FBI queries and still retain these aspects of Recommendation 3.

The government's arguments against requiring a probable cause standard for FBI's U.S. person queries under Section 702 are not compelling. First, we know that it has been a routine practice for FBI to run these searches at preliminary stages of an inquiry,[24] and FBI has asserted that it could not meet a probable cause standard for such queries conducted at these early stages. Yet, rather than demonstrating why a probable cause standard would be inappropriate, its argument actually highlights one of the key problems with these queries – FBI is searching through a database of highly sensitive communications seeking information about specific Americans prematurely, often without any articulable reason to suspect that American of wrongdoing. It may not be easy for FBI to meet a probable cause standard even beyond these early stages, but in the strongest examples offered by FBI, such as the "victim" or "defensive" query examples cited in the Policy Analysis, the government would likely be able to meet a probable cause standard or one of the exceptions contemplated in Recommendation 3.

[21] As noted above, a probable cause requirement that applies to all FBI U.S. person queries conducted at least in part seeking evidence of a crime may, as a practical matter, need to apply to all FBI U.S. person queries.

[22] Where FBI conducts queries solely seeking foreign intelligence information, such queries could be subject to the current "reasonably likely" to return foreign intelligence information standard, as outlined in Recommendation 3.

[23] Analytically, this requirement would be similar to the seizure versus search distinction discussed above. For example, in *Riley*, the Supreme Court held that law enforcement needed to obtain a probable cause warrant in order to search the contents of a cell phone seized incident to arrest of the defendant. It was only after law enforcement identified that the defendant had a cell phone and seized it incident to arrest, that the requirement for the search warrant applied to authorize searching the contents of the phone. A requirement for a FISC order in order to access, or search through, the content returned by a U.S. person query, would be similar.

[24] PCLOB 2014 Report on 702, *supra*, at 137.

In addition, the American legal system does not permit law enforcement to avoid compliance with constitutional safeguards simply because it would be more expedient to avoid such requirements. Fourth Amendment doctrine does take into account the practical needs of law enforcement, and the "ultimate touchstone of the Fourth Amendment is reasonableness."[25] Yet such practical considerations justify only narrow exceptions to the requirement of prior individualized judicial review, such as the exigent circumstances exception to the warrant requirement. To take an extreme example, it would be more expedient for police officers to be able to search homes without obtaining search warrants, but, absent specific emergency exceptions, Fourth Amendment doctrine does not permit abandonment of this fundamental safeguard. Similarly, absent exigent circumstances, FBI should be required to obtain a probable cause order from the FISC approving use of U.S. person query terms, despite the burden this would create.

…[T]he American legal system does not permit law enforcement to avoid compliance with constitutional safeguards simply because it would be more expedient…

Even if FBI were not able to obtain FISC approval for all of its U.S. person queries in which there is a hit and which are not covered by the exigent circumstances or actual consent exceptions, it is far from clear that this would cause a critical setback to FBI's investigations. When the Board requested "information regarding any instance in which the government, as part of a criminal investigation or prosecution, relied on evidence that was identified through a U.S. person query," the government responded that it "does not systematically track when or whether particular Section 702 information was identified via a U.S. person query or via another means of review."[26] FBI has provided examples in which the use of U.S. person queries was valuable to identify and warn victims of attacks, but as noted, these cases may fit within the exigent circumstances or consent exceptions we have outlined. Outside of the category of "victim" or "defensive" queries, FBI has been unable to identify any cases in which a Section 702 U.S. person query provided unique value in advancing a criminal investigation. Moreover, FBI was unable to identify a single criminal prosecution that relied on evidence identified through a U.S. person query.[27]

[25] *Riley v. California*, 573 U.S. at 381.

[26] Intel. Cmty., PCLOB questions received December 15, 2022 (Jan. 26, 2023).

[27] As explained above, in any cases in which FBI seeks to conduct queries exclusively to obtain foreign intelligence information, and not also in part to seek evidence of a crime, it should be subject to the same "reasonably likely to retrieve" foreign intelligence information query standard as applies to queries conducted for such purposes by NSA, CIA, and NCTC.

Rather, in a number of examples that FBI provided to the Board in an effort to demonstrate the value of U.S. person queries, the government ultimately did not use evidence from FISA-derived information. As discussed earlier in this report, the government is required to provide notice when it intends to enter into evidence or otherwise use or disclose information derived from Section 702 in a trial, hearing, or other proceeding against an aggrieved person, where the information is relevant to the case in chief. But, in some of the U.S. person query examples that FBI provided to PCLOB, the government explained that it did not need to provide notice because no Section 702 evidence was ultimately used – demonstrating that the queries themselves were not as valuable as purported and that the government did not need to use the Section 702 database in these investigations, but did so out of ease.

Even if Congress does not agree that the Fourth Amendment requires judicial review under a probable cause standard, Congress can and should choose to heighten standards for policy reasons. Congress has long raised concerns over the government's handling and use of U.S. person information under this foreign intelligence program and has repeatedly debated requirements for FISC review for U.S. person queries.[28] As discussed earlier in this report, during the last reauthorization of the Section 702 program, Congress enacted a narrow warrant requirement, which applies to a small percentage of FBI's U.S. person queries.

More specifically, during the 2018 reauthorization of the Section 702 program, Congress created Section 702(f)(2), which requires the government to obtain an order from the FISC before FBI personnel may view the results from certain U.S. person queries. However, the provision requires a warrant only where the query is conducted in connection with a predicated criminal investigation, for the sole purpose of seeking evidence of a crime, and the criminal investigation does not relate to national security. Particularly because there must be a predicated criminal investigation for the provision to apply, it does not require the government to seek such a warrant for the vast majority of U.S. person queries. Most problematic, FBI has never once submitted an application to the FISC pursuant to Section 702(f)(2), despite many documented cases since the provision was enacted in which the warrant requirement actually applied.

Nonetheless, the Section 702(f)(2) standard provides a useful model: Congress could extend the current requirements under Section 702(f)(2)(C) and (D). Section 702(f)(2) would simply need to be updated to reflect its application to access the results of all FBI U.S. person queries conducted at least in part for evidence of a crime.

[28] The House of Representatives has repeatedly and overwhelmingly passed, on a bipartisan basis, a warrant requirement for all Section 702 U.S. person queries. *See* H.Amdt.935 to H.R.4870 Department of Defense Appropriations Act of 2015, 113th Cong. (2014); H.Amdt.503 to H.R. 2685 Department of Defense Appropriations Act of 2016, 114th Cong. (2015).

At a minimum, the Fourth Amendment requires some type of prior individualized judicial approval before the government can run a search.[29] Requiring individualized judicial review of U.S. person queries as outlined in the Board's Recommendation 3 would insert the hallmark safeguard of the American legal system and significantly mitigate the privacy threats posed by U.S. person queries. For this reason, I join Recommendation 3 and urge Congress to require a role for the FISC in reviewing Section 702 U.S. person query terms at least under the standards outlined in that recommendation.

Further, I agree that where the government is searching Section 702 databases solely for foreign intelligence information, a lower standard may be appropriate, and more practicable, as outlined in Recommendation 3. U.S. person queries conducted by NSA, CIA, and NCTC would thereby remain governed by the same "reasonably likely to retrieve" standard as is currently in place. A probable cause standard in the context of seeking foreign intelligence information presents novel challenges, and it is not clear how a probable cause standard could be applied in the absence of a criminal law predicate.

The government asserts that requiring FISC review of U.S. person query terms under any standard of review would cause undue delay in conducting investigations. However, the government should already be ensuring that it is meeting the "reasonably likely to retrieve" foreign intelligence information or evidence of a crime standards when running a query, and providing the relevant justifications and documentation before doing so.[30] Under Recommendation 3, the only change would therefore be the new requirement of external review by the FISC. Certainly, FISC review can be expected to slow down the process of running a query, but this may simply be a necessary cost to fully protecting Americans' privacy rights. Further, our recommendation is crafted to address these timing concerns. In addition to urging Congress to appropriate additional resources for both the government and the court, we recommend creation of an exigent circumstances exception.

Further, only a small percentage of queries will be affected by this recommendation. The vast majority of FBI's U.S. person queries of Section 702 information return no results. For

[29] *See U.S. Dist. Ct. (Keith)*, 407 U.S. at 317, 323-24 (explaining that "[t]he Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised," and that while "prior judicial approval is required," Congress may prescribe "reasonable standards" for courts to follow in particular contexts); s*ee also* Brief of Amici Curiae in *Muhtorov, supra,* at 19-24.

[30] With recent policy changes made by FBI, all government personnel must document that a query will meet the query standard before running a U.S. person query. *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (2023) (statement of Paul Abbate, Dep. Dir, Fed. Bureau of Investigation). Indeed, NSA personnel are required to seek prior approval for U.S. person query terms from the NSA Office of General Counsel. *See, e.g.* NAT'L SEC. AGENCY, EXHIBIT H, QUERYING PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 4 (2023) (requiring that all U.S. person queries be accompanied by a statement of facts showing that the query term is reasonably likely to retrieve foreign intelligence information).

example, the government has stated that in 2022, approximately 1.58% of FBI's U.S. person queries resulted in an FBI user accessing content information returned by the query.[31] That year, FBI had run an estimated 204,090 U.S. person queries. Accordingly, if our Recommendation 3 were in place, the government would have needed to seek FISC approval in about 3,225 cases (or likely less, assuming some were instances where the government had exigent circumstances or where the government could have obtained consent from the U.S. person to use their identifiers).

Finally, I note that the design of the Board's Recommendation 3 would help ensure that the government could still maintain much of the value of U.S. person queries without delays that would obstruct national security. This recommendation has been carefully crafted to address the government's practical concerns and limit the burden that may be caused by a new requirement for FISC approval of U.S. person queries. As discussed in the Policy Analysis section of this report, U.S. person queries do provide some value in helping government analysts efficiently find connections between targets and U.S. persons, especially in ruling out potential leads. Additionally, the government has placed particular emphasis during public debate surrounding the program on the value of these searches in identifying and informing American victims of cyber-attacks. The Board's Recommendation 3 would allow the government to continue using U.S. person queries for both purposes often without any additional hurdles. The government could, under this recommendation, continue to quickly rule out leads in many cases, as the requirement of FISC approval only applies at the point where a search returns a hit and an analyst or agent seeks to review those results. Further, as laid out in our Recommendation 3, the Board urges that Congress create an exception from the requirement for a FISC order for situations in which the government has instead obtained express consent from the relevant U.S. person to use its query terms for searches. Although it will not always be possible for the government to obtain consent from potential victims, such an exception for express consent would be consistent with the Fourth Amendment and should help to minimize the burden on the government.

Ultimately, I urge Congress to require the higher probable cause standard for FISC approval of FBI's U.S. person queries seeking evidence of a crime, but at a minimum, Congress should adopt the Board's Recommendation 3. Congress can and should protect both Americans' security and our privacy. As the Board stated in its 2014 Report on Section 702, "[t]he response if any feature tips the program over the [constitutional] line is not to discard the entire program; instead, it is to address that specific feature."[32] Providing individualized judicial review for U.S. person queries is critically important to ensure that this aspect of the Section 702 program is on a sound constitutional footing and protects Americans' right to privacy in their communications. This reform should be an essential component of reauthorization of the program.

---

[31] OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2022 (2023), https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022_FINAL.pdf.

[32] *Id.* at 97.

ANNEX B: SEPARATE STATEMENT OF BOARD MEMBERS BETH A. WILLIAMS AND RICHARD E. DIZINNO[1]

We have voted against this Report, and the Report therefore should not be attributed to us.[2] Unlike in 2014, the Board does not speak with one voice.

We did not take this vote lightly. Our goal was to produce a unanimous Report with the support of all Board Members. The Board worked diligently for the better part of a year toward that goal. Indeed, we have spent the last twelve-plus months intensely studying the 702 program; wading through thousands of pages of documents; asking questions and receiving comprehensive briefings from the Intelligence Community; holding public sessions; receiving thoughtful input and recommendations from civil society groups and other stakeholders; and attempting to resolve good-faith differences.

Ultimately, the Majority produced the foregoing Report. Unified, the Board's voice unquestionably would have had more impact on the policy debate as decision-makers parse through incredibly dense, complex material, and craft laws impacting not only the privacy and civil liberties of U.S. persons, but also the safety and security of our nation. Unfortunately, the Board's voice is significantly muted by the Majority's decision.

There is no serious disagreement that (1) the Section 702 program is both legal and incredibly valuable to the safety and security of the American people and (2) significant reforms are needed and should be welcomed.

Although we share points of agreement, much of the Majority's analysis and many of its recommendations miss the mark, in ways both large and small. Some of the Majority's recommendations are sound, and could provide helpful additional protections for privacy and civil liberties. Others would cause serious damage to the country and our national security, while negatively impacting the privacy of U.S. persons.

The two key points, about which there is no serious disagreement, are: (1) the Section 702 program is both legal, and incredibly valuable to the safety and security of the American people; [3] and (2) significant reforms are needed and should be welcomed.

[1] We would like to thank our counselors, Laurence E. Rothenberg and Courtney A. Sullivan, for their dedication and immense contributions to this statement.

[2] The reasons for this are manifold, both procedural and substantive, and need not be recounted here. As merely an example, the Majority never acknowledges that this is not a unanimous report.

[3] Every court to have reached a decision on the program has found it to be constitutional and reasonable under the Fourth Amendment.

The Section 702 program is so valuable that not one Member of this Board believes that Congress should allow it to lapse.[4] Failure to reauthorize the program would cause grave damage to the security of our country, and quite likely, lead to the loss of American lives. Reforms, however, are needed to address concerning compliance issues and to prevent potential misuse of the authority for political or other improper purposes.

Failure to reauthorize the program would cause grave damage to the security of our country, and quite likely, lead to the loss of American lives.

Moments of public doubt, like this one, offer the opportunity to re-double efforts to restore trust in our public institutions and accountability in our public servants. Policies that protect the privacy and civil liberties of U.S. persons should be carefully crafted and scrupulously followed. And strong, additional measures should be implemented to ensure that the authorities granted by Congress to the Intelligence Community are never weaponized against political opponents or otherwise exploited for improper purposes.

Accordingly, we submit this Separate Statement to provide our own analysis of the Section 702 program and offer recommendations to address privacy and civil liberties concerns meaningfully, and to do so in a manner that meets the Board's mission to balance privacy and civil liberties with the need to protect our national security.[5]

EXECUTIVE SUMMARY

The Section 702 Program is vital to national security and should be reauthorized, but substantial reform is needed. The American public deserves comfort that protections are in place to prevent misuse of the intelligence authorities that are designed to keep them safe. The FBI, in particular, is at an inflection point. The actions of certain members of the FBI have shaken the public's trust in our Intelligence Community. This is highly regrettable—not only for the public

[4] *See Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them: Hearing Before the Subcomm. on Crime and Fed. Gov't Surveillance of the House. Comm. on the Judiciary*, 118th Cong. (2023) (statement of Sharon Bradford Franklin, Chair, Priv. and C.L. Oversight Bd.) ("[W]e agree that three things are true: Section 702 is valuable in protecting our national security; Section 702 creates risks to privacy and civil liberties; and these risks can and should be addressed without undermining the core value of the program. We are confident that the privacy risks posed by Section 702 can be addressed while preserving the program's value in protecting Americans' national security."). *See also* The Lawfare Podcast, *Travis LeBlanc and FISA Section 702*, THE LAWFARE INST. (Mar. 22, 2023), https://shows.acast.com/lawfare/episodes/travis-leblanc-and-fisa-section-702 ("Section 702 program has significant and immense value. That lives have been saved as a result of this program, and that the country is safer with Section 702 than without it.").

[5] *See* 42 U.S.C. § 2000(ee) ("The Board shall (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.").

and our nation, but for the thousands of men and women at the FBI and at the other agencies who work hard every day to counter our adversaries and protect our country.

Rebuilding public trust takes more than changing a few policies. It requires a thorough change of culture and a better organization. Privacy and civil liberties cannot be an afterthought, a burden, or a bureaucratic trap. Those tasked with protecting us from harm must be equally vigilant to the liberties and values that make us free. As Special Counsel John Durham stated, "Meeting those responsibilities comes down to the integrity of the people who take an oath to follow the guidelines and policies currently in place," and the answer to some of the questions regarding changing the FBI's culture and rebuilding trust "is not the creation of new rules but a renewed fidelity to the old."[6]

Improper querying of lawfully collected data is a significant source of concern. For the FBI in particular, there is no excuse for the failure to follow policies or to appropriately train and oversee its personnel in the use of Section 702 information. Indeed, the culture that produced the improper queries of donors to a political campaign, people arrested during civil unrest following the killing of George Floyd, individuals investigated for their presence at the January 6, 2021 breach of the Capitol, and others, requires immediate attention and external oversight. We are also deeply troubled by issues of unmasking and the leaking of classified information that occurred during the transition after the 2016 presidential election, which could similarly apply to information obtained pursuant to Section 702. Finally, while current FBI leadership has implemented measures to remedy compliance issues, which have resulted in commendable improvement, the current measures alone are not sufficient. Privacy and civil liberties are an essential part of the core American values that our government and its officials are sworn to protect. In more than a year of examining the Section 702 program in depth, and in reviewing the privacy and civil liberties protections across the Intelligence Community, it has become clear to us that the FBI requires meaningful structural reform in order to facilitate a stronger culture of compliance going forward.

There is no excuse for the FBI's failure to follow policies or to appropriately train and oversee its personnel in the use of Section 702 information.

