



SENATE JUDICIARY COMMITTEE
JOINT STATEMENT FOR THE RECORD

of

CHRIS FONZONE
GENERAL COUNSEL
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

GEORGE BARNES
DEPUTY DIRECTOR
NATIONAL SECURITY AGENCY

DAVID COHEN
DEPUTY DIRECTOR
CENTRAL INTELLIGENCE AGENCY

PAUL ABBATE
DEPUTY DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

and

MATTHEW OLSEN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

JUNE 13, 2023

(U) I. Introduction

(U) Chairman Durbin, Ranking Member Graham, distinguished members of the Committee, thank you for the opportunity to speak to you about Section 702 of the Foreign Intelligence Surveillance Act (FISA), the vital intelligence authority which, along with other FISA provisions, will expire at the end of this year unless Congress renews it.

(U) Section 702 authorizes the Intelligence Community to collect critical foreign intelligence information about foreign targets located outside the United States with the compelled assistance of U.S. communications service providers. In the fifteen years since its enactment, Section 702 has proven indispensable to U.S. national security. Every day it helps protect Americans from a host of new and emerging threats—such as terrorist plots, weapons of mass destruction, malicious cyber activity, and hostile state behavior from China and Russia.

(U) As described below, Section 702 is an elegant solution to an operational challenge created by the advent of the Internet and changes in the technology supporting international communications. It authorizes the Intelligence Community to collect vital intelligence overseas while requiring the Intelligence Community to comply with rigorous safeguards that protect the rights of Americans. It is a cornerstone of our Intelligence Community's efforts to identify and understand a broad range of challenges our country faces in an increasingly complex and dangerous world. And it remains a paradigmatic example of congressional leadership in national security. Without it, the United States and its allies and a partners would be less safe.

(U) Presidents of both parties have strongly supported it and attested to Section 702's importance to national security. Congress, recognizing Section 702's critical value and stringent protections, has three times voted on a bipartisan basis to authorize it, first in 2008, and then in 2012 and again in 2018. If Congress allows this authority to lapse, or renews it in a diminished form, the United States will lose access to critical intelligence about strategic national priorities and threats around the world.

(U) Section 702 is subject to robust privacy protections and oversight by all three branches of government. This structure enables the government to proactively identify, transparently disclose, and swiftly address compliance risks. For example, the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) recently imposed additional safeguards in response to compliance incidents related to procedures for accessing data lawfully collected through Section 702.

(U) This Committee plays an important role in overseeing this critical surveillance authority, and we stand ready to provide you with the information you need regarding the use of Section 702. The executive branch is committed to working with the Committee and the rest of the Congress on reforms to further enhance privacy protections while fully preserving the efficacy of this vital national security tool.

(U) Today we will illustrate the immense national security value of Section 702; describe its origin and legal structure; outline its compliance regime; and address concerns regarding privacy, particularly with respect to U.S. person queries of Section 702 data.

(U) II. The Value of Section 702 Collection

(U) Section 702 provides foreign intelligence information that is indispensable to protect the nation against national security threats. It has proved invaluable in protecting American lives and U.S. national security. There is no way to replicate Section 702's speed, reliability, specificity, and insight. In many cases, Section 702 is the sole source of our information about foreign threats to the United States and its people.

(U) Section 702 has been tremendously effective in combatting international terrorism, the dominant national security concern when Congress initially enacted the authority. In 2009, for example, Section 702 helped foil an active plot to bomb the New York City subway. National Security Agency (NSA) analysts relied on Section 702 to acquire the email communications of a suspected Al-Qa'ida courier in Pakistan and discovered a message sent by someone in the United States seeking advice about making explosives. The FBI identified that person as Najibullah Zazi and was able to disrupt his plot in time to save countless lives. Moreover, Section 702's value to the government's efforts to counter international terrorism continues to the present day. Just last year, in July 2022, Section 702 played an important role in the strike against Al-Qa'ida's leader, Ayman al-Zawahiri. Section 702 collection contributed significantly to our knowledge that al-Zawahiri was living in a safe house in downtown Kabul.

(U) Section 702's utility extends well beyond counterterrorism. It provides critical insights on some of the most urgent threats to U.S. national security.

- (U) 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 collection.

