President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations for Reauthorization

JULY 2023

THE WHITE HOUSE
WASHINGTON

Assistant to the President for National Security Affairs (APNSA) Jake Sullivan, on behalf of the President of the United States, requested that the President's Intelligence Advisory Board (PIAB) and the Intelligence Oversight Board (IOB) undertake an inquiry to assess the effectiveness of Section 702 of the Foreign Intelligence Surveillance Act and to provide a set of policy and legislative recommendations for the President's consideration.

The PIAB, and its component IOB, is an independent element comprised of volunteer citizens who operate within the Executive Office of the President. The PIAB has the authority to access all information it needs to perform its functions. For more than six decades, the PIAB has existed exclusively to assist the President by providing advice on the effectiveness of the Intelligence Community in meeting the nation's intelligence needs.

The IOB is a subset of the PIAB that monitors the Intelligence Community's compliance with the Constitution and all applicable laws, Executive Orders, and Presidential Directives. It complements the oversight roles of the Director of National Intelligence, Department and Agency Inspectors General, and Congressional Oversight Committees. The IOB has no enforcement or sanction authority.

In preparing this report, the Boards assessed the effectiveness of collection under Section 702; the value of being able to conduct U.S. person queries within Section 702-acquired information and the national security implications of restricting such queries, such as by requiring a warrant; and the overall efficacy of oversight of the Section 702 program.

The Boards considered findings resulting from interviews and document reviews and agreed upon 13 recommendations for the President. The Boards issued a single report addressing each aspect of this inquiry. The majority of the report is written at the unclassified level as much of the data on Section 702 noncompliance and on oversight measures are unclassified. Certain classified portions of the report were declassified by the Intelligence Community and others remain redacted in order to protect national security. The resulting reports consists of the Boards' findings and recommendations, followed by appendices addressing the Section 702 program in more detail.

Board members include: Chair, James Winnefeld, Admiral, USN (ret.); Vice Chair, Dr. Margaret Hamburg; Former Secretary Janet Napolitano; Former Senator Evan Bayh; Mark Angelson; Jeremy Bash; Dr. Kim Cobb; Blair Effron; Anne Finucane; Hamilton James; Gilman Louie; Julia Santucci; and, Dr. Kneeland Youngblood.

★ ★ ★ ★ ★ ★

Table of Contents

[redacted]

(U) Executive Summary

(U) Two thousand nine hundred and seventy-seven people died in the terrorist attacks of September 11, 2001. In its investigation, the 9/11 Commission found that the attacks "fell into the void between the foreign and domestic threats..... No one was looking for a foreign threat to domestic targets." Prior to this event, the intelligence community struggled to retrieve and share pertinent information that was being communicated among terrorists using the rapidly evolving technology of the internet and cell phones. Such foreign threat information, had it been identified in a timely manner, could have helped prevent this tragedy.

(U) In order to address this failure, Congress enacted several changes to the nation's intelligence laws over the ensuing years, to include Section 702 of the Foreign Intelligence Surveillance Act (FISA). Originally passed in 2008, Section 702 authorizes the intelligence community to acquire *foreign intelligence information* of *non-U.S. persons* reasonably believed to be *outside the United States*. The Act also allows for the subsequent review and query of these lawfully-collected communications of foreign targets, including incidentally-collected communications with or about U.S. persons, which are necessary in order to rapidly determine whether a U.S. person is either at risk of being a victim of, or is involved in, nefarious foreign activity. Section 702 cannot be used to target U.S. person communications. In cases where the intent is to directly collect a U.S. person's communications rather than reviewing information that has already been lawfully collected, a warrant or court order is already required under other legal processes.

[redacted] Four intelligence agencies have access to unminimized Section 702-acquired information: the National Security Agency (NSA), Central Intelligence Agency (CIA), National Counterterrorism Center (NCTC), and Federal Bureau of Investigation (FBI). *Section 702 has been a vital, foundational intelligence tool upon which a myriad of other foreign intelligence efforts depends.* It has been instrumental in its first 15 years in preventing several potential high-impact events. The intelligence community used Section 702 information to avert the 2009 attempted New York City subway bombing, the 2010 attempted vehicle bombing at a Portland Christmas tree lighting ceremony, [redacted], cyber attacks against critical U.S. infrastructure, and the smuggling of fentanyl into the United States. Section 702 information also underpins a significant portion of the intelligence production that the government uses to inform decision-makers on topics such as [redacted], international terrorist networks and activities, adversary efforts to procure advanced military technologies, and national security threats to the United States and its allies posed by the People's Republic of China and Russia.

(U) Unfortunately, complacency, a lack of proper procedures, and the sheer volume of Section

[redacted]

[redacted]

702 activity led to FBI's inappropriate use of Section 702 authorities, specifically U.S. person queries. The Board, however, found no evidence of willful misuse of these authorities by FBI for political purposes. To date, the Department of Justice (DOJ) has only identified three incidents of intentional misconduct from among millions of FBI queries of Section 702 information and FBI has addressed the incidents appropriately.

(U) Because of these incidents of noncompliance, the ongoing Congressional debate on the efficacy of Section 702 is the first time since 2008 that its reauthorization may be in jeopardy. After careful review, the Board strongly believes that Section 702 authorities are crucial to national security and do not threaten civil liberties, so long as the requisite culture, processes, and oversight are in place.