Our recommendations address these and other most salient concerns, with a clear-eyed view of the program as it currently operates—both how the government is succeeding from a privacy and civil liberties perspective, and how it must improve. Our first set of recommendations focuses specifically on the FBI, where the most widespread compliance violations have been reported over the last several years—particularly with regard to querying Section 702 information that has already been lawfully collected. Much of the reform we recommend is cultural and

[6] JOHN H. DURHAM, OFF. OF SPECIAL COUNSEL U.S. DEP'T OF JUST., REPORT ON MATTERS RELATED TO THE INTELLIGENCE ACTIVITIES AND INVESTIGATIONS ARISING OUT OF THE 2016 PRESIDENTIAL CAMPAIGNS, at 18 (May 12, 2023) (hereinafter Durham Report).

structural; some of it is procedural. All of it, however, is aimed at re-establishing public trust in the FBI. We describe additional, substantial reforms that we urge both Congress and the FBI to implement. These include codifying and expanding protections to ensure that all U.S. person queries, not just sensitive queries, are limited and appropriate.

Our second set of recommendations offer protections across the Intelligence Community to guard against the potential weaponization and misuse of the program for political or other improper purpose. While many of the most egregious recent violations concerning the 2016 presidential transition did not involve Section 702, we nevertheless recommend that additional safeguards be enacted to ensure appropriate oversight over the program. Specifically, Congress should have the opportunity to review sensitive queries, including those involving public officials, political candidates, members of the news media, and others involved in protected First Amendment activities, on a regular basis—not only when those queries are reported as compliance incidents. The best branch to safeguard against political misuse is a political branch accountable to the people—not a court with limited resources, appropriately focused only on legal issues, and operating largely out of the public eye. More stringent policies should be adopted for requests to "unmask" U.S. persons. And Congress should enact a new criminal statute with significant penalties for those who leak protected Section 702 information concerning U.S. persons.

Finally, we are deeply concerned that under the current statutory framework of Section 702, the government may already have in its possession—but be legally unable to access—information that foreigners entering the United States, or persons applying for U.S. government security clearances, present threats to national security. In our view, it is unacceptable that such information is lawfully collected, but rendered essentially unusable or severely limited. Vetting is a crucial national security function, and Congress should make clear that Section 702 may be utilized to support it.

The Majority's Report fails to address many of these concerns, focusing instead on a scattershot list of old ideas disconnected from the current moment. The Majority Report fails to differentiate in any meaningful way between areas where the government is largely succeeding in its efforts to protect privacy and civil liberties and areas where it is not. In confounding this distinction, the Report makes it difficult, if not impossible, for policymakers to understand what reforms would make an actual difference for protecting privacy, especially for U.S. persons. For example, with regard to targeting, while the evidence shows that the government has excelled at lawfully collecting information pursuant to Section 702, the Majority Report nevertheless dwells on speculative harms, untethered to operational realities or available evidence, and offers recommendations that, in some cases, would do more to violate rather than protect the privacy of individuals.

The Majority Report also undervalues key aspects of the program, such as by minimizing Section 702's importance in responding to the current threat of terrorist attacks from regions of

the globe where the U.S. military has a reduced footprint, and failing to consider the role of Section 702 in countering the flood of fentanyl trafficked into the United States by foreign actors. It also fails to discuss the value of the program to U.S. allies and U.S. private industry, while significantly undervaluing the operational role of U.S. person queries. Most significantly, it elevates form over function by placing heavy bureaucratic burdens on agency personnel and the FISC without evidence there would be much, if any, privacy and civil liberties improvement. Indeed, some of the recommendations would force additional investigation of U.S. persons, which could pose a negative privacy impact, while significantly damaging the national security value of the program.

We thus recommend stronger changes more focused on the concerns at hand. Every court to have reached a decision on the program has found it to be legal. And every Member of this Board has concluded the program is valuable. We offer the following analysis and recommendations to help ensure that the program accords with the high standards for privacy and civil liberties protection consistent with the nation's values.

I. Brief History of Section 702

More than 20 years have passed since the terrorist attacks on September 11, 2001 that killed almost 3,000 of our fellow citizens. Many Americans remember exactly where they were that day, and the images of the attacks are engrained in our collective memory. Yet more than 20 percent of our population today was not even born when the attacks occurred.[7] A brief reminder of some events of that day as well as the days and months that followed is helpful to contextualize actions the government took in response.

For example, in the immediate aftermath of the attacks, the fear remained that the terrorists were not done with their plans, and that more attacks were imminent. As the U.S. government ramped up its efforts to prevent the next attack, changes in technology impeded the government's ability to find terrorists plotting against our country. By the early 2000s, even foreign individuals living abroad were using U.S.-based electronic communications service providers to communicate with each other. According to the language of the FISA statute at the time, because these non-U.S. persons in other countries were using U.S.-based service providers, the government needed to obtain an order from the FISC, based on probable cause, in order to intercept those foreigners' communications. Intelligence Community personnel and DOJ attorneys had to spend inordinate amounts of time preparing applications for FISC orders to intercept communications of foreign terrorists in foreign countries.

[7] Bill Hutchinson et al., *On 20th Anniversary of 9/11, Questions, Anger and Death Linger*, ABC NEWS (Sept. 11, 2021), http://abcnews.go.com/US/20th-anniversary-911-nears-questions-anger-death-linger/story?id=79606569 ("More than 70 million people living in the United States…had not been yet been born on 9/11. Millions more…were too young to comprehend the destruction and the metamorphosis that followed.").

These requirements created serious "intelligence gaps"[8] and "degraded capabilities in the face of a heightened terrorist threat environment."[9] In July 2008, Congress took action to fix the intelligence gap with a statute that included additional privacy protections and the new Section 702 of FISA. As codified: targets were foreigners located abroad, and therefore the government would not need to obtain individualized orders based on probable cause in order to intercept their communications to acquire foreign intelligence information. Instead, the FISC would review and approve the program itself on an annual basis.

The Section 702 program was re-authorized in 2013 with overwhelming bipartisan support. In 2018, Congress again re-authorized the Section 702 program in a bipartisan vote, and included reforms to strengthen the protection of privacy and civil liberties. The reforms included prohibiting "abouts" collection unless the government obtained FISC authorization and notified Congress; requiring the Intelligence Community agencies to develop querying procedures and submit them to the FISC for review and approval; requiring a court order for FBI to review the results returned by certain U.S. person queries in predicated non-national security investigations; and several other measures to further improve the program's transparency. Since then, the Intelligence Community has instituted additional policy changes to the operation of the program in order to improve its compliance with the rules governing its operation, described below.

II. Legal Status of the Section 702 Program

In 2014, this Board concluded, unanimously and unequivocally, that the core of the Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool. The Board stated:

> [T]he core of the Section 702 program—acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight—fits with the "totality of the circumstances" standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date.[10]

[8] Select Intelligence Committee, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007, S.Rep. 110-209, at 31 (2007) (additional views of Senators Bond, Chambliss, Hatch, and Warner).

[9] *Id.* at 5.

[10] PRIV. AND C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, at 9 (2014) [hereinafter 2014 PCLOB Report]. The Board was concerned about certain aspects of the program—"abouts" collection; the extent of incidental collection of U.S. persons' data; and querying of U.S. persons' communications—and recommended policy solutions to "push the program more comfortably into the sphere of reasonableness, ensuring the program remains tied to its constitutionally legitimate core."

This Board has not conducted an updated legal analysis with this Report.[11] It did not have to. United States courts have repeatedly found the Section 702 program to be legal. Over the course of approximately 15 years, eight different independent federal judges serving on the FISC have found the program reasonable under the Fourth Amendment each year the program was reviewed.[12]

The FISC is not alone. "[I]t is long settled as a matter of American constitutional law that foreign citizens outside U.S. territory do not possess rights under the U.S. Constitution." *Agency for Int'l Dev. v. All. For Open Soc'y Int'l, Inc.*, 140 S. Ct. 2082, 2086 (2020). Indeed, the Supreme Court has ruled that the Fourth Amendment has "no application" to foreign persons outside the United States, but only "to 'the people,'" a constitutional term that "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). In applying *Verdugo-Urquidez* to Section 702 surveillance of foreigners abroad, the Second, Ninth, and Tenth Circuits have all held that the Fourth Amendment does not apply to collection of communications "[w]hen the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States." *United States v. Muhtorov*, 20 F.4th at 28 (10th Cir. 2021).

"[A]ll three United States Circuit Courts of Appeals to consider the issue [the Second, Ninth, and Tenth Circuits] have held that the incidental collection of a U.S. person's communications under Section 702 does not require a warrant and is reasonable under the Fourth Amendment."

FISC, April 21, 2022

Courts are similarly in agreement with regard to the lawfulness of incidental collection of U.S. persons' communications when a foreigner abroad is legally targeted under Section 702. Americans, of course, are entitled to the protections granted in the Fourth Amendment of the U.S. Constitution. As the FISC noted, "all three United States Circuit Courts of Appeals to consider the issue [the Second, Ninth, and Tenth Circuits] have held that the incidental collection of a U.S. person's communications under Section 702 does not require a warrant and is reasonable under

A number of these recommendations (modified in some respects) were later adopted by Congress during the 2018 reauthorization of Section 702.

[11] We also do not conduct our own legal analysis here, but rather describe what United States courts have held.

[12] *See* Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications,* Docket No. 702(j)-23-01 and predecessor dockets, *In re DNI/AG 702(h) Certification 2023-B and its Predecessor Certifications,* Docket No. 702(j)-23-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2023-C and its Predecessor Certifications,* Docket No. 702(j)-23-03 and predecessor dockets (FISA Ct. Apr. 11, 2023) [hereinafter Apr. 11, 2023 FISC Opinion and Order]. *See also* Memorandum Opinion and Order, at 66, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Apr. 21, 2022) (holding that the procedures "protect private U.S. person information from unjustified intrusion and misuse") [hereinafter Apr. 21, 2022 FISC Opinion and Order].

the Fourth Amendment."[13] Analogizing to the Supreme Court's "incidental overhear" and "plain view" doctrines in criminal law, the Ninth Circuit explained "when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted person is also lawful." *United States v. Mohamud*, 843 F.3d 420 at 440-41 (9th Cir. 2016) (quoting *United States v. Hasbajrami*, No. 11-cr-623 (JG), 2016 WL 1029500, at *9 (E.D.N.Y. Mar. 8, 2016)).

The incidental collection of U.S. persons' communications has also repeatedly been found to be "reasonable in its scope and manner of execution." *Maryland v. King*, 569 U.S. at 448. Courts have concluded that the privacy interest at issue is "outweighed by the government's manifest need to monitor the communications of foreign agents of terrorist organizations operating abroad"—a need that "makes the incidental collection of communications between such foreigners and United States persons reasonable." *Muhtorov*, 20 F.4th at 48 (quoting *United States v. Hasbajrami*, 945 F.3d, 641, 666 (2d Cir 2019)). The Second Circuit explained that the communications of U.S. persons with foreign targets heightens the argument for reasonableness:

> Even in the context of conventional warfare, identifying domestic agents of foreign powers is a principal concern of intelligence-gathering. The need to identify potential domestic co-conspirators of hostile foreign persons or groups is even greater in the context of informal non-state terrorist organizations and movements. The recruitment of persons inside the United States or the placement of agents here to carry out terrorist attacks is one of the very threats that make it vital to surveil terrorist actors abroad. *The communications of terrorist operatives abroad with persons inside the United States is thus of particular importance, and at least as important as monitoring the communications of foreign terrorists abroad among themselves*. . . . And when the conversations being monitored constitutes evidence of criminal conspiracies between the foreign operative and someone located within the United States, the urgency becomes greater, not less.

Hasbajrami, 945 F3d. at 666-67 (emphasis added).

At least two courts have also considered and found lawful the government's ability to *query* a database containing 702-derived information using U.S. person identifiers. The district court in *Mohamud* concluded that the "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment." *United States v. Mohamud*, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420 (9th Cir. 2016).[14] The FISC reached the same conclusion in

[13] *Id*. at 59.

[14] *See also U.S. v. AWS Mohammed Younis Al-Jayab*, No. 1:16-cr-00181, at 55-56 (N.D. Ill. June 28, 2018) ("The government must review information collected pursuant to § 702, including concerning U.S. persons or those located in

2018, and re-affirmed that holding in 2022.[15] The court rejected the position of *amici* that queries were distinct Fourth Amendment events, finding that the cited opinions of other courts interpreting the Fourth Amendment in other contexts "were not 'instructive' regarding "the government's examination of information lawfully acquired under a statutory framework that requires a judicial determination that the totality of attendant circumstances, including the government acquisition, retention, use, and dissemination of such information, is reasonable under the Fourth Amendment."[16] The FISC concluded, "This Court respectfully adheres to the view that those objectives [of protecting U.S. persons' privacy] are properly served…by examining the reasonableness of such procedures as a whole."[17]

In reviewing the program as a whole, the FISC does consider the government's querying procedures and its compliance with those procedures. The FISC has stated that continued large-scale failures to comply with the procedures, particularly by the FBI, would indeed raise legal concerns. In 2022 the court explained:

> [I]f the scope and pervasiveness of FBI querying violations were to continue unabated, they would present greater statutory and Fourth Amendment difficulties in the future. There is a point at which it would be untenable to base findings of sufficiency on long promised, but still unrealized, improvements in how the FBI queries Section 702 information.[18]

The FISC, however, was "encouraged by the amendments to the FBI's querying procedures and the substantial efforts to improve FBI querying practices, including heightened documentation requirements, several systems changes, and enhanced guidance, training, and oversight

---

the United States, to determine whether to retain or disseminate it under its minimization procedures. The additional intrusion upon an individual's privacy in searching that information using a U.S. person identifier is not significant and, in light of the minimization procedures already in place, does not render § 702 unreasonable.").

[15] Apr. 21, 2022 FISC Opinion and Order, *supra*, at 66 (quoting Memorandum Opinion and Order, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Oct. 18, 2018) [hereinafter 2018 Cert. FISC Opinion and Order].

[16] *Id.*

[17] *Id.* The Second Circuit in *Hasbajrami* did not hold otherwise. The court reasoned that "querying [] stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable." However, the court did not find querying using U.S. person identifiers to be unreasonable. Instead, it explicitly left that question open, noting that it "did not purport to answer" … "what kinds of querying, subject to what limitations, under what procedures, are reasonable within the meaning of the Fourth Amendment . . . ." And it suggested that the FBI querying its own database, which is far smaller and more targeted, might indeed be reasonable, where "such a review of the agency's own files is arguably analogous to traditional law enforcement techniques." *Hasbajrami*, 954 F3d. at 672.

[18] Apr. 21, 2022 FISC Opinion and Order, *supra* note 12, at 67. *See also* Apr. 11, 2023 FISC Opinion and Order, *supra* note 12, at 93 ("Given recent indications that the FBI is improving its implementation of Section 702 querying requirements, the Court finds that the FBI's querying and minimization procedures, taken as a whole and as likely to be implemented, are consistent with the requirements of the statute and the Fourth Amendment.").

measures,"[19] noting "[t]here are preliminary indications that some of these measures are having the desired effect."[20]

In 2023, the FISC found that the FBI had further improved its querying compliance noting that reported violations "do not approach the scale of a number of prior ones," and concluding "[o]n balance…FBI application of the querying standard appears to have improved."[21] The court noted that in its review of fourteen field offices, the NSD found that the FBI's querying error rate for Section 702 information was approximately 1.7 percent.[22]

Many of our policy recommendations below are aimed at addressing querying problems going forward.

III. Policy Analysis

The Majority reaches two conclusions with which we agree unequivocally: 1) the Section 702 program is highly valuable—indeed, the United States is safer with the Section 702 program than without it; and 2) reforms are needed. Thus, we are unanimous as a Board that the program should be reauthorized, with certain key reforms to improve protections for privacy and civil liberties.

We disagree significantly as to how we evaluate the impact on privacy and civil liberties; which reforms are necessary; and how those reforms will more effectively protect privacy and civil liberties interests and restore public trust in both the 702 program and the Intelligence Community more broadly.

Improper querying of lawfully collected data—particularly by the FBI—is a source of serious concern. There is no excuse for the Bureau's failure to follow its own policies or to appropriately train and oversee its personnel in the use of Section 702 information. Indeed, the culture that produced the improper queries of donors to a political campaign, people arrested during civil unrest tied to protests following the killing of George Floyd, and people investigated for their presence at the January 6, 2021 breach of the Capitol, and others, requires immediate attention and external oversight. Moreover, the FBI has failed in the past to prioritize a culture of compliance across the FBI—in leadership, tone, attention, and resources—with regard to accessing lawfully collected 702 information. We address these issues at length below.

[19] Apr. 21, 2022 FISC Opinion and Order, *supra* note 12, at 49.

[20] *Id.*

[21] Apr. 11, 2023 FISC Opinion and Order, *supra* note 12, 88-87.

[22] *Id.* at 84.

In addition to providing greater safeguards for U.S. person queries, we believe that additional reforms should be considered to guard against the risk of misuse of the authority for political, or other improper purposes. We also believe that the program could be better utilized to ensure that non-U.S. persons who want to live or work in our country, and U.S. persons with access to our most sensitive classified materials are able to be appropriately vetted.

The evidence clearly shows that what has most worried Americans for decades about government surveillance programs—the improper collection of U.S. person data—is *not* occurring under the Section 702 program.

The Majority's analysis, by contrast, fails to differentiate in any meaningful way between areas where the U.S. government is largely succeeding in its efforts to protect privacy and civil liberties, and areas where it is not. In confounding this distinction, the Report makes it difficult, if not impossible, for policymakers to understand what reforms would make an actual difference for protecting privacy, especially for U.S. persons.