- (U) For example, Section 702 played an important role in the U.S. Government's response to the cyberattack on Colonial Pipeline attack in 2021. Using 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.

- (U) Section 702–acquired information related to sanctioned foreign adversaries was used in U.S. government efforts to stop components for weapons of mass destruction from reaching foreign actors.

- (U) Section 702 information has identified key economic security risks, including strategic malign investment by foreign actors in certain U.S. companies.

- (U) Section 702 collection has helped identify when hostile foreign intelligence services are trying to send their operatives into the United States to recruit spies here in the United States.

- (U) Finally, Section 702–acquired information revealed:
    - insights that have informed the U.S. government's understanding of the Chinese origins of a chemical used to synthesize fentanyl;
    - foreign actors' illicit plans to smuggle methamphetamine across the U.S. border;
    - 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; and
    - a foreign narcotics trafficker's purchase of a vast quantity of pills for transfer to the United States.

(U) Today, Section 702 not only helps defend and protect the United States but also helps advance U.S. foreign policy priorities around the world. For example:

- (U) Section 702 has helped uncover gruesome atrocities committed by Russia in Ukraine—including the murder of non-combatants, the forced relocation of children from Russian-occupied Ukraine to the Russian Federation, and the detention of refugees fleeing violence by Russian personnel. This and other information have helped the U.S. government to galvanize accountability efforts related to Ukraine by confidently and accurately speaking to the international community about Russia's atrocities.

- (U) Section 702 data helped expose efforts by foreign powers, including China, to coerce nations to oppose international responses to human rights violations. This reporting enabled U.S. diplomats to assist countries in shielding themselves from coercion and influence.

- (U) In 2021, Section 702 data enabled U.S. diplomats to demarche a Middle Eastern country over its efforts to monitor and track dissidents abroad, as well as dissidents here in the United States.

- (U) 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 US businesses, to generate revenue for its nuclear program.

(U) Section 702 plays a key role in advancing the missions of each of our agencies.

- (U) Central Intelligence Agency (CIA): At CIA, Section 702 collection enables missions against the full range of foreign intelligence priorities—including all adversarial nation states, counterproliferation, cyber, counterintelligence, counternarcotics, and counterterrorism—and is foundational to our analysis in support of policymakers. Section

702 collection illuminates actionable opportunities against foreign individuals and networks of intelligence concern more comprehensively than any other single data source; for example, Section 702 collection enabled over 70% of the successful weapons and counterproliferation disruptions supported by CIA from 2018 to2022. Section 702 has also been used in efforts to prevent U.S. technology being acquired by adversaries for their advanced weapons programs, and Section 702 supports CIA's ability to run safe human intelligence operations abroad and gain invaluable insight into human assets, the individuals who have put their lives on the line to work for the United States.

(U) Moreover, every day CIA analysts produce dozens of products to inform the President, Congress, and other senior officials within our government, and a sizeable proportion of the intelligence that goes into these products comes from Section 702 collection. To take one example, the WIRe—or the World Intelligence Review—is one of CIA's primary tools for disseminating intelligence electronically. CIA analysts cited at least one FISA Section 702 intelligence report in nearly 40% of WIRe products published over the past year. FISA Section 702–derived intelligence reports are published by several agencies, and they are most-often cited in WIRe products on some of our most critical intelligence targets.

(U) National Security Agency: Section 702 is essential to NSA's foreign signals intelligence (SIGINT) mission: Approximately 20% of NSA reporting in 2022 contained Section 702 information, and 702 also plays a significant role in enabling SIGINT collection under other authorities. Intelligence obtained from Section 702 has protected U.S. and allied forces, stopped significant terrorist plots, and prevented cyber-attacks. Section 702 also regularly provides NSA with insights into the strategic intentions of China, Russia, Iran, and North Korea. Across all of NSA's mission areas, this authority is an invaluable resource. 100% of the President's intelligence priorities topics reported on by NSA were supported by the Section 702. With Section 702, NSA's ability to provide intelligence on the most significant threats to our nation would be significantly diminished.