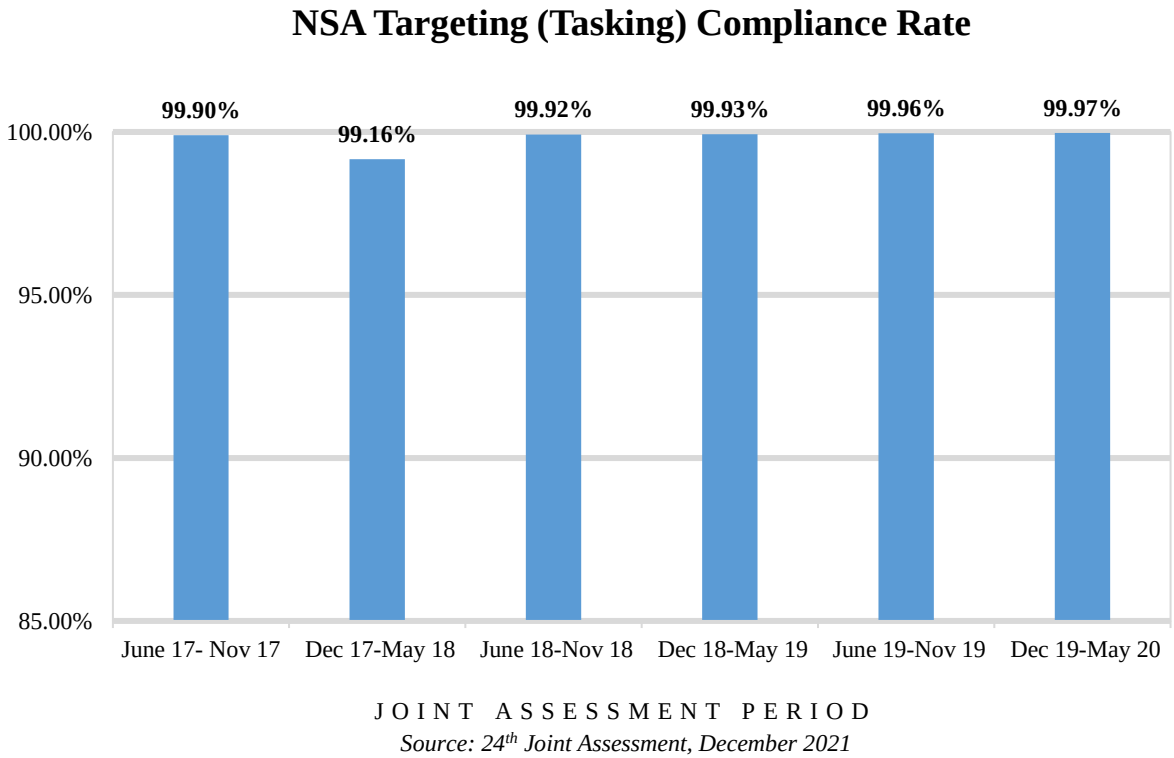
The evidence clearly shows that what has most worried Americans for decades about government surveillance programs—the improper collection of U.S. person data—is ***not*** occurring under the Section 702 program. Thanks largely in part to stricter requirements from Congress, the attention of the privacy advocacy community, and the dedication of innumerable compliance officers and other watchdogs, the targeting compliance error rate is incredibly low. Indeed, from the summer of 2019 through the fall of 2021, the NSA had a 99.85 percent targeting compliance rate or better, according to the most recent unclassified statistics provided to PCLOB.[23] Likewise, the FBI had a 99.99 percent targeting compliance rate during the winter of 2019 through the spring of 2020, again according to the most recent unclassified statistics.[24] This means, among other things, that overwhelmingly, the Intelligence Community is not inadvertently, or mistakenly, targeting Americans. It is not "reverse-targeting" Americans (i.e. targeting a foreigner in order to collect communications with

From the summer of 2019 through the fall of 2021, the NSA had a 99.85 percent targeting compliance rate or better, according to the most recent unclassified statistics provided to PCLOB. Likewise, the FBI had a 99.99 percent targeting compliance rate during the winter of 2019 through the spring of 2020, again according to the most recent unclassified statistics.

[23] U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 1 JUNE 2021-30 NOVEMBER 2021, Fig. 7 at 20 (March 2023) [hereinafter 27th Joint Assessment].

[24] U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 DECEMBER 2019 – 31 MAY 2020, at 42 (Dec. 2021) [hereinafter 24th Joint Assessment].

an American). And it is not targeting non-U.S. persons without a valid foreign intelligence purpose.[25]



Source: 24th Joint Assessment, December 2021

Measures taken to prevent unnecessary incidental collection of U.S. person communications have also greatly improved. In 2014, the Board spent many pages of its report on the privacy and civil liberties impacts of "abouts" collection—communications that are neither to nor from an email address—but that instead merely include a reference to that selector. The Board called "abouts" collection "[o]ne of the most controversial aspects of the Section 702 program," explaining that such collection "may be more likely than other forms of collection to acquire wholly domestic communications."[26] In 2018, Congress codified NSA's 2017 decision to end "abouts" collection, and thanks to improvements, the NSA is now proceeding with a much higher degree of accuracy that it is only collecting "to/from" an authorized foreign target overseas.

[25] These conclusions are consistent with those made by the full Board in our 2014 Report. *See* PCLOB 2014 Report, *supra* note 10, at 103 ("The Board has been impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program. Available figures suggest, consistent with the Board's own assessment, that the primary focus of the Section 702 program remains monitoring non-U.S. persons located overseas for valid foreign intelligence purposes.").

[26] PCLOB 2014 Report, *supra* note 10, at 119-120.

Notwithstanding the concerns we address herein, there can be little question that the Section 702 program is both more valuable and more privacy-protective than at any time in its history.[27]

Privacy and Civil Liberties Implications of Section 702[28]

The actions of certain members of the FBI have shaken the public's trust in our Intelligence Community. This is highly regrettable—not only for the public and our nation, but for the thousands of men and women at the Bureau and at the other agencies who work hard every day to counter our adversaries and protect our country.

The FBI is at an inflection point. Rebuilding public trust takes more than changing a few policies. It requires a thorough change of culture, and a better organization—not dissimilar from the changes made by NSA in the wake of the leaks by Edward Snowden. Privacy and civil liberties cannot be an afterthought or a burden. Those tasked with protecting us from harm must be equally vigilant to the liberties and values that make us free. As Special Counsel John Durham stated in his report, "meeting those responsibilities comes down to the integrity of the people who take an oath to follow the guidelines and policies currently in place"; and the "answer" to some of the questions regarding changing the FBI's culture and rebuilding public trust "is not the creation of new rules but a renewed fidelity to the old."[29]

Effective government surveillance for counterterrorism and foreign intelligence purposes is impossible without some impact on privacy and civil liberties. The question for Congress and other policymakers is how maximally to protect privacy and civil liberties, especially of U.S. persons, while maintaining the value of a program that keeps those same people safe.

The Majority Report and its recommendations are largely off-base in this regard. By elevating form over function, they suggest layers of process without meaningful change. Indeed, some of their recommendations would add little, if any benefit, while significantly damaging both the security and privacy of U.S. persons.

As discussed above, and as is evident from the statistics in Part III of the Majority Report, the government is not improperly *collecting* the communications of U.S. persons. The compliance

[27] As the Majority concedes, it is also more privacy-protective than other intelligence collection methods, such as those pursuant to EO 12333 and National Security Letters. Majority Report at Part IV § II(A).

[28] We lack the time to address all of the privacy and civil liberties implications of the program, or to address each of the ways in which the Majority's analysis errs. Nevertheless, we have endeavored here to respond to some of the most salient issues.

[29] Durham Report, *supra* note 6, at 18.

error rate with regard to collection has consistently been below 1 percent.[30] But Congress and the Intelligence Community must ensure that the information of U.S. persons that is lawfully collected is not subsequently misused, particularly through U.S. person queries.

A. U.S. Person Queries

A U.S. person query is one conducted using a term that "is reasonably likely to identify one or more specific United States persons."[31] As discussed in the Majority Report, the foreign intelligence agencies with the ability to query Section 702 holdings—NSA, CIA, and NCTC—have not conducted an inordinate number of U.S. person queries given their missions.[32]

The FBI's mission, however, is different. Because the FBI is tasked with domestic operations—for both intelligence and law enforcement purposes—it is expected to conduct more U.S. person queries; and it has. According to its self-disclosed figures, the FBI used 852,894 U.S. person query terms in 2020, and 2,964,643 in 2021.[33] After its recent policy change to make the default query "opt out" of Section 702 information, rather than "opt in," the number of U.S. person query terms used decreased 94 percent to 119,383.[34]

The FBI is routed information collected by the NSA only from targets who are relevant to predicated national security investigations—which in 2022 was approximately 3.2 percent of the total number of Section 702 targets, or about 8,000 of them.

Several caveats are important to consider with regard to these numbers. First, the numbers refer not to

[30] *See* notes 22 and 23, *supra*.

[31] FED. BUREAU OF INVESTIGATION, EXHIBIT I, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 FBI Querying Procedures]; NAT'L SEC. AGENCY, EXHIBIT H, QUERYING PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 NSA Querying Procedures]; CENT. INTEL. AGENCY, EXHIBIT J, QUERYING PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 CIA Querying Procedures]; NAT'L COUNTERTERRORISM CTR., QUERYING PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2021) [hereinafter 2021 NCTC Querying Procedures]. *See* Majority Report Part III § V(A)-(H).

[32] NSA, CIA, and NCTC have performed a relatively low, and recently decreasing, number of U.S. person queries each year. In total, they used about 4,700 U.S. person query terms in 2022, a drop from about 8,400 in 2021, and 7,200 in 2020. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2022, (2023), at 20, 21 [hereinafter CY2022 ASTR].

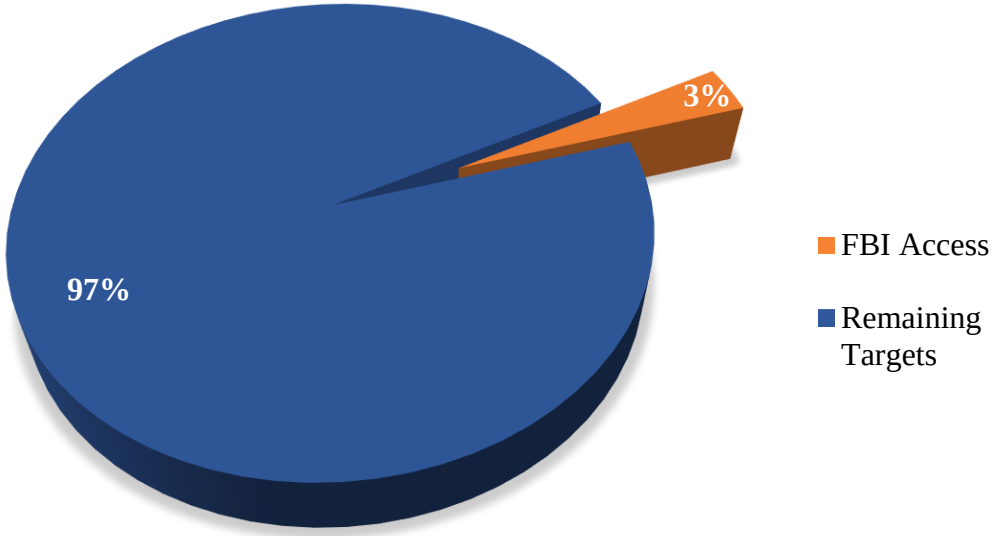
[33] *Id*. at 24.

[34] *Id*. at 23-24.

actual persons, but to "query terms or identifiers." For example, an individual may use multiple selectors to communicate with a foreign target (i.e. email, phone, etc.); a single selector may be queried multiple times; or the U.S. person associated with the query term may be a company or association, not a specific American citizen. Indeed, in many cases involving cyber threats, the "U.S. person query term" is an inanimate object, such as critical infrastructure physically located in the United States whose identifier is queried as part of an investigation. The numbers of "U.S. person queries," therefore, are almost certainly greater than the number of actual U.S. natural persons whose identifiers have been searched.

Second, the FBI has access only to a small fraction of the collection of Section 702-acquired information. The FBI is routed information collected by the NSA only from targets who are relevant to predicated national security investigations—which in 2022 was approximately 3.2 percent of the total number of Section 702 targets, or about 8,000 of them. That is to say, the FBI's U.S. person queries run through data of the communications collected from 8,000 foreigners whom the FBI was investigating for acts of terrorism, spying on behalf of foreign adversaries, cyberattacks on U.S. victims, or other similar acts. The FBI does not run queries against the communications of every U.S. person who communicated with a foreign target.

FBI Access to Collection as a Percentage of Total Targets



Source: Office of the Director of National Intelligence, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, April 2023, p. 22.

Third, because FBI queries are run against this much-narrowed database, the vast majority of FBI's U.S. person queries return no hits, and over 98 percent of FBI U.S. person queries do not return content that is reviewed by an FBI user.[35] That is, no U.S. person communications are ever retrieved as a result of almost all of those queries.

Finally, the FBI has reported that 1.9 million of the query terms used in 2021 were for a single cyber investigation and were conducted primarily for the purpose of identifying victims of a foreign-government sponsored hack of critical infrastructure.

Nevertheless, and even with these caveats, the number of U.S. person queries conducted by the FBI over the past several years appears inordinately high. However, as discussed above, the change in design of FBI's query tool, which ran queries through numerous databases at once by default, seems to have greatly reduced the sheer number of queries being run through Section 702-acquired information.

A more pressing issue, however, is not merely how many U.S. person queries were run, but how many were run improperly.[36] With regard to U.S. person queries, three categories of potential misuse are among the most problematic: 1) that U.S. person information will be accessed for improper purposes, such as for political or personal misuse; 2) that U.S. person information will be used for non-national security law enforcement purposes, without the appropriate safeguards for criminal defendants; and 3) that U.S. person information will be used to surveil or suppress lawful First Amendment activity.

[35] FBI does not track whether a particular query results in a hit; however, FBI calculated that, in 2022, approximately 1.58 percent of U.S. person queries resulted in a user accessing content. There may be some queries that return content that an FBI user does not access, but overall, that statistic indicates that the vast majority of queries never find any content in the databases that contain Section 702-acquired data.

[36] There are different measures of FBI querying compliance error rates, with large variations. For example, for one six-month reporting period in 2019, the querying compliance error rate was as high as 36.59 percent, although that was due to several large, improper batch queries. *See* 24th Joint Assessment, *supra* note 24, at 43. The FBI's Office of Internal Audit found a querying error rate of 4 percent, based on a sample of selected queries performed between July 2021 and March 2022. Office of Internal Auditing, FISA Query Audit, slide 5 (May 10, 2023). More recently, the FBI's querying error rate has been relatively low over last several reporting periods covering June 2020-November 2021: 2.23 percent; 0.36 percent; and 3.22 percent. *See*, 27th Joint Assessment, *supra* note 23 at 2, Fig.1B.

1. *Improper Queries*

A proper query is one that is "reasonably likely to retrieve foreign intelligence information…or evidence of a crime."[37] The NSA, CIA, and NCTC may only query for foreign intelligence information, but the FBI may query for either purpose.

As discussed in the Majority Report, the FISC determined in 2018 that the FBI had been using a different standard, as a result of a disagreement between the FBI and the Justice Department's National Security Division (NSD), and had therefore been running U.S. person queries that were not in fact reasonably likely to retrieve foreign intelligence information or evidence of a crime.[38] The FBI took steps to rectify this misunderstanding, but the disagreement and compliance incidents continued.[39] Auditors from ODNI and NSD would determine, in some situations, that FBI personnel did not have sufficient factual basis to justify the query, even though the FBI personnel believed at the time they did and FBI management defended many of the queries.[40] An analyst in one field office, for example, routinely queried the names of victims and witnesses of crimes, even though there was not a basis to believe there would be any relevant information in the Section 702 databases.[41]

Although there have been a handful of examples where queries were run with improper intent—such as one incident in 2022 in which an NSA analyst conducted queries on two occasions seeking information about two individuals that the analyst had met through an online dating service—the vast majority of improper queries did not involve intentional misuse. Instead, improper queries have often been the result of poor training, and/or a misunderstanding of the query standard.

Nevertheless, queries of Section 702 information run with improper purpose—especially for political or personal benefit—pose one of the most significant privacy and civil liberties risks of the program. The NSA and the FBI have attempted to address this risk by putting in place new

[37] 2021 FBI Querying Procedures, *supra* note 31, at 3-4; FED. BUREAU OF INVESTIGATION, EXHIBIT D, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 15-16 (2021) [hereinafter 2021 FBI Minimization Procedures].

[38] Memorandum Opinion and Order, at 76, [*Caption Redacted*], [Docket No. Redacted] (FISA Ct. Oct. 18, 2018) [hereinafter 2018 Cert FISC Opinion and Order].

[39] *See* Order in Response to Querying Violations, *In re DNI/AG 702(h) Certifications 2020-A, 2020-B, 2020-C, and Predecessor Certifications*, Docket Nos. 702(j)-20-01, 702(j)-20-02, 702(j)-20-03, and predecessor dockets, *In re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under FISA*, Docket No. 08-1833, *In re FBI Standard Minimization Procedures for Tangible Things Obtained Pursuant to Title V of FISA*, Docket No. BR 13-49 (FISA Ct. Sept. 2, 2021).

[40] *Id.* at 6.

[41] *Id.* at 6 n. 4, 8 n. 6-7.

restrictions and oversight of sensitive queries, such as those involving elected officials and journalists. Under the new FBI policy, issued in March 2022, FBI's Deputy Director needs to personally approve certain queries before they can be conducted. However, FBI and NSA policies differ in how they categorize queries considered sensitive and the levels of internal approvals required for each, which could potentially result in these agencies approving and conducting sensitive queries inconsistently. They also currently do not cover individuals participating in several important types of protected First Amendment activity.

The government's capabilities to surveil for foreign intelligence should never be misused against political opponents, and strong oversight must be in place to prevent those who would seek to coopt our country's capabilities for their own use.

While the new sensitive query policies are a step in the right direction, in our view, it is insufficient in this circumstance to allow the Executive Branch to oversee itself. The government's capabilities to surveil for foreign intelligence should never be misused against political opponents, and strong oversight must be in place to prevent those who would seek to coopt our country's capabilities for their own use. Indeed, for this reason, we think the FISC—a court that operates out of the public eye, with legal, not political, oversight as its mission—is not the appropriate body to review these especially sensitive queries. Instead, as detailed more fully below, we suggest that Congress receive regular reports on the sensitive queries that have been run, so that it will promptly be made aware of any potential misuses of the intelligence authority.

2. *Queries for Non-National Security Law Enforcement Purposes*

A second major risk of running U.S. person queries in Section 702-collected information is the chance that U.S. person information will be used for non-national security law enforcement purposes, without the appropriate safeguards for criminal defendants. Congress, of course, explicitly provides in the statute that the FBI *may* query Section 702 information for evidence of a non-national security crime, but it must receive an order from the FISC before viewing the results of such queries in a predicated criminal investigation.[42] The concern is that the government could routinely run such "evidence of crime" queries in non-national security matters, and thus turn a foreign intelligence authority into a domestic criminal investigative tool.

Currently, the FBI does not document every "evidence of a crime" query it runs; it is only required to report these queries when personnel seek to view the results returned from such a U.S. person query. Thus, it is possible that the FBI is performing large numbers of these queries but returning no results. It is also possible that the FBI is under-reporting such queries given that it is running most queries at the pre-assessment or assessment stage, and they are therefore never

[42] 50 U.S.C. § 1881a(f)(2).

triggering the FISC-ordered reporting requirement that applies only at the criminal predicated investigation stage.

Despite these possibilities, the evidence currently available to the Board does not support a conclusion that the FBI is mis-using or over-using Section 702 for domestic law enforcement purposes. The Board has not received information of any case in which the FBI improperly used Section 702-derived information for a criminal prosecution. Indeed, the government has provided notice of its intention to enter into evidence or otherwise use or disclose information derived from Section 702, pursuant to its obligations under Section 106(c) of FISA, in just nine criminal prosecutions—all of which were prosecutions for national security crimes. It would be inappropriate to jump to a presumption of misuse where the evidence does not support it.

Nevertheless, we share the Majority's concern that the FBI has never submitted an application to the FISA Court pursuant to Section 702(f)(2), despite at least six times over the last two years when it was warranted.[43] We also believe that the FBI should improve its tracking of the total number of "evidence of a crime" queries, in order for improved oversight and transparency about how the information is used.

3. *Queries Associated with Protected First Amendment Activity*

Finally, querying Section 702-acquired information with U.S. person terms presents the risk that the government will use the authority to surveil or suppress First Amendment activity. One of the most concerning revelations from the recently declassified FISC opinions was the identification of a significant number of noncompliant queries related to instances of civil unrest and protests, including related to the events of January 6, 2021 and in connection with the protests following the killing of George Floyd.[44] As described in Part III of this report, many of these queries were run without sufficient cause to believe the individual query terms would retrieve Section 702-acquired information.

Because the contents of Section 702-acquired information would only include communications with foreign targets overseas, it is unlikely that many, if any, of these queries actually returned information, or played a role in the subsequent prosecutions of crimes associated with these events.[45] As the unanimous Board explained in 2014:

[43] CY2023 ASTR, *supra* note 32, at 26.

[44] Apr. 21, 2022 FISC Opinion and Order, *supra* note 12, at 28.

[45] *See, e.g.*, *id.* at 29 (regarding three batch queries of 23,132 terms used by a group "involved in the January 6 Capitol breach," "No raw Section 702 information was accessed as a result of these queries.") Some queries of individuals thought to be involved in the Capitol breach did retrieve results, but "the retrieved information was not used for any analytical, investigative, or evidentiary purpose." *Id.* at 33-34.

> Because it disallows *comprehensive* monitoring of any U.S. person, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the United States, the [Section 702] program would serve as a relatively poor vehicle to repress domestic dissent, monitor American political activists, or engage in other politically motivated abuses of the sort that came to light in the 1970s and prompted the enactment of FISA.[46] (emphasis in the original).

Nonetheless, it is concerning that these queries lacking a proper justification were run at all. It is clear that for the FBI, the policies and training that had been in place were plainly insufficient. We address this below in our recommendations.

B. Unmasking of U.S. Persons

The FISC-approved Minimization Procedures for each agency contain rules to protect the privacy of U.S. persons by limiting dissemination of information collected under Section 702 authority. As discussed in the Majority Report, data concerning a non-consenting U.S. person that is identified as foreign intelligence information or, in certain cases, evidence of a crime, may be disseminated outside of the agency only for certain purposes. Unless the identity of a U.S. person is itself foreign intelligence information or is necessary to understand foreign intelligence information,[47] the identities of U.S. persons in intelligence reports are "masked" by using a generic phrase such as "U.S. person 1." For NSA reports, a recipient may request that the U.S. person's identity is unmasked if he or she has a "need to know" and the disseminating U.S. person's identity would be consistent with NSA's minimization procedures. As discussed in Part III of the Majority Report, the agencies' policies on masking, unmasking, and dissemination vary.

During the transition period following the 2016 presidential election campaign, public concerns about unmasking of U.S. person identities in intelligence reports were ignited by accusations that officials in the outgoing administration had improperly requested unmasking of the identities of members of the incoming administration. These concerns centered on the alleged improper use of government intelligence authorities against domestic political rivals. A subsequent investigation—declassified and made available to the public in 2022—conducted by then U.S. Attorney for the Eastern District of Texas, John Bash, ("Bash Report") found that career employees had requested the unmasking for reasons related to their duties to provide information to national security leadership, and that the requests were not inappropriate. Nevertheless, U.S. Attorney Bash expressed that he was "troubled by how easy it is for political appointees of the incumbent administration to obtain nonpublic information about individuals associated with a

[46] PCLOB 2014 Report, *supra* note 10, at 114.

[47] Such disseminations are also permissible if they contain evidence of a crime and are being disseminated for law enforcement purposes.

presidential campaign or transition team."[48] He noted that "[t]here exists a significant potential for misuse of such information—misuse that could be difficult to detect."[49]

It is crucial, therefore, to restore trust among the public that unmasking will not be used to intrude upon the privacy or damage the reputation of U.S. persons for political purposes. Unmasking of Members of Congress and their staff has been limited since 1992.[50] In reaction to the public concerns in 2016, the Director of National Intelligence instituted similar limits on the unmasking of members of Presidential transition teams.[51] The Bash Report recommended that the Intelligence Community consider limiting the unmasking of Presidential campaign associates, in addition to members of Presidential transition teams.[52] It further recommended that all requests to unmask political figures be subject to centralized approval and tracking, and that those requests require a higher level of "substantial need" for the unmasked U.S. person identity.[53]

It is crucial to restore trust among the public that unmasking will not be used to intrude upon the privacy or damage the reputation of U.S. persons for political purposes.

We agree with U.S. Attorney Bash's recommendations, and, as described in more detail in the final section, recommend that they be strengthened and implemented.

C. Unauthorized Leaks of Section 702 Information

Those with access to sensitive national security information—including information collected pursuant to Section 702—have the highest responsibility to guard and protect that information.[54] Unauthorized leaks for improper purpose, such as for personal or political ends,

[48] United States Attorney John F. Bash, REQUESTS FOR U.S. PERSON IDENTITIES IN INTELLIGENCE REPORTS DURING THE 2016 PRESIDENTIAL ELECTION PERIOD AND THE ENSUING PRESIDENTIAL-TRANSITION PERIOD: REPORT FOR THE ATTORNEY GENERAL, at 3 (2020) [hereinafter Bash Report].

[49] *Id.*

[50] These are known as the Gates Procedures, named after CIA Director Robert Gates who originally issued them. *See* OFF. OF THE DIR. OF NAT'L INTEL. INTELLIGENCE COMMUNITY DIRECTIVE 112, ANNEX A, DISSEMINATION OF CONGRESSIONAL IDENTITY INFORMATION (2017).

[51] *See* OFF. OF THE DIR. OF NAT'L INTEL. INTELLIGENCE COMMUNITY POLICY GUIDANCE 107.1, REQUESTS FOR IDENTITIES OF U.S. PERSONS IN DISSEMINATED INTELLIGENCE REPORTS (2018).

[52] Bash Report, *supra* note 48, at 48.

[53] *Id.* at 49.

[54] As discussed in Part III of the Majority Report, Section 702 requires that agencies adopt minimization procedures to reduce the privacy and civil liberties impact of the acquisition, retention, and dissemination of incidentally collected U.S. person information. Among other things, the procedures require that non-publicly available information that is not foreign intelligence information shall not be disseminated in a manner that identifies any U.S. person without that person's consent, unless the identity is necessary to understand such foreign intelligence information or assess its importance. 50 U.S.C. § 1821(4)(B).

are reprehensible. These leaks have the potential to harm not only the subject of the disclosure, but to erode public trust in our institutions and officers.

It was beyond the purview of U.S. Attorney Bash's Report to address the leak concerning General Michael Flynn's contacts with the Russian Ambassador to the United States.[55] We do not know whether the information regarding General Flynn that was disclosed was derived from Section 702; indeed, we suspect it was not. Nevertheless, we find the leak to the media that occurred—and the lack of accountability for it—deeply concerning.[56]

The American public should have comfort that the incidental collection of any communications that might occur pursuant to Section 702 will not be misused, and that any misuse will be met with legal consequence.

The American public should have comfort that the incidental collection of any communications that might occur pursuant to Section 702 will not be misused, and that any misuse will be met with legal consequence. We therefore recommend below that Congress enhance protections for the privacy and civil liberties of U.S. persons by specifically criminalizing leaks of Section 702-acquired information, and prescribing appropriate penalties for those who would misuse this sensitive information.

D. Structure and Culture at the FBI

As has been discussed at length, the present compliance concerns with regard to Section 702 rest largely with the FBI. Current FBI leadership has taken notable steps to remedy many of these specific problems, as recognized by the FISC in its most recent order approving the annual Section 702 certifications.[57] Indeed, there is no question that the FBI's operational system changes—and subsequent reduction of U.S. person queries by 94 percent—have been significant.[58]

Nevertheless, we agree with both former Assistant Attorney General David Kris and Special Counsel John Durham, who, in their examinations of other FBI matters, independently concluded that policy changes alone are insufficient. In his 2020 letter brief to the FISC as *amicus curiae* concerning the factual accuracy in FBI Title I FISA applications, Mr. Kris wrote:

[55] U.S. Attorney Bash stated that determining "how that information was provided to the media[ ] was beyond the scope of [his] review." Bash Report, *supra* note 48, at 2.

[56] There has been no prosecution for the leak that led to General Flynn's resignation.

[57] *See* Apr. 11, 2023 FISC Opinion and Order, *supra* note 12, at 93 ("Given recent indications that the FBI is improving its implementation of Section 702 querying requirements, the Court finds that the FBI's querying and minimization procedures, taken as a whole and as likely to be implemented, are consistent with the statute and the requirements of the Fourth Amendment.").

[58] CY2022 ASTR, *supra* note 32, at 24.

> Standards and procedures, checklists and questionnaires, automated workflows, training modules, and after-the fact audits are all important. But they cannot be allowed to substitute for a strong FBI culture of individual ownership and responsibility for the accuracy and completeness of FISA applications. Without that, even the best procedures will not suffice; indeed, expanded procedures dictating multiple layers of review and approval could backfire, creating a kind of moral hazard, in which each layer believes, or assumes, that errors have or will be caught by others. Organizational culture is paramount to real reform . . . A culture of operational personnel who feel checked and second-guessed by distant compliance officers is far less effective than a culture in which operators themselves are made to feel like compliance officers, with direct responsibility and accountability for following the rules.[59]

Similarly, in his more recent report on Matters Related to the Intelligence Activities and Investigations Arising Out of the 2016 Presidential Campaigns, Special Counsel Durham concluded:

> The promulgation of additional rules and regulations to be learned in yet more training sessions would likely prove to be a fruitless exercise if the FBI's guiding principles of "Fidelity, Bravery and Integrity" are not engrained in the hearts and minds of those sworn to meet the FBI's mission of "Protect[ing] the American People and Uphold[ing] the Constitution of the United States.[60]

We concur that cultural reform across the organization must be a bedrock priority for the FBI moving forward, and that the Bureau must undertake serious, concrete measures to reestablish confidence that they are using their national security authorities responsibly and without favor.

The FBI's existing organizational structure is suboptimal for compliance with privacy and civil liberties protections in national security matters. Currently, compliance with Section 702 rules and procedures are largely outsourced to the National Security Division at the Department of Justice. This directly contributes to what Mr. Kris described as "a culture of operational personnel who feel checked and second-guessed by distant compliance officers."[61] "After-the-fact" assessments by external attorneys can be detrimental to proper use of authority in the first instance, and can also lead to a chilling effect such that FBI personnel are disincentivized from appropriately querying the information when doing so would be mission-appropriate. Compliance must instead be woven into the fabric and internal culture of the agency.

---

[59] Letter Brief of Amicus Curiae David S. Kris, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02 (FISA Ct. Jan. 15, 2020) at 12 [hereinafter Kris Letter Brief].

[60] Durham Report, *supra* note 6, at 18-19.

[61] Kris Letter Brief, *supra* note 59, at 12.

The FBI has made some progress with improving internal compliance but more could be done. For example, a senior official was recently appointed within the Office of the Associate Deputy Director to oversee FISA compliance, but that individual has no dedicated staff. Meanwhile, compliance in field offices is the responsibility of each office's Chief Division Counsel, who each report to the local Special Agent-in-Charge. The CDCs (and, in larger offices, their staff) are responsible for FISA compliance, privacy and civil liberties matters, and general legal advice. A different official, however, at FBI headquarters, is designated as Civil Liberties and Privacy Officer ("CLPO"), as required by 42 USC 2000ee-1, but is also a Deputy General Counsel responsible for numerous other functional sections of the Office of the General Counsel, in addition to privacy and civil liberties. Hence, the CLPO portfolio is only one among many competing responsibilities that occupy the CLPO's time and attention. Furthermore, the CLPO reports to the General Counsel for OGC responsibilities and, per the statute, to the Director for privacy and civil liberties purposes.

By contrast, the CLPO at NSA is a full-time position that directly reports to the NSA Director, the ODNI CLPO reports directly to the DNI, and CIA's Privacy and Civil Liberties Officer reports directly to the CIA Director. The NSA CLPO's access to the Director and high profile at NSA—instituted in response to critical FISC opinions—have cemented compliance as a crucial part of the Director's daily work. They also signal to the workforce the priority and commitment that privacy and civil liberties are accorded. Structurally, NSA's CLPO has been integrated as a collaborative working partner alongside operational components, rather than a police force tasked with second-guessing operational decisions and handing out discipline. NSA implemented these measures and others as part of a thorough compliance program reset after criticism by the FISC and the illegal Snowden leaks. As a result, NSA has suffered relatively few compliance incidents and has more proactively identified problems as well as solutions for those problems.

The FBI's privacy and civil liberties program is thus less well integrated into the FBI's everyday mission work. The Bureau is far more decentralized, which makes a headquarters-based program difficult. FBI's measures to ensure protection of privacy and civil liberties and to improve compliance with Section 702 requirements—constructed over time and often in response to discrete compliance incidents—are more disconnected, and reactive to public controversies and Congressional pressure. Structural changes at the FBI could improve the FBI's culture of compliance.

Value of the Section 702 Program

In assessing the value of the Section 702 program, the Board undertook a comprehensive evaluation of how and to what extent the government uses Section 702 to protect Americans and inform national decision-makers regarding pressing threats to the United States. In doing so, the Board reviewed thousands of pages of classified and unclassified documents; held meetings and

requested briefings from the Intelligence Community; studied reports issued by the Intelligence Community; reviewed written responses from the Intelligence Community in response to numerous, specific Board questions; and analyzed Intelligence Community examples of specific instances where Section 702 intelligence gathering and analysis led to significant positive outcomes (often referred to by the Intelligence Community as "vignettes").[62] We conclude that the Section 702 program is vital to protecting the safety and security of the United States and its citizens. We agree with the Majority that without it, we would be far less safe.

Section 702 provides critical insights into some of most urgent threats facing the country, including the proliferation of weapons to hostile nations and militant groups, ransomware threats to critical infrastructure, the conflict in Ukraine, hostile state behavior, malicious cyber activity, including from China, Russia, and Iran, the trafficking of fentanyl across our borders, and the resurgence across the globe of hubs of terrorist activity focused against the United States.

Indeed, the value of the program has increased in several ways since the Board issued its 2014 Report. Although the Board's mandate extends only to counterterrorism-related authorities and programs, Section 702 supports a broad array of the nation's strategic and defensive goals beyond just counterterrorism. Section 702 provides critical insights into some of most urgent threats facing the country, including the proliferation of weapons to hostile nations and militant groups, ransomware threats to critical infrastructure, the conflict in Ukraine, hostile state behavior, malicious cyber activity, including from China, Russia, and Iran, the trafficking of fentanyl across our borders, and the resurgence across the globe of hubs of terrorist activity focused against the United States.[63] Based on Section 702's speed, flexibility, reliability, and effectiveness, it is uniquely positioned to facilitate the government's identification and response to these emerging threats to the homeland

[62] As discussed below, many of the most significant examples of Section 702's value remain classified in order to protect highly-sensitive sources and methods. Those examples are contained in the Classified Annex to this Statement. The Intelligence Community has recognized the importance of demonstrating to the public and Congress the value and utility of Section 702 in protecting Americans, and has declassified and published some facts, at a general level, representing certain circumstances in which Section 702 collection played a key role. The Intelligence Community has publicly stated that it is working to declassify additional examples. We support those efforts and agree that additional examples should be declassified to the extent that doing so would not harm national security. *See Oversight of Section 702 of the Foreign Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 5 (2023) (June 2023 Joint Statement for the Record of Chris Fonzone, Gen. Couns., Off. of the Dir. of Nat'l Intel., et al.) [hereinafter June 2023 Intelligence Community Joint Statement]. We have assessed this classified information and carefully considered it in reaching our conclusions. In our view, these examples establish significant additional support for the program.