- (U) Federal Bureau of Investigation: Section 702 collection is critical to the FBI's ability to fulfill its unique role and responsibility in the Intelligence Community, which is focused on protecting the homeland, and Americans, from foreign threats. The FBI uses Section 702 across the entire range of its national security investigations: to go after foreign terrorist organizations seeking to conduct attacks within the U.S., counter foreign spies and proliferators, and get in front of increasingly sophisticated and prolific foreign cyber actors targeting Americans.

  (U) Section 702 is a particularly, and increasingly, important tool in the FBI's mission to protect the United States and its critical infrastructure from malicious foreign cyber activity. Its agility is especially important in a technology environment where those foreign cyber actors can move to new communication accounts and infrastructure in a matter of hours, if not minutes. Section 702 produces valuable insight the FBI uses to notify victims who often don't know they've been compromised, warn targeted entities

who are likely to be compromised next, and provide unclassified threat intelligence to help mitigate active or recent intrusions and prevent potential future incidents.

(U) Many of the most significant examples of the utility and importance of Section 702 remain classified by virtue of the need to protect intelligence sources and methods. While classified examples are available to this Committee, it is essential that the legislative and public discussion of these authorities be informed, to the extent possible, by concrete examples of its value. To that end, the Intelligence Community is working to declassify additional examples of the role Section 702 plays in defending the United States and its citizens.

(U) III. Overview of Section 702

(U) Origin of Section 702

(U) When Congress first passed FISA in 1978, it primarily intended for the law to regulate surveillance activities inside the United States. The advent of the Internet and changes in the technology supporting international communications led to significant unintended consequences in the operation of FISA. As a result of these technological changes, terrorists, hackers, spies, and other foreign intelligence targets abroad used communications services based in the United States, including those provided by U.S.-based Internet service providers (ISPs).

(U) Prior to the enactment of Section 702, when the Intelligence Community wanted to collect communications between, for example, two terrorism targets both located overseas who happened to be using a U.S.-based ISP, the government was required to obtain a court order under Title I or Title III of FISA ("traditional FISA") from the Foreign Intelligence Surveillance Court (FISC). A traditional FISA order requires that the government demonstrate probable cause that the target is a foreign power or an agent of a foreign power and, in the case of Title I orders, that the target is using or about to use the targeted facility, such as a telephone number or an e-mail account. Requiring individual court orders for intelligence collection aimed at non-U.S. persons abroad was both extraordinarily burdensome operationally and unnecessary legally, because the Supreme Court has held such individuals are not entitled to Fourth Amendment protections. Indeed, no other country is known to require individualized court orders to authorize intelligence activities targeting foreigners outside their borders.

(U) Requiring traditional FISA orders became operationally unsustainable in the years following the 9/11 terrorist attacks because of the increasing terrorist threats emanating from overseas to the United States and our allies. In 2008, against this backdrop, Congress enacted Section 702 as part of the FISA Amendments Act (FAA).[1] As mentioned above, Section 702 authorizes the

[1] (U) The FAA added several other provisions to FISA. Section 701 provides definitions for the Act. Section 703 allows the FISC to authorize an application targeting a U.S. person outside the United States where the acquisition is conducted in this country. Section 704 provides additional protections for collection activities directed against U.S. persons outside of the United States. Sections 703 and 704 require a finding by the FISC that there is probable cause that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Section 705 allows the government to obtain various authorities simultaneously. Section 708 clarifies that nothing in

government, with the approval and oversight of the FISC on a programmatic basis, to compel the assistance of providers in the United States in obtaining communications of non-U.S. persons located outside the United States to acquire foreign intelligence information. It allows the government to target for collection *only* foreign targets located overseas that are reasonably assessed to have foreign intelligence information.

(U) The statute also provides for comprehensive oversight by all three branches of government. This ensures the information collected about non-U.S. persons overseas is used responsibly and protects the constitutional and privacy interests of Americans whose information may be incidentally acquired when collecting foreigners' communications.

(U) Legal Structure

(U) Under Section 702, the FISC approves annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that specify classified categories of foreign intelligence that the government is authorized to acquire pursuant to the authority. The certifications serve as the legal basis for targeting specific non-U.S. persons outside the United States. Based on the certifications, the Attorney General and the DNI can direct U.S. communications service providers to assist in collection against authorized Section 702 targets. The FISC also reviews and approves the agencies' targeting, minimization, and querying procedures on an annual basis.