[63] *See id.* *See also* Letter from Merrick Garland, U.S. Att'y Gen., and Avril Haines, Dir. of Nat'l Intel., to S. Majority Leader et al., *Reauthorization of FISA Section 702* (Feb. 28, 2023).

and abroad.[64] In many cases, it is the government's sole source of information about a foreign threat.[65]

The Majority agrees that Section 702 has been highly valuable in protecting the United States from a range of national security threats beyond terrorism.[66] Yet it undervalues the Section 702 program in several important ways: (1) it minimizes or neglects to consider Section 702's importance in responding to two of the most pressing threats facing the country today—the reemergence of terrorist threats against the United States in areas of the globe where the U.S. military has a reduced footprint, and the flood of fentanyl trafficked into the country by foreign actors; (2) it fails to include and consider compelling vignettes demonstrating the importance of Section 702 to U.S. response to strategic competition with foreign powers;[67] (3) it fails to discuss the value of Section 702 to our allies, and to U.S. private industry and infrastructure; and (4) it significantly undervalues the importance of U.S. person queries and batch queries to the FBI, and ignores the value of U.S. person queries to the NSA, CIA, and NCTC. On this final point, the Majority disregards critical lessons learned from the September 11 attacks and important assessments and recommendations made by the 9/11 Commission in its aftermath.

A. The Reemergence of Hubs for Terrorist Plotting Against the United States

There is significant concern that terrorist activity in Afghanistan is surging, and it is once again becoming a safe haven and staging ground for coordinated attacks against the United States and the West. In his March 16, 2023 statement to the Senate Armed Services Committee on the Posture of U.S. Central Command, General Michael Kurilla, Commander, advised Congress that ISIS-Khorasan (a regional syndicate of the international Islamic States terrorist group), which has increased regional terrorist attacks, "is building a capability in Afghanistan from which to strike

[64] *2023 Annual Threat Assessment of the U.S. Intel. Comm.: Hearing Before the S. Select Comm. on Intel.* (Mar. 8, 2023) (statement of Avril Haines, Dir. of Nat'l Intel.) (Section 702 is "principally relied upon for vital insights across a range of high-priority threats" including "malicious cyber actors targeting U.S. critical infrastructure, stopping WMD, threats emanating from China, Russia, North Korea . . .") [hereinafter 2023 Annual Threat Assessment of the U.S. Intel. Comm.].

[65] NSA Director General Paul Nakasone described Section 702 as "irreplaceable," stating that its authorities provide "exquisite foreign intelligence" that "cannot be obtained through other means," and that it plays an "outsized role in protecting the nation." Priv. and C.L. Oversight Bd., Public Forum on Foreign Intelligence Surveillance Act (FISA) Section 702, at 19 (Jan. 12, 2023) (keynote speech by General Paul M. Nakasone, Nat'l Sec. Agency) [hereinafter PCLOB Public Forum]. CIA Deputy Director David Cohen testified that "Section 702 collection illuminates opportunities against foreign individuals and networks of intelligence concern more comprehensively than any other single data source . . ." June 2023 Intelligence Community Joint Statement, *supra* note 62, at 4. Deputy Director Cohen also testified by way of example of its value, that Section 702 collection enabled over 70 percent of the successful weapons and counter proliferation disruptions supported by CIA from 2018 to 2022. *Id.*

[66] Majority Report at Part IV § II(A).

[67] Included in the Classified Annex to our statement are classified vignettes provided by the Intelligence Community, categorized by reference to the Intelligence Community's most recent Annual Threat Assessment, see, Off. of the Dir. of Nat'l Intel., Annual Threat Assessment of the U.S. Intelligence Community (2023). These classified vignettes provide compelling examples of how Section 702's unique capabilities are deployed to protect national security on a daily basis.

Western interests worldwide, with the ultimate goal of a strike on the American homeland."[68] It is critical that the government maintains the ability to monitor and thwart this activity.[69] In the most publicized example, Section 702 collection contributed to the government's knowledge that Ayman-al-Zawahiri, Osama Bin Laden's successor as the head of al-Qa'-ida, was living in a safe house in downtown Kabul, resulting in the July 31, 2022 precision strike that killed him.[70]

B. The Trafficking of Fentanyl Across Our Borders

The head of the Drug Enforcement Administration has reported that fentanyl is the deadliest single drug that our nation has ever encountered.[71] It is estimated that 196 Americans die every day due to fentanyl, which is roughly the equivalent of the September 11, 2001 death toll every fifteen days.[72] Fentanyl flows over the nation's borders at an alarming rate, stemming largely from foreign actors abroad, primarily in China and Mexico. On April 14, 2023, the Justice Department announced charges against the Mexico-based Sinaloa Cartel, which it described as "the largest, most violent, and most prolific fentanyl trafficking operation in the world," run by the cartel and fueled by Chinese precursor chemical and pharmaceutical companies.[73] On May 16, 2023, a bipartisan group of senators introduced a bill to declare fentanyl trafficking a national security crisis.[74]

CIA Director William Burns testified in a March 8, 2023 Senate hearing that Section 702 has been "crucial in illuminating" the networks of Mexican cartels, has enabled the government to

[68] *Posture of USCENTCOM and USAFRICOM in Review of the Defense Authorization Request for FY24 and the Future Years Defense Program: Hearing Before the S. Armed Services Comm.*, 118th Cong. (Mar. 16, 2023) (testimony of Gen. Michael Kurilla, Commander, U.S. Cent. Command).

[69] On March 8, 2022, FBI Director Wray testified that "[Section 702] is the tool that we are going to need more and more not less and less over the next 5 years as the terrorist landscape with the withdrawal in Afghanistan, . . . , I could go on and on, but just about every threat that you have heard about to, the extent that it affects the homeland from overseas, 702 is going to be the tool that protects us." *Annual Worldwide Threats: Hearing Before the H. Permanent Select Comm. on Intel*, 117th Cong. 77 (Mar. 8, 2022) (statement of Christopher A. Wray, Dir., Fed. Bureau of Investigation) [hereinafter 2022 Wray Annual Worldwide Threats Statement].

[70] June, 2023 Intelligence Community Joint Statement, *supra* note 62, at 2. *See also* Jim Garamore, *U.S. Drone Strike Kills al-Qaida Leader in Kabul*, DOD NEWS (Aug. 2, 2022), https://www.defense.gov/News/News-Stories/Article/Article/3114362/us-drone-strike-kills-al-qaida-leader-in-kabul/ (announcing that al-Zawahiri was killed in an over-the-horizon operation, involving multiple streams of intelligence, in which he was struck by Hellfire missiles and was the only casualty).

[71] U.S. Drug Enforcement Admin., *Fentanyl Awareness*, dea.gov/fentanyl/awareness (last visited Sept. 18, 2023).

[72] Press Release, U.S. Sen. Joni Ernst, *Ernst, Kaine Solution to Fentanyl Crisis Advances in the Armed Services Committee* (June 23, 2023).

[73] Press Release, U.S. Dep't. of Justice, *Justice Department Announces Charges Against Sinaloa Cartel's Global Operation* (Apr. 14, 2023), https://www.justice.gov/opa/pr/justice-department-announces-charges-against-sinaloa-cartel-s-global-operation.

[74] News Release, *Ernst, Kaine, Bice, Carbajal Introduce Bill to Combat Threat of Fentanyl* (May 16, 2022). In June, 2023, Sen. Shaheen and Sen. Hassan co-sponsored a bipartisan bill that would declare fentanyl a "national emergency."

work with Mexican partners to take action against the Sinaloa Cartel, and has enabled "significant action" against fentanyl production and processing equipment in Mexico and the U.S."[75] The government recently declassified information demonstrating the intelligence value that Section 702 provides to support international fentanyl interdiction:

- The quantities and potency of drugs, including fentanyl, destined for illegal transfer to the United States, as well as specific smuggling techniques used to avoid detection;
- The involvement of a foreign official in one foreign narcotics trafficker's scheme to transport fentanyl pills within the United States;
- A different foreign narcotics trafficker's purchase of a vast quantity of pills for transfer to the United States; and
- Insights that have informed the U.S. government's understanding of the Chinese origins of a chemical used to synthesize fentanyl.[76]

The government also provided the Board with classified vignettes describing the value of Section 702 in disrupting a cartel's drug trafficking efforts, which are included in the Classified Annex to our Separate Statement.

C. The U.S. Response to Strategic Competition with Major Powers

While the Majority recognizes the crucial role that Section 702 plays in the U.S. response to strategic competition with hostile nation-state adversaries, their report downplays the significance of the following additional examples. Several others are included in the Classified Annex to our Separate Statement.

- Through U.S. person queries of Section 702-acquired information, the FBI discovered that Iranian hackers had conducted extensive research on the former head of a Federal Department. FBI then notified that individual and the Department of the specific threat, so that FBI could take action to protect them and help secure their accounts.[77]
- Section 702 collection has helped identify when hostile foreign intelligence services are trying to send their operatives into the United States to recruit spies. [78]

[75] 2023 Annual Threat Assessment of the U.S. Intel. Comm., *supra* note 64 (statement of William Burns, Dir., Cent. Intel. Agency).

[76] June 2023 Intelligence Community Joint Statement, *supra* note 62, at 3.

[77] The Majority fails to note the use of U.S. person queries.

[78] June 2023 Intelligence Community Joint Statement, *supra* note 62, at 2.

D. The Value of Section 702 to U.S. Allies

Section 702 is valuable not only to the United States, but to our allies. By sharing critical intelligence derived from Section 702, the government assists our allies in countering terrorism, weapons proliferation, malicious cyber activity, and aggression by hostile foreign adversaries.[79] The government has declassified some examples in which it provided Section 702-derived information to aid an ally in responding to a grave threat; additional examples remain classified.

- NSA analysis of Section 702 collection discovered communications between a member of a major terrorist group in the Middle East and an extremist in Europe who was sharing ideas on how to commit a terrorist attack. Specifically, NSA discovered communications where the individual in Europe was discussing buying material to build a suicide belt. NSA shared this critical information with European partners in an attempt to disrupt further attacks against U.S. and allied interests.[80]

- NSA used Section 702 collection to report the 2015 travel of several extremists from the Middle East to Europe, likely for the purpose of conducting terror attacks. One of these travelers was directed by and maintaining contact with one of the planners of the 2015 Paris attacks. NSA provided identifying information to foreign partners, who located, detained, and charged the individual.[81]

- NSA Section 702 reporting helped thwart efforts of front companies seeking to obtain weapons likely bound for a rebel group in the Middle East hostile to U.S. interests. Information derived from Section 702 was shared with a European government, which prompted that government to prevent a nearly $1 million shipment of weapons and ammunition. This European government also revoked the export license of multiple arms companies based on the intelligence.[82]

[79] *See* U.S. DEP'T OF JUST. ET AL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER SCHREMS (Sept. 2020) (including above examples and noting that in its 2014 Report on 702, PCLOB found that, after an extensive review of fifty-four cases in which Section 702 was used, approximately forty cases exclusively involved operatives and plots in foreign countries); Priv. and C.L Oversight Bd., *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program* (Nov. 19, 2020) (stating that U.S. agencies frequently share intelligence produced under Section 702 with European counterparts and citing to sources of examples); Off. of the Dir. of Nat'l Intel., *Section 702 Overview*, at 10, dni.gov/files/icotr/Section702-Basics-Infographic.pdf (stating that the government uses information collected under Section 702 to protect U.S. allies) [hereinafter ODNI Section 702 Overview].

[80] Nat'l Sec. Agency, *Section 702 Saves Lives, Protects the Nation and Allies*, Dec. 12, 2017, nsa.gov/press-room/news-highlights/article/article1627009/section-702-saves-lives-protects-the-nation-and-allies/.

[81] *Id.*

[82] *Id.*

- Section 702 helped the government uncover gruesome atrocities in Ukraine—including the murder of noncombatants and the forced relocation of children from occupied areas to Russia.[83]

E. The Value of Section 702 to U.S. Businesses and Critical Infrastructure

Information derived from Section 702 has proven crucial in the government's efforts to assist private U.S. industry and operators of critical infrastructure in identifying and responding to cyber threats and corporate industrial espionage, including theft of intellectual property.

- Section 702 has been used to identify ransomware attacks on U.S. critical infrastructure, and multiple attacks have been identified and defended against because of Section 702 information.[84] In a highly-publicized example, Section 702 aided the FBI in responding to the May 2021 Darkside ransomware attack that shut down Colonial Pipeline's networks, comprised of more than 5,500 miles of pipeline helping move oil from the Gulf of Mexico to the East Coast, for several days.[85] The President declared this shutdown of U.S. critical infrastructure a national state of emergency, calling for an "all of government response." On June 7, 2021, the Department of Justice announced that it had seized $2.3 million worth of bitcoin—a portion of the proceeds from the ransom payment. Intelligence collected under Section 702 enabled the government to identify the hacker and recover the majority of Colonial's funds.[86]

- U.S. person queries against Section 702-acquired information helped FBI to identify intrusion efforts against a transportation hub in the United States. In that case, the U.S. person queries helped FBI to identify the particular network infrastructure that the Chinese hackers had successfully compromised. This enabled FBI to quickly alert the network operators to the particular portion of their network that had been compromised and assist with fixing the vulnerabilities.[87]

---

[83] *Holding Russian Kleptocrats and Human Rights Violators Accountable for Their Crimes Against Ukraine: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. (2023) (statement of Lisa O. Monaco, Deputy Att'y Gen., U.S. Dep't of Just.) (stating that Section 702 information and other information "has helped us as a country and as a national security community galvanize accountability efforts regarding Ukraine by allowing us to confidently and accurately speak with the international community about atrocities").

[84] 2023 Intelligence Community Joint Statement, *supra* note 62, at 2.

[85] Darkside is a transnational organized crime group believed to operate in Russia. *See* Press Release, U.S. Dep't. of Just., *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021).

[86] June 2023 Intelligence Community Joint Statement, *supra* note 62, at 2.

[87] Letter from Christopher Wray, Dir., Fed. Bureau of Investigation, to Congress in Response to Section 702 Querying Compliance (July 21, 2023) [hereinafter Wray Letter to Congress].

- Section 702-acquired information successfully identified and mitigated an Iranian ransomware attack against a non-profit organization's systems in 2022. Within one week, this intelligence enabled the U.S. government to respond to, mitigate, and ultimately recover the organization's information without paying the ransom.[88]

- In 2022, Section 702 data was vital in warning the international community, the private sector, and the public, about efforts by North Korea to deploy information technology workers to commit fraud against a global industry, including against U.S. businesses to generate revenue for a nuclear program.[89]

F. The Value of U.S. Person Queries

Perhaps the most egregious problem with the Majority's value analysis is its curt dismissal of the value of U.S. person queries to the safety and security of the nation. Eliminating U.S. person queries, or making it bureaucratically infeasible to conduct them—as the Majority recommends—would effectively destroy the crucial portion of the program that enables the U.S. government to prevent, among other things, terrorist attacks on our soil.

The Majority erroneously suggests that a dearth of criminal prosecutions arising directly from U.S. person queries indicates minimal value to the queries. But this utterly misunderstands the program. Domestic criminal prosecutions are not the lone—or even primary—goal of U.S. person queries. A focus on that metric wrongly ignores the significant foreign intelligence and preventative functions described above. A relatively small number of domestic criminal prosecutions resulting from Section 702 information may instead indicate that the government is *not* turning a foreign intelligence tool into a domestic law enforcement tool, as some worry.[90]

We have seen no evidence that Section 702 is being used for domestic surveillance, and as the unanimous Board in 2014 explained, if it were, it would be an extremely poor vehicle for doing so.

The Majority also wrongly implies that Section 702 has somehow morphed from a foreign intelligence program to a domestic surveillance program.[91] We strongly disagree with that implication. We have seen no evidence that Section 702 is being used for domestic surveillance, and as the unanimous Board in 2014 explained, if it were, it would be an extremely poor vehicle for doing so. Nor are the incidental collection of U.S. person information, or the querying of that information, new features of the program. At the outset,

[88] Email from Off. of the Dir. of Nat'l Intel. to PCLOB Staff (June 13, 2023).

[89] June 2023 Intelligence Community Joint Statement, *supra* note 62, at 3.

[90] The privacy risks of using Section 702-acquired information in the domestic criminal context are mitigated by numerous rules and procedures that protect defendants' rights at each stage of a criminal proceeding.

[91] *See, e.g.*, Majority Report Recommendation 3.

following the September 11 attacks, it was clear that one of the program's major purposes was to identify the connections between foreign targets and their associates in the United States.

That is not to say that Congress should abandon consideration of additional protective measures to ensure that U.S. person queries are run properly. As discussed above, Congress can and should. To that end, we support strong additional reforms, and discuss them in the section that follows. However, Congress should consider these reforms with clear eyes about the value that U.S. person queries play with regard to Americans' security.

1. *Discovering Persons in the United States Working In Concert With Foreign Terrorists*

The primary reason that U.S. person queries are so valuable is because they allow the government to identify links between foreign national security threats and persons in the United States. The rationale underpinning U.S. querying authority runs all the way back to the September 11 attacks, and is rooted in the reality that the hijackers had been planning and preparing for the attacks *while on American soil* for up to 18 months preceding the attacks.[92] Moreover, the attackers were in contact with other individuals who lived in the United States for many years preceding the attacks.[93] The 9/11 attacks demonstrated that our adversaries act not only from bunkers abroad, but often within the United States or in direct concert with individuals traveling to, or already in, our country.[94]

Queries are a quick, preliminary step that return focused information. They help analysts to uncover plots, identify bad actors, and recognize links between foreign intelligence targets and U.S. persons. For example, if our military recovers on the battlefield the cellphone of a terrorist insurgent that contains a 212 (New York) area code, our Intelligence Community would likely seek to run that phone number in Section 702-acquired information. Such a query would be presumed to be a U.S. person query because it is an American phone number. Running such a query could provide urgent information about connections between terrorists abroad and their compatriots here.

Importantly, queries facilitate the use of information that the government *already* lawfully possesses, to identify such links swiftly and efficiently. U.S. person queries are not new collections of information. Any targeted surveillance of U.S. persons for foreign intelligence information

[92] *See* THOMAS H. KEAN & HAMILTON H. LEE, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS ON THE UNITED STATES, at 215 (2004) (describing first arrivals in California of two hijackers in January 2000) [hereinafter 9/11 Commission Report].

[93] *See, e.g.*, U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS, at Ch. 5 § IV.B.1. (2004).

[94] The Intelligence Community reported to the Board, and Congress, that U.S. person queries are a critical part of how the agencies utilize their Section 702 authorities. *See* 2023 Intelligence Community Joint Statement.

must be done pursuant to Title I of FISA, and requires a showing of probable cause before the FISC.[95] A U.S. person query in Section 702-acquired information will only return communications between that person and authorized foreign targets abroad or communications in which a foreign target references a query term. It would never allow the government to view a U.S. person's entire email inbox, or listen to all of her cell phone communications. For this reason, the Majority's contention that querying is "analytically equivalent to targeting" is patently false.[96]

It is worth recalling that in analyzing the intelligence and systemic failures that facilitated the September 11, 2001 attack, the 9/11 Commission assessed that "The U.S. government has access to a vast amount of information . . . But the U.S. government has a weak system for processing and using what it has."[97] The Commission thus concluded that "the importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to connect the dots."[98] The design of U.S. person queries—to uncover links between U.S. persons and national security threat actors outside of the United States—addresses this critical observation of the 9/11 Commission Report: that analysts and agents failed to gather information already in the hands of the government and identify individuals involved in the attack.[99]

The Fort Hood Commission, established in the wake of the attack on Fort Hood by a U.S. Army Major who killed 13 fellow soldiers and wounded 32 others after being radicalized by Anwar al-Aulaqi, reached similar conclusions. It concurred fully with the Presidential directive, issued January 7, 2010, to "accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographical information with terrorism-related intelligence."[100]

It does little good to collect information pursuant to Section 702 if the government cannot then effectively use it. Running U.S. person queries is a basic, often minimally invasive, analytical step taken to confirm links to dangerous foreign targets, or to assist in eliminating such suspicions.[101]

[95] Targeting of U.S. persons overseas for foreign intelligence information is governed by Sections 703 and 704 of FISA and is also subject to FISC approval.

[96] Majority Report at Part IV § II(B).

[97] 9/11 Commission Report, *supra* note 91, at 416-17.

[98] *Id.* at 408.

[99] *Id.* at 434.

[100] FORT HOOD INDEP. REVIEW COMM., REPORT OF THE FORT HOOD INDEPENDENT REVIEW COMMITTEE, at 140 (2020).

[101] ODNI Section 702 Overview, *supra* note 79, at 10.

2. *Aiding Actual and Potential U.S. Victims*

The FBI identified to the Board a number of successful examples of "victim" or "defensive" queries, which have been used to identify and warn victims of potential cyberattacks, identify victims of hostile state actors, and identify victims of foreign espionage. The Majority concedes the value of such queries, calling them the "strongest examples of the value of U.S. person queries provided to the Board."[102] The Majority Report, nevertheless, understates the value of these victim queries. U.S. person victim queries are the primary way that the Intelligence Community uses Section 702 to identify potential and actual U.S. victims of foreign attack. If the FBI, for example, receives a tip that a foreign terrorist organization is targeting a particular U.S. person, it would query Section 702 data for that potential victim's identifiers to see if the specific plans against him can be identified. If done quickly enough, the FBI could then take steps to notify the victim and thwart the plan before it is executed.[103] The FBI recently declassified two such examples:

- The FBI ran U.S. person queries against Section 702-acquired information to identify the extent of a foreign government's kidnapping and assassination plots. The timely identification of the foreign government's plans and intentions in Section 702-acquired information contributed to FBI's disruption of the plots.[104]

- Through U.S. person queries of Section 702-acquired information, the FBI discovered that Iranian hackers had conducted extensive research on a former head of a Federal Department. FBI then notified that individual and the Department of the specific threat, so they could take action to protect them and help secure their accounts.[105]

The ability to run U.S. person victim queries is especially important in cases of cyberattack and cyberintrusion. Adversaries increasingly target U.S. critical infrastructure and private U.S. corporations, in addition to targeted attacks on U.S. individuals. The Intelligence Community often runs U.S. person queries using identifiers linked to entities—U.S. companies or associations—rather than individuals, in order to follow a lead that those entities are current or potential targets. Query terms may also be inanimate objects, such as identifiers for critical infrastructure that are not linked to a natural U.S. person but may fall nevertheless under the definition of a U.S. person query. This allows the government to protect U.S. industry and the private information of the American people. As the FBI explained, it may query identifiers related

[102] Majority Report at Part IV § I(E).

[103] PCLOB Public Forum, *supra* note 65 (opening statement of Mike Herrington, Sr. Advisor, Fed. Bureau of Investigation) [hereinafter 2023 Herrington Statement].

[104] Wray letter to Congress, *supra* note 86.

[105] Email from Off. of the Dir. of Nat'l Intel. to PCLOB Staff (June 13, 2023).

to a company that has suffered a cyber-breach in order to determine if the breach is the work of a foreign cyber actor. These queries allow the government to "determine attribution, identify adversary footholds on the network, and share specific information about that cyber group with the company," in a timely manner, and hopefully before major damage is done.[106]

U.S. person queries are also necessary for counterintelligence, in order to identify targets—or accomplices—of foreign espionage. Agents of foreign powers often seek to make contact with U.S. persons, both in government and in private corporations, in order to gain valuable information from them unwittingly or to coopt them as sources. If the FBI finds a foreign spy possesses identifiers for several U.S. persons, this represents a critical investigative crossroads: it is often impossible to determine at this early stage whether individuals associated with those identifiers are malign co-conspirators seeking to pass secrets that could put American lives and partners at risk; or merely innocent and unwitting victims being targeted by our adversaries and in need of protection. A query of the identifiers against Section 702 data allows investigators to take a preliminary, minimally invasive step to help make these critical determinations. If accomplices or co-optees, the FBI would likely pursue additional avenues of investigation. A query also serves to protect the integrity of the investigation, preventing targets from discovering the government's knowledge of their illegal activity. If actual or potential victims, the FBI may conduct defensive briefings or put other protective measures in place to help keep the individuals safe.[107] The FBI recently declassified the following example of a counter-intelligence related query:

- After receiving intelligence from another agency that a U.S. person was in contact with intelligence officers from a particular threat country, FBI queried that U.S. person's identifiers against the FBI's Section 702 collection. The queries returned results from collection on intelligence officers of a "different" threat country. Those results confirmed that the U.S. person had been in contact with officers from the first threat country. FBI subsequently investigated, determined the U.S. person to be unwitting of the illicit activities of the intel1igence officers, and interviewed the U.S. person, obtaining important intelligence on a hostile foreign state's attempts to acquire sensitive information relating to proliferation of weapons of mass destruction.[108]

Querying Section 702 information is significantly less intrusive than seeking a Title I order, as the former returns communications between an individual and the foreign spy or those that contain an authorized query term. It does not return all of the U.S. person's communications. These types of searches are protective not only of the U.S. persons themselves, but also of the intellectual property and sensitive data of the employers of those U.S. persons. The Intelligence

[106] *See* 2023 Herrington Statement, *supra* note 102.

[107] *Id.*

[108] Email from Off. of the Dir. of Nat'l Intel. to PCLOB Staff (June 13, 2023).

Community has provided several examples, some of which are included in the Classified Annex to our Separate Statement, in which these types of victim queries led to successful results.

3. *Investigating Leads*

Querying lawfully acquired data is the primary way that collected information is made accessible to analysts. Running a U.S. person query is an efficient way for investigators to ***rule out*** inaccurate tips or leads. A U.S. person query that returns no results is operationally significant, because it may eliminate further or more intrusive means of investigation such as invasive physical or electronic searches, or electronic surveillance.[109]

In noting that the vast majority of FBI's U.S. person queries of Section 702 information that are conducted return no results, the Majority extrapolates that such searches must therefore have minimal value. Such a position is both illogical and contrary to the evidence the Board has received. While the privacy implications of searches that return no results are minimal, the investigative value is real. In an environment of scarce resources—such as the one in which our Intelligence Community operates—the ability to direct personnel toward real leads instead of false ones can make the difference in preventing an attack or thwarting a foreign operation.

4. *The Value of U.S. Person Queries Across the Intelligence Community*

Finally, the Majority errs by focusing only on the FBI for its analysis of the value of U.S. person queries. As discussed in Part III of the Majority Report, other elements of the Intelligence Community also conduct U.S. person queries to identify links between foreign threats and those in the United States.[110] The value of those queries is significant. For instance:

- Section 702-acquired information related to sanctioned foreign adversaries was used in U.S. government efforts to stop components of weapons of mass destruction from reaching foreign actors.

The Board requested and received additional material from the CIA, NSA, and NCTC demonstrating the value of U.S. person queries to those agencies, and we have included those examples in the Classified Annex to our Separate Statement.

[109] Evidence of a crime-only queries can also prove valuable in cases such as distribution of child sexual abuse material, where the government does not have a separate foreign intelligence purpose. However, such queries are currently subject to a higher legal standard. They are also rare: there were only 16 in all of 2022. Fourteen of those 16 queries were conducted to fulfill discovery obligations in criminal prosecution cases. CY2022 ASTR, *supra* note 32, at 27.

[110] In the 2022 calendar year, NSA, CIA, and NCTC conducted a combined number of 4,684 U.S. person queries. *Id.* at 20.

G. The Value of Section 702 for Vetting

While Section 702 is highly valuable in many respects, the current statutory framework results in under-utilization for vetting. The government conducts vetting in several contexts in order to determine whether an individual might pose a risk to national security. For purposes of this statement, we discuss two of those contexts: the vetting of non-U.S. person applicants for visas to visit, work, or live in the United States, and the vetting of U.S. person applicants for high-level security clearances which would allow those persons access to classified or other sensitive information.

Under the current statutory framework of Section 702, the government may already have in its possession—but be legally unable to access—information that foreigners entering the United States, or persons applying for U.S. government security clearances, present threats to national security. In our view, it is unacceptable that such information is lawfully collected, but rendered essentially unusable or severely limited.

Currently, the government is limited in its ability to query unminimized existing Section 702-acquired data as part of the vetting process. As discussed in Part III of the Majority Report, the government may generally only query Section 702 data if doing so is "reasonably likely to return foreign intelligence information" (or evidence of a crime in the case of the FBI). Thus, if the government lacks a specific reason to believe it will find foreign intelligence information (or evidence of a crime) related to the search term, it may not run the query. As a result, the government may already possess information relevant to the assessment of national security risk that is never seen.

To address this gap, and in response to Presidential directives, the NSA's current FISC-approved querying procedures permit it to "use certain unminimized section 702-acquired information for valid counterterrorism foreign intelligence purposes as directed to support the federal government's vetting of non-United States persons who are being processed for travel to the United States or a benefit under U.S. immigration laws (a 'travel or immigration applicant')."[111] Thus, notwithstanding the "reasonably likely to retrieve foreign intelligence standard," the NSA has promulgated a three-step process to support "travel vetting." The FISC has held this process to be consistent with the requirements of the Fourth Amendment.[112]

[111] NSA Querying Procedures, *supra* note 31.

[112] Apr. 11, 2023 FISC Opinion and Order, *supra* note 12, at 81

The NSA's process, however, is limited in several ways, which must be discussed in a classified setting. And the NSA has not promulgated any similar querying procedures for applicants for U.S. government security clearances.

1. *Visa Applicants*

The United States government granted more than 7 million visas in 2022 to non-U.S. citizen immigrants and various categories of non-immigrants, such as tourists, students, and temporary workers.[113] The government has endeavored to create a coordinated visa applicant vetting system through the National Vetting Center (NVC).[114] Despite those efforts, terrorists and spies have been able to use the visa process to penetrate our borders.[115] The potential consequences resulting from admission of even a single individual seeking to commit an act of terrorism or mass destruction could be catastrophic.

The NVC aims to ensure that travel and immigration-related security checks are complete and coordinated by allowing adjudicating agencies to review certain information lawfully collected by the Intelligence Community.[116] Data provided to NVC continues to be owned and controlled by the Intelligence Community and maintained under their authorities.[117] Nevertheless, as discussed above, current statutory limitations on querying Section 702-acquired information preclude sufficient review of this information in connection with visa applications. Statutory change could allow vetting to be a clear exception to the querying standard, with applicant consent. Such access to Section 702 information for vetting purposes would allow NVC to provide adjudicating agencies additional insight into an applicant before that person is admitted to live, work, or visit the United States.

[113] U.S. DEP'T OF STATE, REPORT OF THE VISA OFFICE (2022).

[114] U.S. DEP'T. OF HOMELAND SEC., PLAN TO IMPLEMENT THE PRESIDENTIAL MEMORANDUM ON OPTIMIZING THE USE OF FEDERAL GOVERNMENT INFORMATION IN SUPPORT OF THE NATIONAL VETTING ENTERPRISE (2018).

[115] For example, on April 28, 2021, a Chinese national who gained admission to the United States through the EB-5 Immigrant Investor Visa Program pleaded guilty after admitting that he illegally procured and exported items with use in anti-submarine warfare to a Chinese military university. Press Release, U.S. Dep't. of Just., *Chinese National Pleads Guilty to Illegal Exports to Northwestern Polytechnical University* (Apr. 28, 2021), https://justice.gov/opa/pr/chinese-national-pleads-guilty-illegal-exports-northwestn-polytechnical-university. According to a criminal complaint filed in the United States District Court for the District of Ohio in 2022, an Iraqi citizen with ties to al-Qa'-ida in Iraq and ISIS obtained a B-1/B-2 "business or pleasure" non-immigrant visa in September 2020 (and later applied for asylum) with the intent of smuggling terrorists into the United States to murder former President George W. Bush. *U.S. v. Shihab*, No. 2:22-mj-366 (S.D. Ohio Mar. 23, 2022).

[116] U.S. Customs and Border Prot., *National Vetting Center*, https://www.cbp.gov\border-security/ports-entry/national-vetting-center (last visited Sept. 18, 2023).

[117] Any Section 702-acquired information permitted to be queried for vetting visa and security clearance applicants would be governed by the FISA Court-approved dissemination and retention rules.

2. *National Security Clearance Applicants*

According to a 2020 report by the National Counterintelligence and Security Center, in 2019, roughly 2.9 million individuals held a U.S. federal security clearance, 1.3 million of whom held Top Secret clearance.[118] Applicants for national security clearances submit to extensive background checks and consent to credit checks, medical records checks, and criminal records checks as a condition of employment in these positions of public trust and in order to perform work involving access to sensitive information. Three of the intelligence agencies granting clearances—NSA, FBI, and CIA—have existing authority to query Section 702 data (for foreign intelligence purposes) and each has its own minimization procedures. The agencies, however, are precluded by FISC-approved querying procedures from conducting searches of unminimized Section 702-acquired data unless such searches are "reasonably likely to return foreign intelligence information" (or evidence of a crime in the case of the FBI). Thus, in many cases the agencies may be unable to determine whether an applicant for national security clearance is in contact with a foreign target, and whether that applicant may be a witting or unwitting associate of that target.

* * *

While assessing the Section 702 program to be highly valuable, the Majority Report is unnecessarily dismissive of several aspects of the program that directly contribute to the safety of the homeland. Indeed, it is crucial for the Intelligence Community to maintain the ability to use lawfully-collected information to discover those in the United States who are plotting with foreign actors.

As the adversaries of the United States increasingly use electronic communications to achieve their ends, the value of the Section 702 program has grown. Its loss or impairment would be a crucial setback to our national defense.

IV. Response to the Majority's Analysis and Recommendations

As is plainly apparent, the Majority has produced a very different document than the report the Board unanimously issued in 2014. As stated at the outset, we do not join in the Majority Report for a number of reasons. Rather than simply enumerate our criticisms, we have separately analyzed the program's impact on privacy and civil liberties, and expanded upon the Majority's analysis of the value of the program. In Section V, we offer substantive recommendations that meaningfully address privacy and civil liberties concerns. Nevertheless, because we take issue with much of the Majority's Report, we briefly address some of the most significant flaws—without detailing an exhaustive list of problems we see—including that (1) the analysis of privacy

[118] OFF. OF THE DIR. OF NAT'L INTEL. NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FISCAL YEAR 2019 ANNUAL REPORT ON SECURITY CLEARANCE DETERMINATIONS (2020).

and civil liberties implications raises speculative harms, often unmoored from evidence, while largely failing to evaluate countervailing mitigation or context; (2) many of the Majority's recommendations fail to meet concerns raised in the analysis; and (3) most concerningly, certain of the Majority's recommendations would gravely damage national security, and negatively impact the privacy and civil liberties of U.S. persons.