(U) Multiple provisions ensure that targeting is properly aimed at non-U.S. persons located outside the United States who are likely to possess, receive, or communicate foreign intelligence information that falls within one of the specified categories. First, the law requires the Attorney General and the DNI to certify that a significant purpose of an acquisition is to obtain foreign intelligence information. Second, only non-U.S. persons may be targeted. Third, the government may not target any person known at the time of the acquisition to be located in the United States at that time, regardless of whether they are a U.S. person. Fourth, the government may not target someone outside the United States for the purpose of targeting a particular known U.S. person or anyone in this country ("reverse targeting"). Fifth, Section 702 protects domestic communications by prohibiting the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States. Finally, of course, any collection must be consistent with the Fourth Amendment.

(U) Targeting and Acquisition

(U) An agency requesting authority under Section 702 must propose for court approval detailed procedures to ensure that it targets only non-U.S. persons outside the United States and also that it does not intentionally acquire domestic communications.

(U) The National Security Agency (NSA) initiates all Section 702 collection. NSA's targeting procedures require that there be an appropriate foreign intelligence purpose for the acquisition and that a "selector" associated with a particular target—like a phone number or e-mail

---

the FAA is intended to limit the government's ability to obtain authorizations under other parts of FISA. All provisions added by the FAA would expire if Section 702 is not reauthorized.

address—be used by a non-U.S. person reasonably believed to be located outside the United States. An analyst must conduct due diligence to identify information in the NSA's possession that may bear on the location or citizenship status of the potential target. NSA's basis for obtaining communications associated with a particular selector must be documented, and DOJ reviews the documentation for every selector.

(U) Under Section 702, each target is approved for tasking based on an individualized determination. The Intelligence Community has reported that approximately 246,073 targets were authorized for collection under the Section 702 program in 2022.

(U) FBI and CIA do not initiate Section 702 collection but may nominate selectors to NSA for collection.[2] FBI, CIA, and NCTC also do *not* receive all Section 702 collections, but only a small fraction relevant to their respective missions. For example, FBI may receive information only as to those Section 702 targets that the FBI determines are relevant to a full, predicated FBI national security investigation. As of 2022, that amounted to approximately 3.2% of all Section 702 targets.

(U) Minimization, Querying, Dissemination, and Use

(U) Under the statute, each agency must have its own minimization procedures. These impose strict controls with respect to all acquired data, regardless of the nationality of the individual to whom the data pertains. All personnel who are granted access to Section 702 information are required to receive training on the minimization procedures. The minimization procedures specify the duration of time for which data can be retained.[3]

(U) Since 2018, the statute has required the government to have separate procedures governing queries, which had previously been addressed as part of minimization procedures. Queries do not result in any additional collection. Rather, they allow an agency to quickly and effectively locate foreign intelligence information within what the agency collected previously through the use of Section 702. The query procedures limit the ways in which personnel can query Section 702 data using a term that is associated with a U.S. person, such as a name or telephone number. As discussed further below, U.S. person queries of Section 702 collection help us detect and evaluate connections between lawfully targeted non-United States persons involved in terrorist plots, cyber attacks, and other national security threats and U.S. persons.

(U) Queries are subject to a three-part standard. First, the query must have an authorized purpose: to obtain foreign intelligence information, or, only in the case of the FBI, to obtain evidence of a crime. Second, the query must be reasonably designed for that purpose. And third, there must be a specific factual basis to believe the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime. As described below, the Intelligence Community

[2] (U) NCTC does not initiate Section 702 collection or nominate selectors to NSA for collection.

[3] (U) In cases in which, despite the government's initial reasonable belief to the contrary, a target is found to be located in the United States or is discovered to be a U.S. person, the procedures require the collected data to be purged, except in the limited circumstance whereby, for example, the Director of the NSA determines that the collection contains significant foreign intelligence information.

and DOJ in recent years have taken steps to impose additional privacy safeguards surrounding querying of Section 702 data.