A. The Majority's Analysis of Privacy and Civil Liberties Implications Is Deeply Flawed.

The Majority's analysis of the privacy and civil liberties implications of Section 702 (the "Analysis") contains sparse evidence or investigation. The Analysis conjures the specter of certain harms to privacy and civil liberties, unsubstantiated by evidence of actual harm, and largely without consideration for potential mitigation, or context that appropriately frames the risk. Without this crucial evidence and context, the Analysis presents a false equivalence between the documented value of the program and theorized, unmitigated "risks." The proper comparison, though, is between the documented value of the program and *relative* risk and the *likelihood* of harm. As we discussed above, privacy risks and the misuse of intelligence authorities, are, of course, real, and must be guarded against. But it is the Board's duty to identify and evaluate these risks through careful consideration and evidentiary analysis. For that reason, the kitchen-sink approach taken in the Analysis confuses the issues—failing to distinguish actual risks with those that are theoretical or significantly mitigated.

The Majority conjures the specter of certain harms to privacy and civil liberties, unsubstantiated by evidence of actual harm, and largely without consideration for potential mitigation, or context that appropriately frames the risk.

The Analysis first addresses Section 702 targeting and collection.[119] Among other complaints, the Analysis theorizes: the definition of "foreign intelligence information" is overly broad;[120] persons targeted under Section 702 could instead be targeted under other legal authorities, such as Title I;[121] and the program poses risks that "targeting can be overbroad or unjustified."[122]

First, as Part III of the Majority Report states, the evidence convincingly demonstrates that the collection side of the Section 702 program has incurred incredibly low rates of error: as noted above the NSA's targeting compliance rate is 99.85 percent and the FBI's targeting compliance

[119] *See* Majority Report at Part IV § II(A).

[120] *Id.* at Part IV § II(A)(1).

[121] *Id.* at Part IV § II(A)(2).

[122] *Id.*

rate is 99.99 percent. This means, quite simply, that the government is neither intentionally nor inadvertently targeting Americans for surveillance through Section 702.

Second, with regard to the statutory definition of "foreign intelligence information," the Analysis concedes that the government is operating within the narrowed, specific certifications approved by the FISA Court for Section 702 collection.[123] While the Analysis deems the definition of foreign intelligence information to be "very broad," it provides no explanation for why (or how) future theoretical, lawful collection of the information of foreigners overseas "extending to the outer bounds of the FISA definition" should be circumscribed. Additionally, the Analysis declines to explain what categories of collection could be sought outside the current certifications; why seeking collection for those categories would be more harmful than beneficial; whether there is any indication that the government would intend to expand the current scope by seeking additional certification; or whether there is any reasonable likelihood the FISC would approve it.

The Analysis further speculates that there is an "increasing" risk that targeting within the 702 design structure can be "overbroad or unjustified" without pointing to examples where overbroad or unjustified targeting is occurring. The evidence of consistently low compliance error rates with regard to targeting undercut this conclusion.

Third, the Analysis makes the unsupported assertion that "more privacy protective legal authorities like Title I of FISA may be available to the government in many cases."[124] The Analysis provides no basis for this assertion, nor any explanation for why foreigners overseas who are appropriately targeted for foreign intelligence purposes should be entitled to the same court procedures as U.S. persons.

Fourth, the Analysis states that the Board undertook a "review [of] individual tasking sheets" and as a result of that review "identified many instances in which analysts' written foreign intelligence justifications lack sufficient detail."[125] To our knowledge, the Board reviewed only ten tasking sheets in total. We have no assurance, and are indeed highly doubtful, that this very small number could be a representative sample. While the Analysis concedes that each of the tasking sheets appropriately showed the targets to be non-U.S. persons located outside of the United States, it declares the documentation of foreign intelligence purpose to be insufficiently detailed. It reaches this conclusion without reference to the existing standard for documenting foreign intelligence purpose.[126] A conclusion as to what would constitute "sufficient detail"

[123] *Id.* at Part IV § II(A)(1).

[124] *Id.* at Part IV § II(A)(2).

[125] *Id.*

[126] Targeting procedures require an analyst to "reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a FISC-approved certification. Analysts must provide a

requires not only expertise in operational foreign intelligence gathering, but also consideration of the countervailing costs and benefits of requiring additional information. Such consideration is not present in the Analysis.

Finally, the Analysis describes a new collection technique, which, following briefing, including by the amicus, was approved by the FISC. The Analysis concedes that the technique has only been approved for use in very narrow circumstances, but nevertheless concludes it could become "extraordinarily intrusive" if "used in widespread fashion."[127] The Analysis fails to point to any evidence of intent—or ability—to use the technique in such a fashion. It further fails to describe the layers upon layers of pre- and post-targeting procedural checks to ensure the collection has no connection with a United States person or anyone in the United States.[128] Indeed, it appears there are not even any incidental U.S. person collections or any U.S. person communications associated with this technique. Given the significant privacy mitigations and heavy procedural oversight over this technique, the risks to U.S. person privacy from this are extraordinarily low.

For these reasons and others, the Analysis draws a speculative conclusion that the risks of overbroad or unjustified targeting are increasing. The evidence points firmly to the fact that the government is not using the Section 702 program unlawfully to target Americans or anyone on U.S. soil.

With respect to querying, the Majority is also largely off-base. As a threshold mater, considering that the government could legally surveil under Section 702 entire communications of a foreign target as they occurred in real time, it would be anomalous to construe a focused query of that target's communications in a database sometime later as more privacy invasive. The Analysis also fails to grapple with the question of whether queries that return no results are themselves problematic from a privacy and civil liberties standpoint. As has been discussed previously, the FBI has access to a very small percentage (roughly 3 percent) of the overall Section 702 information acquired from foreign targets. The FBI therefore only queries data from targets who are relevant to predicated national security investigations. Moreover, U.S. person queries run by the FBI only infrequently return information. When there is no result, then—by definition—the government has ***not*** reviewed any U.S. person communications with regard to that query. In fact, the Majority later implicitly concedes the lack of privacy intrusion by recommending FISC

written explanation of the basis of that determination sufficient to demonstrate that the targeting of each target is likely to return foreign intelligence information. NAT'L SEC. AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, at 9 (2021) [hereinafter "NSA 2021 Targeting Procedures"], at 9.

[127] Majority Report at Part IV § II(A)(4).

[128] Apr. 21, 2022 FISC Opinion and Order, *supra* note 12, at 113.

pre-approval only to review results. Nonetheless, the Analysis fails to differentiate between queries that return results and queries that do not.

The lack of critical evaluation in the Analysis contrasts with the Board's approach to documenting the value of the program. The Board applied rigorous standards to evaluate the examples of value proffered by the Intelligence Community. For every case cited in the Majority Report, the Board thoroughly investigated the Intelligence Community's claims of success and how Section 702 authorities directly contributed to it. As a result, the value discussion in Part IV of the Majority Report is largely convincing, particularly when supplemented by the classified examples that have been provided. Indeed, as we stated earlier, we agree with almost all of it.

The Analysis, however, fails more broadly by declining appropriately to credit changes in the program since 2014 that have increased protections for privacy and civil liberties. As one significant example, the Board in its 2014 Report devoted almost half its analysis of privacy and civil liberties implications to so-called "abouts" collection. The Board described "abouts" as "the NSA's acquisition of Internet communications that are neither to nor from an email address—but that instead merely include a reference to that selector."[129] The Board was concerned that "abouts" collection was improper because it was "more likely than other forms of collection to acquire wholly domestic communications,"[130] and it allowed "the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications."[131] These problems were real and needed to be corrected. In 2017, NSA suspended abouts collection. Congress then codified the suspension in the 2018 Section 702 reauthorization, requiring approval of the FISC and notification to Congress if NSA proposed to restart that form of collection. Since then, the government has not sought to collect "abouts" communications.

The Analysis also fails to credit changes instituted recently—albeit belatedly—to improve FBI compliance. The FBI has redesigned its query tool so that FBI personnel must "opt-in" to search through Section 702 acquired information. This change has likely been central to the reduction in U.S. person queries by 94 percent. The FBI also modified its systems to require FBI personnel to enter written "case-specific" justifications for running U.S. person queries (i.e. why the query is reasonably likely to return foreign intelligence information or evidence of a crime). Even more significantly, the FBI is redesigning its systems to require that the written justification be provided before running a U.S. person query, whereas previously, the justification was required only if the query returned a "hit" and the personnel wanted to view the contents of that

[129] 2014 PCLOB Report, *supra* note 10, at 119.

[130] *Id.* at 120.

[131] *Id.* at 121.

communication. The FBI also now requires preapproval for all batch queries; previously it required attorney pre-approval only for those with greater than 100 query terms. And the FBI has enhanced its query training and accountability, including mandatory annual training for any personnel with access to Section 702 acquired information, performance measures for field office senior leadership based on their office's FISA compliance, and disciplinary procedures for intentional misconduct, reckless behavior, or performance incidents involving negligence.

B. The Majority's Recommendations Fail to Address the Most Significant Concerns, And Would, In Some Cases, Negatively Affect the Privacy and Civil Liberties of U.S. Persons.

Because the Majority's recommendations are based on a flawed analysis that fails meaningfully to differentiate among perceived risks, their recommendations do little to enhance the protection of privacy and civil liberties. Indeed, for certain recommendations that require the government to do ***more*** research into the identity and background of U.S. persons, privacy of those U.S. persons could be negatively impacted. At the same time, the recommendations prioritize haphazard additional layers of bureaucratic burden without meaningful structural and organizational change. In many cases, there is insufficient consideration of burden and the resulting impact on the protection of national security.

The Majority's recommendations do little to enhance the protection of privacy and civil liberties. Indeed, for certain recommendations that require the government to do *more* research into the identity and background of U.S. persons, privacy of those U.S. persons could be negatively impacted.

The Majority's most substantive recommendation, Recommendation 3, encapsulates these problems. Recommendation 3 states that Congress should require FISC authorization of all U.S. person query terms before the government can access the results of any U.S. person query. As drafted by the Majority, it is deeply problematic.

As a threshold matter, the standard the Majority adopts is unmoored from any legal justification. The Majority declines to recommend a probable cause standard, and instead would ask the FISC to apply a "reasonably likely to retrieve" foreign intelligence standard—the same standard that the Intelligence Community already must apply before querying the data. They thus would interpose third-party review, and the time and burden that accompanies that, without any heightened legal standard. Because they do not posit that a probable cause standard is legally required, the entire exercise becomes a question of policy: whether the benefits of additional third-party review outweigh the resulting costs.

Under this rubric, the answer is a resounding no. First, for the majority of the Intelligence Community, the number of query compliance errors is already relatively low. It is far from clear

that another layer of third-party review under the same standard would provide much, if any, benefit. Moreover, such a process is likely to diminish significantly the value of the program. As discussed repeatedly, U.S. person queries are valuable, first and foremost, because they allow the government to identify links between foreign national security threats and persons in the United States. If Intelligence Community personnel had to pause their analysis every time they performed a U.S. person query and wait (potentially weeks or longer) for lawyers to prepare thorough packages for court review, and for the court to review those packages, before they could review the query results, they could not effectively follow leads, rule out suspects, or "connect the dots" between malign actors abroad and their associates in the United States. Worse, if the results of the query provided further intelligence for the Intelligence Community personnel to track down and evaluate, they would have to stop and wait *again* for court pre-approval to perform their next query. Research and analysis that can now be performed with relative speed would grind to a halt. The Intelligence Community provided the Board with several examples of successful intelligence operations that would have failed had court approval been required.

Indeed, because it applies to U.S. person queries that return results, the Majority's recommendation would most negatively impact *the most important and urgent* queries—the ones that show a connection between foreign targets and U.S. persons, the ones that the FBI must review as quickly as possible. The Majority further fails to acknowledge that their recommendation would apply to *all* queries conducted by NSA, CIA, and NCTC, which do not—and in fact cannot with current system design—differentiate between queries that return results and those that do not. Hence, the recommendation would simultaneously prevent the FBI from quickly evaluating and responding to the results of the most important queries it performs, while potentially eliminating the other agencies' performance of *any* U.S. person queries. And, as written, the requirement would apply to queries of metadata in addition to content, which would cripple the program by making it harder to distinguish U.S. persons from non-U.S. persons. In this way, targeting decisions would likely become less accurate.

FISC pre-approval would most negatively impact *the most important and urgent* queries—the ones that show a connection between foreign targets and U.S. persons, the ones that the FBI must review as quickly as possible.

Second, the Majority does not assess the significant burden on the Intelligence Community or the FISC that would be created by their recommendation. As a threshold matter, it is unclear what collection of information would be sufficient to support a submission to the FISC under a reasonably likely to retrieve foreign intelligence standard. The FISC is not suited to put itself in the shoes of intelligence analysts making real-time research and analytic investigative decisions across cases. Moreover, the time and effort required to prepare an application to the FISC for pre-approval of query terms would be enormous. Analysts would have to document their investigation up to that point, prepare affidavits, and coordinate back and forth with their own and DOJ attorneys. The attorneys would then have to review the application package, which would entail

their own assessment of whether the court would be convinced by the evidence proffered, to meet a standard that would be untested and changing for some time. Then the court would have to evaluate the package, including back and forth with the government about the evidence, as frequently happens in the FISA Title I and criminal search warrant contexts. The entire process would paralyze urgent national security investigations.[132]

Third, the Majority does not take into account the likely chilling effect of their recommendation. The 9/11 Commission identified not just the "wall" between foreign intelligence operations and law enforcement investigations as a contributing factor to the failure of the government to find the two terrorists present in the United States in the time before the attack. The Commission also described in detail the impact of the procedures designed to maintain the "wall" on individual agents trying to perform their duties. To avoid coming close to the "wall," agents did not do as much as they legally could and would have been justified by policy to do. Similarly, the burdens of the process that the Majority would impose would disincentivize personnel from using their lawful authorities to protect the nation.

Fourth, the Majority's proposed exceptions to the requirement for FISC pre-approval of U.S. person query terms are detached from reality. The government cannot practically seek consent from apparent victims of foreign action because they often do not know, at this early stage, whether the individuals are victims or co-conspirators. In the latter case, and sometimes the former, seeking consent would no doubt tip off those seeking to do harm, revealing the government's source of information and effectively shutting it down. Nor does the Majority's proposed exigency exception resolve the problem of delay. Before a query, when the investigation is still underway, the government may not know an exigency exists—as with the 9/11 hijackers who had entered the country. Attributing omniscience to investigators falsely assumes that they are acting with perfect information.

The resulting effect on privacy and civil liberties would be minimal, at best, and affirmatively harmful, at worst. As mentioned above, there is no evidence that most of the relevant agencies have large-scale query compliance issues. Nor would pre-approval to review query results address FBI's query compliance issues, because those occur almost exclusively when queries are run, not when the results are viewed (except for the handful of violations of the (f)(2) requirement). Moreover, the additional investigation into the background of U.S. persons in order to prepare a full package for the FISC for each query could be quite significant, requiring Intelligence Community resources affirmatively to compile information on U.S. persons in ways that are currently unnecessary, and, ironically, are more invasive of U.S. persons' privacy and civil liberties interests.

[132] The government has represented in a number of briefings that the Majority's recommendation would effectively eliminate the ability to run U.S. person queries.

Many of the Majority's other recommendations similarly lack sufficient consideration for the actual impact on privacy and civil liberties, and countervailing balance for national security. Abouts collection is already suspended in practice and statutorily prohibited without FISC approval and Congressional notification. Banning it entirely upsets the compromise reached by Congress in 2017, does not address an existing privacy issue, and could prevent the NSA from applying to use it if necessary.[133] Codifying the already broad list of authorized reasons for electronic surveillance in EO 14086 would not substantively limit the Intelligence Community; and would raise various legal concerns by allowing the FISC to second-guess foreign intelligence purposes. Requiring individual justifications for each term in a batch query for non-U.S. persons is not required by E.O. 14086 and would oblige analysts to write out hundreds or even thousands of justifications, many of which would likely be the same.[134]

In sum, the Majority's recommendations do not address the real concerns with the Section 702 program. However, if adopted, they would degrade its value substantially, and some would negatively affect privacy and civil liberties. Alternatively, our recommendations squarely address the privacy and civil liberties risks identified, while maintaining the significant operational value of the program.

V. Recommendations

We encourage Congress and the Intelligence Community to consider the following significant reforms to the Section 702 program in order to better protect privacy and civil liberties while maintaining the program's high value. We have divided the recommendations into three categories: (1) Recommendations to Structurally and Procedurally Reform the FBI; (2) Recommendations To Guard Against Potential Weaponization and Misuse of the Section 702 Program; (3) Recommendations to Improve the Use of the Program to Vet Applicants for Visas and High-Level Security Clearances. To the extent that implementation of these recommendations would require additional resources, we urge Congress to authorize and appropriate the necessary funds.

A. Enact Structural Reform of the FBI and Procedural Reform of Its Section 702 Practices

The widespread compliance violations that have been reported over the last several years—particularly with regard to the querying of Section 702 information—leave no question that the FBI requires additional, significant reform.

[133] Indeed, the exigency exception proposed would be less privacy protective because the NSA could invoke it and restart abouts collection without the current pre-approval by the FISC and Congressional notification required.

[134] Contrary to the Majority's claim, running a query of all of the names in the contact list of a phone seized from a known terrorist meets the query justification of a search that is reasonably likely to retrieve foreign intelligence.

Much of the reform we recommend is cultural and structural; some of it is procedural. All of it, however, is aimed at re-establishing public trust in the FBI. This requires both reorganization and accountability. After the Snowden leaks in 2013, the NSA engaged in serious reform—embedding privacy and civil liberties protections throughout its organization. As a result, the NSA now discovers internally the majority of its compliance incidents, which are relatively low in number. The FBI must engage in similar, wide-scale reform. While we commend the FBI for many of its recent policy changes, we are of the opinion that they are both too little and too late. We describe below additional, substantial reforms that we urge both Congress and the FBI to implement.

RECOMMENDATION 1: Reform the Structure and Culture of FBI.

FBI should reform its structure to better incorporate privacy and civil liberties into the fabric of its operations.

Privacy and civil liberties are not an afterthought. They are an essential part of the core American values that our government and its officials are sworn to protect. In more than a year of examining the Section 702 program in depth, and in reviewing the privacy and civil liberties protections across the Intelligence Community, it has become plainly apparent to us that the FBI requires meaningful structural reform in order to facilitate a stronger culture of compliance.

Specifically, we would recommend moving the FBI's Civil Liberties and Privacy Officer out of the Office of General Counsel to a stand-alone office with a direct report to the Director. This framework is consistent with how NSA, ODNI, and CIA are currently organized. This move would elevate the role of privacy and civil liberties to senior leadership. It would also better facilitate the consideration of privacy and civil liberties issues in policy and operational decisions, as well as legal decisions.

We also recommend that privacy and civil liberties officers, distinct from division counsels, be embedded in the field—at a regional level, at a minimum. These officers would be direct reports both to the Special Agent in Charge (SAC) and to the main Civil Liberties and Privacy Officer at headquarters. The FBI is a decentralized organization, largely driven by the work in field offices. While this current structure presents certain key advantages from a mission perspective, it has the potential to make compliance control substantially more difficult. A review of the FBI's recent Section 702 querying compliance incidents underscores this point: many of the most egregious querying compliance incidents stemmed from field office operations. Often, numerous incidents occurred in the same office.

The embedded officers should work in partnership with FBI personnel in support of the mission. Allowing agents and analysts to work hand-in-glove directly with these officers should facilitate lawful and appropriate queries—avoiding both improper over-querying, and the risk of

under-querying. When accessing Section 702-acquired information is called-for and proper, officers should ensure that FBI personnel are not hesitant to access that information and are not chilled from important investigation.

Finally, we agree that training—especially at field offices—needs to be substantially improved. Re-training in the standards and requirements for accessing unminimized Section 702 data must be completed at regular intervals, and must be mandatory for those who have not accessed such data recently. All FBI personnel with access to Section 702 information must be made exceptionally aware of the thresholds that must be met for querying the database, and the protections required to preserve the privacy of that information.

RECOMMENDATION 2: Codify Privacy and Civil Liberties Protections for Querying.

Congress should codify and expand protections to ensure that all queries of Section 702 information are limited and appropriate.

Congress should enact significant reforms to the FBI querying process for all queries. As described in Part III of the Majority Report, the FBI has recently—and belatedly—instituted a number of changes to address the compliance issues with the FBI's querying, especially with regard to U.S. person identifiers, including: policy changes requiring pre-query approvals; process enhancements that safeguard against non-compliant queries; increased training for agents with access to Section 702 data; and substantially increased internal oversight. As a result of these changes, the number of U.S. person queries conducted by the FBI has decreased by 94 percent and, concomitantly, querying compliance incidents have greatly decreased, as noted by the FISC, to 1.7 percent.[135] Although these reforms are certainly needed, they can be strengthened. Congress can further address FBI's compliance and trust issues by limiting the amount of Section 702 data available to the FBI in the first instance.

The FBI currently receives—and can thus query against—only a small percentage of the government's total Section 702 collection. As published in the Director of National Intelligence April 23, 2023 Annual Statistical Transparency Report for the calendar year 2022, the FBI received data from only 3.2 percent of all Intelligence Community Section 702 targets as of February 2023—only those who were relevant to predicated national security investigations.[136] This substantial limitation is prescribed by FBI policy.[137] Codifying these limited parameters would be

[135] Apr. 11, 2023 FISC Opinion and Order, *supra* note 12, at 84

[136] CY 2022 ASTR *supra* note 32, at 22.

[137] FED. BUREAU OF INVESTIGATION, FOREIGN INTELLIGENCE SURVEILLANCE ACT AND STANDARD MINIMIZATION PROCEDURES POLICY GUIDE, at 301 (2021). The FBI must have an adequate factual predicate to open a full investigation based on threats to national security (e.g., terrorism or foreign computer intrusions) and agents must follow detailed

consistent with the FBI's narrower national security mission relative to other Intelligence Community counterparts. It would also assure the public that the FBI will not expand its collection beyond those parameters.

Congress can further strengthen the privacy and civil liberties protections in place for U.S. persons by mandating that FBI institute more rigorous justification and approval requirements for running U.S. person queries at the outset.

First, and most importantly, Congress should require internal leadership and compliance group approval prior to accessing the contents of *any* "hit" obtained as a result of a U.S. person query.[138] The FBI has so far declined to require this, although other agencies have taken this step. Strong supervisory review and review for legal sufficiency would strengthen accountability and can help detect and prevent compliance incidents before they occur.

This would be in addition to the current mandates of attorney pre-approval for both sensitive queries and batch queries. Congress should codify these requirements as well, absent exigency. These requirements will directly and meaningfully address some of the more significant compliance incidents that have resulted from batch job queries; and will provide a layer of protection for issues arising from queries that have fueled speculation regarding politically-motivated querying.[139]

Second, Congress should require the FBI maintain the revised structure in its Section 702 database system so that FBI personnel with access to that system must "opt-in" to querying Section 702 information as an initial step in the querying process. This will directly and meaningfully address inadvertent access issues, which have caused a significant percentage of FBI compliance incidents.[140]

---

guidance to do so. FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, at 6-2, 701 (2022).

[138] At NSA, personnel are required to receive such approvals prior to running queries of Section 702-acquired content, *see* Majority Report at Part III § VI(B)(3)(a) ("the approving system then routes the terms and associated justification through, at a minimum, two levels of internal leadership and then to the Compliance Group for Cybersecurity and Operations and OGC, both of which must approve the query term prior to use."). For FBI, this pre-approval would likely be unworkable prior to running the queries. However, approval would be required only upon accessing the content of U.S. person queries that receive "hits" – a much smaller number.

[139] U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: 01 JUNE 2020 – 30 NOVEMBER 2020 (Apr. 2022).

[140] *See* Majority Report at Part III § IX(C), note 549 ("Some of the more significant compliance incidents caused by the opt-out system design involved FBI personnel querying their own name in order to locate work products drafted by them, without realizing the query term would run in Section 702-acquired information.")

Third, Congress should codify the requirement that compels the FBI to (a) provide factual justifications supporting queries prior to running the query; and (b) implement system design changes to capture and store those justifications. Previously, FBI agents and analysts were not required to do this. Instead, they were permitted to run a query term to determine if they got a "hit," and then only needed to provide a written justification for the query if they wanted to see the contents of the "hit." These recommended changes will obligate agents and analysts to reflect on the querying standards each time they run a search, which is likely, in turn, to result in fewer non-compliant queries. The recorded information will also provide records for the FBI and its oversight bodies to review in the event of a non-compliant query.

RECOMMENDATION 3: Improve FBI Compliance and Auditing.

FBI should improve its Section 702 compliance processes and auditing; DOJ should annually review FBI field offices.

We agree that FBI must strengthen its current Section 702 compliance program and supplement its existing internal auditing. The FBI established the Office of Internal Auditing ("OIA") in 2020 at the direction of Attorney General Barr in order to develop auditing programs and augment internal compliance with FBI's national security functions.[141] This office should be the first line in detecting compliance problems and working to remedy them, in addition to the current higher-level auditing and oversight by DOJ and ODNI. OIA is currently developing the structure of its auditing processes and plans on performing robust Section 702 auditing in the near future, but it is under-funded and under-staffed. The FBI should conduct its own internal compliance reviews and post hoc auditing, which will likely result in a further reduction of compliance incidents with more frequent audits.

To underscore this effort, we agree that DOJ should conduct annual compliance reviews at all FBI field offices. The Board's investigation has shown that DOJ's oversight of FBI's compliance with the Section 702 procedures has been important in identifying and working to mitigate FBI's compliance issues; however, DOJ's annual compliance reviews are conducted at only a portion of the FBI's 56 field offices each year. Its annual reviews should extend to all field offices.

B. Guard Against Potential Weaponization and Misuse of the Section 702 Program

As discussed above, we share the real and significant concern that the authorities given to the Intelligence Community can be misused for political or other improper purpose. We understand that the most egregious recent violations concerning the 2016 Presidential transition

[141] Memorandum from William Barr, Att'y Gen., to the Deputy Att'y Gen. et al., *Augmenting the Internal Compliance Functions of the Federal Bureau of Investigation* (Aug. 31, 2020).

did not involve Section 702. However, numerous queries were run inappropriately in connection with civil unrest following the killing of George Floyd, and the events of January 6, 2021. We therefore recommend that additional safeguards be put in place to ensure appropriate oversight over the program going forward. Specifically, *Congress* should have the opportunity to review sensitive queries, including those involving public officials, political candidates, members of the news media, and protected First Amendment activities, on a regular basis. More stringent procedures should be adopted for requests to "unmask" U.S. persons. And Congress should enact harsher penalties for those who leak protected Section 702-acquired information concerning U.S. persons.

RECOMMENDATION 4: Congressional Oversight of Sensitive Queries.

Congress should require that the Intelligence Community develop, or further refine, policies regarding sensitive queries in coordination with DOJ and ODNI. These policies should be submitted to the FISC for review and approval as part of the annual certification process, and included in the agency querying procedures. Congress should require that each agency report to Congress, at least once every six months, each of the sensitive query terms used during the previous six-month period.

NSA and FBI have adopted sensitive query policies, which require internal pre-approval of certain queries of raw Section 702 collection that have been deemed "sensitive." NSA's policy covers U.S. person query subjects whose work is understood to be integral to the exercise of the First Amendment and the protection of our democratic political system. FBI's policy is not specific to U.S. person queries, and applies to categories of queries that are similar to Sensitive Investigative Matters as described in the Attorney General Guidelines for Domestic FBI Operations and the FBI's Domestic Investigative and Operations Guide. Generally, however, both NSA's and FBI's policies require heightened review for queries involving elected officials and journalists. Senior-level pre-approval is required before such queries may be run.

We are encouraged that NSA and FBI have developed these sensitive query policies, albeit belatedly, and recommend that Congress require CIA and NCTC develop similarly specific, detailed policies. We further recommend that Congress require NSA, FBI, CIA, and NCTC coordinate with DOJ and ODNI on their sensitive query policies, and that consistency be achieved where practicable. These policies should include queries associated with protected First Amendment activities, including protests and other government criticism. These sensitive query policies should be submitted for approval by the FISC as part of the annual Section 702 certification process, and included in the agency querying procedures.

Finally, due to the nature of sensitive queries and their potential for abuse, we recommend that Congress require each element of the intelligence community authorized to query Section 702

data (FBI, NSA, CIA, and NCTC) to report to the relevant congressional committees, at least once every six months, all query terms that each agency used during the previous six-month period that were deemed to be sensitive under its policies. This independent oversight will guard against the improper use of queries that are or appear to be politically motivated, target a First Amendment-protected activity, or that may otherwise be utilized for an improper objective. The best branch to safeguard against political misuse is a political branch, accountable to the people—not a court with limited resources, appropriately focused only on legal issues, and operating largely out of the public eye.

Section 702 currently requires the Department of Justice and the DNI to assess the relevant intelligence agency's compliance with procedures and guidelines issued pursuant to Section 702 (including querying procedures) and to submit such assessments to the FISC and relevant congressional committees at least once every six months. This disclosure to Congress could be included in that Joint Assessment.

RECOMMENDATION 5: Strengthen Procedures Concerning Unmasking.

The Intelligence Community should adopt new rules to protect against the unmasking of U.S. persons for political purposes.

The Intelligence Community should ensure that unmasking of U.S. person identity information cannot be used to intrude upon the privacy or damage the reputation of U.S. persons for political purposes by adopting measures to protect from abuse the unmasking of presidential campaign associates and transition officials.

In a September 2020 report of the investigation into the 2016 presidential transition unmasking, United States Attorney John F. Bash recommended that, to strike the appropriate balance between preventing the abuse of intelligence reporting and ensuring that outgoing officials have the information needed to protect the United States, the Intelligence Community consider four prophylactic measures:

- Require centralized approval—possibly by the ODNI General Counsel and the Assistant Attorney General for the Department of Justice National Security Division—of all unmasking requests reasonably believed to be related to an associate of a presidential campaign or a transition official;

- Require a notification process, similar to those of the Gates procedures, under which the first Director of National Intelligence and Attorney General confirmed by the Senate after a new president takes office be notified of unmasking of any campaign associates or transition officials during preceding election and transition periods, and that the congressional notification requirements set forth in the ODNI's 2018 Intelligence

Community Guidance regarding requests for the identities of U.S. persons in disseminated intelligence reports be extend to campaign associates;

- Require all agencies that grant unmasking requests to maintain records of requests that appear to be related to campaign associates or transition officials;

- Adopt a more demanding standard for unmasking the personal identity information of presidential campaign associates or transition officials. For example, a requestor could be required to demonstrate a "substantial need" for the personal identity information.

To date, we are not aware that the Intelligence Community has undertaken any of these measures. We agree with the reforms recommended by the Bash Report. Protections should be enacted to ensure that appointees of an incumbent administration do not improperly obtain or misuse non-public information about individuals associated with a presidential campaign or transition team, and unmask U.S. person information for improper purposes. These sensible measures will guard against such misuse, make such misuse easier to detect, and help eliminate the appearance of political bias in unmasking U.S. person identities.

RECOMMENDATION 6: Enact Specific Penalties for Leakers of Section 702 Information.

Congress should enact a new criminal statute with significant penalties for those who leak protected Section 702 information concerning U.S. persons.

It is improper for a U.S. person's information, lawfully acquired for foreign intelligence purposes under Section 702, to be publicly leaked. Bona fide foreign intelligence collection should not be misused and leveraged to discredit political opponents, chill First Amendment-protected activity, or for any other improper purpose. Such leaks have the potential to cause reputational or career damage to the U.S. person whose information was improperly disclosed. They also undermine public trust in the intelligence community.

Currently, several overlapping statutory provisions criminalize unauthorized disclosures of protected government information.[142] None, however, specifically penalize leaks of U.S. person information acquired through Section 702. Many also require that the prosecution prove harm to national security as a result of the leak. These current authorities, therefore, fail to capture the very real injury that can occur not only to the country, but to the affected individual.

[142] A number provisions of federal law criminalize unlawful retention or disclosures of classified information and theft or conversion of government information, whether classified or not. For instance, the Espionage Act, 18 U.S.C. §§ 793-798 prohibits the transmittal of national defense information; 18 U.S.C. § 1924 prohibits a government employee from knowingly removing and retaining classified documents; and 18 U.S.C. § 641 prohibits the conversion of government property, regardless of classification.

In order to ensure and vindicate the privacy and civil liberties protections of U.S. persons whose information is collected under Section 702, Congress should fill this important gap by criminalizing the unauthorized disclosure of Section 702-acquired U.S. person information to an unauthorized recipient. Congress should make it illegal for any officer, employee, contractor or consultant of the United States government, without authorization, to willfully and knowingly disclose, to one not authorized to receive it, Section 702-acquired information that originated, is owned, or possessed by the U.S. government. Congress should impose appropriate fines and imprisonment.[143]

C. Increase the Value of the Program by Statutorily Authorizing the Use of the Program to Vet Applicants for Visas and High-Level Security Clearances

We are deeply concerned that under the current statutory framework of Section 702, the government may already have in its possession—but be legally unable to access—information that foreigners moving to the United States, or persons applying for U.S. government security clearances, present threats to national security. In our view, it is unacceptable that such information should have been lawfully collected, but rendered essentially unusable. Vetting is a crucial national security function, and Congress should make clear that Section 702 may be utilized to support it.

RECOMMENDATION 7: Amend Section 702 to Permit the Government to Query Its Holdings for Limited Vetting Purposes.

Congress should amend Section 702 to permit vetting, in limited circumstances, to be an exception to the querying standard, with applicant consent.

Congress should provide statutory clarification that Section 702-derived information may be used in the context of vetting—both for immigration purposes, and for individuals applying for high-level security clearances. Specifically, we recommend that Congress affirmatively authorize, with the consent of applicants, queries of U.S. persons as part of background investigations for U.S. government security clearances, as well as for vetting of non-U.S. person visa applicants seeking to enter the United States.

For most agencies, a query of unminimized Section 702-acquired information is permitted only where the search is "reasonably likely to retrieve foreign intelligence information."[144] As a result, the U.S. government may already have in its possession information that a visa applicant or

[143] Maximum penalties for violating other provisions that prohibit the disclosure of national defense information, classified information, or the theft of government property, range in severity from fines and imprisonment for one year to the death penalty.

[144] For the FBI, queries are also permitted to retrieve evidence of a crime.

person applying for a high-level security clearance poses a threat to national security. No one from our government might see this information, however, because our agents and analysts cannot run the relevant query in unminimized Section 702 collection unless they first have specific information tying a prospective visa or clearance applicant to foreign intelligence information or evidence of a crime.

The NSA's three-step process for "travel vetting" that the FISC has approved remains limited in certain key ways. The NSA also has not promulgated any similar querying procedures for applicants for U.S. government security clearances. It would therefore be useful for Congress to establish an exception to the querying standard, stating clearly that Section 702-acquired information is appropriately queried for these purposes. Permitting queries of unminimized Section 702-acquired information for these limited purposes would *not,* of course, entail targeting any additional persons, or collecting any additional information. It would merely allow the government to search for information already in its databases—communications with foreign targets abroad—and assess that information for a national security threat, before applicants are granted access—either to our country or to sensitive, classified information.

We therefore recommend that Congress authorize the above-described queries of Section 702-aquired information with a consent-based model. Specifically, Congress should permit such queries after the government first obtains the knowing and express consent of applicants. If implemented, this recommendation would help ensure that those individuals seeking to work and live in the United States, or those entrusted with our most sensitive national security information, would be thoroughly vetted against information already in the government's possession.