(U) There are also additional controls on the dissemination and use of Section 702–acquired information. An agency is permitted to disseminate information identifying a U.S. person to other entities only under the limited exceptions in the minimization procedures, for example, when such information is foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime. The statute dictates that all FISA-acquired information, including Section 702 information, may be used in a criminal proceeding only with the approval of the Attorney General. Additionally, the government must give notice to individuals if the government intends to use information against them that is either obtained or derived from Section 702. The statute also prohibits the use in a criminal proceeding of any communication to or from, or information about, a U.S. person acquired under Section 702, except for crimes involving national security or in a limited set of additional enumerated serious crimes.[4]

(U) IV. Privacy Protections: Compliance, Oversight, and Transparency

(U) The government is committed to ensuring that the Intelligence Community's use of Section 702 is consistent with the law, complies with FISC orders, and protects the privacy and civil liberties of Americans. By approving the annual certifications, as well as the targeting, minimization, and querying procedures, the FISC plays a central role in ensuring that Section 702 activities are conducted lawfully—consistent with statutory and constitutional requirements. The FISC may require the government to provide additional filings and testimony at hearings to ensure that the court has a full understanding of the operation of the program. In addition, on multiple occasions, the FISC has appointed amici curiae to address Section 702–related legal questions. In the annual evaluation of whether a proposed certification meets all statutory and constitutional requirements, the FISC makes findings regarding the operation of the program and the government's compliance record.

(U) Internal components in each agency with access to Section 702 information, including Inspectors General, oversee activities conducted under the authority. All Section 702 targeting decisions made by NSA are reviewed at least three times—by the drafting analyst, the more senior analyst, and a specifically trained adjudicator—prior to tasking and are further reviewed by NSA compliance personnel and DOJ National Security Division (NSD) personnel after tasking. CIA and FBI require multiple layers of review before nominating selectors to NSA for tasking to Section 702. NSA, CIA, and FBI require that all personnel who nominate selectors for

[4] (U) Other than national security crimes, FISA information may be used in criminal proceedings involving death, kidnapping, serious bodily injury as defined in section 1365 of Title 18, conduct that constitutes a criminal offense against a minor as specified in section 11 of the Adam Walsh Child Protection and Safety Act of 2006, incapacitation or destruction of critical infrastructure, cybersecurity, transnational crime, including transnational narcotics trafficking and transnational organized crime, and human trafficking.

tasking under Section 702 or task selectors complete training on targeting, minimization, and querying procedures, as well as on other agency policies.[5]

(U) DOJ personnel routinely review the agencies' targeting, querying, minimization, and dissemination decisions. This oversight includes DOJ's review of all tasking decisions by NSA and reviews at least once every two months at NSA, FBI, CIA, and NCTC to assess each agency's compliance with its legal procedures. In addition, agencies conducting activities under Section 702 must report promptly to DOJ and to ODNI incidents of noncompliance with the targeting, querying, or minimization procedures. NSD attorneys investigate each potential instance of non-compliance and work with the agencies to remediate any such instances. NSD reports any incident of noncompliance with the statute, court orders, or the approved legal procedures to the FISC and to Congress.

(U) As required by FISA, NSD submits reports regarding the government's use of Section 702 to the congressional intelligence and judiciary committees at least every six months. These semiannual reports are also provided to the FISC and include a description of every identified Section 702 compliance incident in the reporting period. NSD and ODNI also prepare semiannual joint assessments focused on compliance incidents impacting U.S. persons, compliance trends, and remedial measures. The joint assessments are provided to both Congress and the FISC. The FISA statute also requires the government to provide Congress with any pleading, FISC opinion, or order that contains a significant interpretation of the law.

(U) The Intelligence Community and DOJ work to be as transparent as possible with the public regarding the operation of the Section 702 program, consistent with the need to protect sources and methods. We have declassified and released FISC opinions regarding the authorization and operation of the Section 702 program. DOJ has provided to Congress every Section 702 opinion the FISC has issued to date. In addition, by statute, DOJ is required to produce to Congress any FISC opinion that includes a significant construction or interpretation of any provision of law or a novel application of any provision of FISA. Relatedly, the DNI, in consultation with the Attorney General, is required to publicly release such opinions containing a significant construction or interpretation of any provision of law.

(U) V. Query Compliance and Remedial Measures

(U) In recent years, a key oversight focus has been on queries of Section 702 information, in particular those involving U.S. person identifiers. As explained above, a query involves using a term to retrieve specific information from an agency's database of previously collected information. In other words, queries do not return newly collected data but merely retrieve lawfully collected data that is already stored in agency computer systems.

[5] (U) NCTC does not nominate or task selectors but instead receives a limited amount of counterterrorism information acquired pursuant to Section 702. Similar to the other agencies, NCTC is subject to specific minimization and querying procedures and requires all personnel with access to Section 702 information to complete annual training.

(U) Queries using U.S. person identifiers, such as a name or e-mail address, are critical to protecting U.S. national security. These queries can identify links between foreign threats and those inside the United States, including those related to terrorism, malicious cyber threats, hostile nation state activity, or other threats to the American people. U.S. person queries are especially important at the early stages of a national security investigation. They can help the government learn critical information needed to protect U.S. victims of malicious foreign adversaries, and they can help the U.S. government learn more about significant threats by foreign surveillance targets in contact with U.S. persons.

(U) This is particularly true for the FBI, which is responsible for protecting the homeland from national security threats emanating from overseas. In many cases, the FBI conducts U.S. person queries to identify U.S. person victims of foreign hacking or spying to enable the agency to warn and protect those individuals. These queries are vital to the ability to protect Americans from terrorism and from escalating cyber and espionage threats. To name but a few examples:

- (U) The FBI 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 the FBI's disruption of the plots.

- (U) Through U.S. person queries of Section 702-acquired information, 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 they could take action to protect them and help secure their accounts.

(U) Just as this tool is critical to protecting the nation, it is vital that the government maintain the trust and confidence of Congress, the courts, and the American public in its use of Section 702 information. In recent years, oversight by DOJ and ODNI has identified serious compliance issues in the FBI's queries of FISA collection for information about U.S. persons. These incidents were reported promptly to the FISC and Congress, and they are described in detail in court opinions that are now public.

(U) The most recent such opinion, which was issued in spring of 2022 and declassified in May 2023, reflects a number of serious incidents of non-compliance, including improper queries of Americans involved in peaceful protests. These incidents are unacceptable. The FBI, the DOJ, and the entire Intelligence Community are committed to addressing them completely, including by implementing stronger safeguards and accountability mechanisms. All these incidents predated a set of significant reforms undertaken by the FBI beginning in the summer of 2021, which are discussed below and were designed to address the root causes of these incidents and prevent similar errors from occurring again.

(U) In 2021 and 2022, FBI worked with DOJ and ODNI to institute remedial measures that have since significantly strengthened compliance. These measures include:

- (U) Requiring FBI Personnel to "Opt-In" to Query Unminimized Section 702 Information: In June 2021, the FBI changed the default settings in the systems where it

stores unminimized Section 702 information so that FBI personnel with access to unminimized FISA Section 702 information need to affirmatively "opt-in" to querying such information. This system change was designed to address the large number of inadvertent queries of unminimized Section 702 information DOJ had identified in its reviews, in which FBI personnel did not realize their queries would run against such collection.

- (U) Heightened Approvals on Large Batch Job FISA Queries: Also in June 2021, the FBI instituted a policy requiring FBI attorney approval prior to conducting a "batch job" that would result in 100 or more queries. The term "batch job" refers to a capability in one of the FBI's systems that allows FBI personnel to more efficiently run queries involving multiple query terms. Attorney preapproval is aimed at providing additional review in situations where one incorrect decision could potentially have a greater privacy impact due to the large number of query terms.

- (U) Supplemental Guidance and Mandatory Training on Query Requirements: In November 2021, DOJ, ODNI, and the FBI issued new comprehensive guidance to all FBI FISA users on the proper application of the query rules, and in December 2021, the FBI instituted new mandatory training on that guidance, which personnel were required to complete by the end of January 2022. The FBI expanded and updated this training at the end of 2022. On an annual basis, all FBI personnel with access to unminimized FISA information are required to complete the expanded and updated query training or lose access to FISA systems.

- (U) Requirement for Case-Specific Justifications for U.S. Person Query Terms in FBI Systems: In the fall of 2021, at the direction of the FISC, the FBI modified its systems containing unminimized Section 702 information to require a case-specific justification for every query using a U.S. person query term before accessing any content retrieved by such a query from unminimized Section 702 information. Previously, personnel were permitted to use a pre-populated common justification, when applicable, for the query. These case-specific justifications are subject to review and audit by DOJ as part of its regular oversight reviews.

- (U) New Restrictions and Oversight of Sensitive Queries: In March 2022, the FBI instituted a new policy requiring enhanced preapproval requirements for certain "sensitive" queries, such as those involving elected officials, members of the media, members of academia, or religious figures. Under the new policy, an FBI attorney must review these queries before they are conducted. The FBI's Deputy Director must also *personally approve* certain queries before they can be conducted. This measure was designed to ensure that there is additional review at a leadership level of queries that reflect particular investigative sensitivities.

(U) These initial remedial measures are already achieving significant compliance benefits and

protecting privacy. For example, the number of U.S. person queries FBI conducted in 2022 was approximately 200,000, more than a 93% decrease from the previous year. Further, the FBI's Office of Internal Auditing—established at the direction of former Attorney General Barr to audit the FBI's use of its national security authorities—found an increase in the FBI's rate of compliance with the FISA query standard from 82% before these measures were instituted to 96% after their implementation.

(U) Implementation of robust privacy protections is not a one-time solution but rather an ongoing and iterative process involving repeated review and evaluation. DOJ and the FBI are continuing to develop additional measures to enhance privacy protections and ensure personnel comply with existing policies.

(U) Compliance reviews conducted by DOJ and ODNI have found that deliberate misconduct with respect to Section 702 information is extremely rare. In those rare cases of intentional misconduct, the individuals involved are referred for investigation and appropriate action—up to and including suspension, revocation of security clearance, or termination. By contrast, the vast majority of the compliance issues that prompted DOJ and FBI's remedial measures were the result of FBI personnel misunderstanding the rules governing U.S. person queries. For example, in some other instances, FBI personnel queried raw Section 702 information inadvertently, without realizing that the Section 702 dataset was included in the query as a default. However, DOJ and FBI are committed to addressing these unintentional errors, and the remedial measures described earlier are designed to do so; DOJ and FBI are also working to implement additional measures to ensure compliance.

(U) VI. Potential Reforms to Section 702

(U) The Administration is committed to working with Congress to address concerns regarding the use of Section702 and to identify reforms to enhance privacy and civil liberties protections while fully preserving Section 702's efficacy.

(U) As discussed above, the FBI has imposed a number of remedial measures, the codification of which could serve as the starting point for additional statutory reforms. This would entrench these policies into law, making them hard to undo. The Executive Branch is committed to working with this Committee and the Congress to explore potential additional changes to enhance the authority and its associated privacy, oversight, and transparency functions.

(U) However, it is essential that we pursue reforms that do not impair the benefits of Section 702; doing otherwise would imperil U.S. national security. In particular, more sweeping proposals—such as prohibiting U.S. person queries, imposing a warrant requirement for all such queries, or barring the FBI from receiving Section 702 collection—would force the government to turn a blind eye to threat information that it had lawfully acquired, with potentially grave consequences to our nation's security.

(U) But there is no need to go down that path. Other reforms would meaningfully enhance Section 702 safeguards while also continuing to preserve its national security benefits. We look

forward to continuing to work with this Committee and others in the Congress regarding such proposals.

(U) VII. Conclusion

(U) Section 702 is an indispensable foreign intelligence tool that allows our Intelligence Community to target non-U.S. persons located outside the United States to acquire information critical to our national security. Courts have repeatedly found that Section 702 is consistent with the Constitution and upholds the rights of Americans. Section 702 operates under stringent procedures and is subject to oversight from all three branches of government. In a world in which digital authoritarianism and technological repression are on the rise, Section 702 is a model for democratic countries to conduct intelligence activities consistent with the rule of law.

(U) The government recognizes the enormous responsibility it has to use this tool responsibly, protect the privacy and civil liberties of U.S. persons, and uphold the trust and confidence placed in the law enforcement and intelligence community. We are committed to addressing mistakes, being transparent with you and the American people, and continually reinforcing a system and culture that protects Americans' privacy and civil liberties. We look forward to working with this Committee on reauthorization of this critical tool that advances our shared goal of protecting the United States.