(U) Accordingly, *the Board proposes several important areas for reform that we believe would have minimal negative impact on national security, while increasing the public's confidence in Section 702*. These recommendations include measures that would establish a common standard for U.S. person queries across all agencies, improve FBI's internal compliance regime, streamline FBI Section 702 authorities, engender a single culture of compliance across the intelligence community, further strengthen the program's already robust overall oversight framework, codify policies in statute, and enhance transparency with the public.

(U) *Implementing the Board's recommendations and outlining a revitalized system to Congress and the public should restore much-needed faith in these authorities and enable their reauthorization.* The cost of failure is real. If Congress fails to reauthorize Section 702, history may judge the lapse of Section 702 authorities as one of the worst intelligence failures of our time.

[redacted]

[redacted]

(U) Findings

(U) You directed this Board to assess the following three aspects of the Section 702 program, in addition to recommending policy or legislative reforms:

- (U) The effectiveness of collection under Section 702;
- (U) The effectiveness of oversight under Section 702; and
- (U) The value of conducting U.S. person queries and the national security implications of restricting such queries, such as by requiring a warrant.

(U) This report is the product of reviews of relevant classified and unclassified literature, and interviews of representatives from the intelligence community, the oversight community, and civil society.

(U) Effectiveness of Collection

(U) Section 702 is one of the intelligence community's most effective and powerful tools. As a world leader in telecommunications, U.S. telecommunications services are ubiquitous, and the intelligence community can leverage this national advantage to collect foreign intelligence information by lawful, court-approved methods in order to protect America from its adversaries and support foreign policy decisions that help advance America's standing in the world.

[redacted] Examples of Section 702 successes abound: [redacted]; locating prominent international terrorists; identifying threats to U.S. troops; and enabling the seizure of numerous fentanyl pills, powder, precursor chemicals, and production equipment. The real value of the Section 702 program, however, cannot be captured solely in pithy vignettes. Section 702 forms the cornerstone of the intelligence community's ability to uncover and track threats to America because it is an integral signals intelligence capability. Signals intelligence forms the bedrock of intelligence collection, and in calendar year 2022, 59% of PDB articles contained Section 702 information reported by the NSA. It is no exaggeration to state that signals intelligence, made possible by Section 702 information, is likely to inform every substantial national security decision our leaders make, now and in the future.

(U) Effectiveness of Compliance and Oversight

(U) In general, the current Section 702 oversight framework is expansive, and DOJ, in particular, has been effective in detecting noncompliance and reporting it to the Foreign Intelligence

[redacted]

[redacted]

Surveillance Court (FISC) and Congress. Oversight entities, including the FISC, DOJ, and the Office of the Director of National Intelligence (ODNI), report that over the last several years, most compliance incidents have been attributable to FBI's pervasive lack of understanding regarding query standards.

(U) The Board assesses that this lack of understanding led to a lack of rigor, an abundance of complacency about the proper use of Section 702 authorities, and a lack of urgency to comply. The Board further found issues with inappropriate configuration settings in FBI's system that houses Section 702 data, inadequate internal compliance controls, and a lack of proper internal auditing measures. The result was a high volume of noncompliant U.S. person queries over the years by FBI.

(U) While we found no instances of FBI personnel willfully using Section 702 for political purposes, and intentional misconduct of FBI querying for any reason was exceedingly rare, FBI's conduct has nevertheless undermined public confidence in its ability to use Section 702 in the way it was intended.

(U) While DOJ's external oversight of FBI is extensive, FBI's large volume of U.S. person queries and limited DOJ personnel capacity have prevented DOJ from reviewing 100 percent of FBI's queries. Further complicating matters, DOJ's stand-down of in-person oversight reviews due to COVID delayed DOJ from discovering that mandatory training instituted in the fall of 2019 was not effective in addressing FBI's query compliance issues. Upon DOJ's resumption of in-person oversight reviews, DOJ helped FBI institute additional remedial measures in 2021. Despite COVID-related obstacles and the inability to conduct a 100 percent review of FBI queries, this oversight mechanism detected the problem and brought it to light—as oversight should.

(U) In attempting to optimize its limited capacity for oversight of FBI's U.S. person queries, DOJ conducted an FBI-wide audit in 2021 that focused on sensitive queries and queries conducted during the time period of a high-profile event in order to confirm whether FBI personnel properly followed procedures. Through this audit, DOJ found a large number of noncompliant incidents (although the number of noncompliant incidents amounted to a small percentage of noncompliance during this period of time due to the high volume of queries overall). Some of these noncompliant queries included individuals arrested during the January 6 Capitol breach. DOJ subsequently directed FBI to undertake reforms to address its compliance issues.

(U) While FBI has put in place reforms since 2021 that have led to significant improvements in compliance noted by DOJ and ODNI, the Board deems them insufficient to ensure compliance

[redacted]

[redacted]

and earn the public's trust. There is both a need and an opportunity for FBI to strengthen its internal compliance regime.

(U) U.S. Person Queries

[redacted] Intelligence agencies are focused on understanding foreign threats to U.S. interests. *Without U.S. person queries, the government would be far less capable of identifying potentially harmful links between foreign threats and U.S. persons.* U.S. person queries are necessary in order to identify foreign threats to the homeland. Query terms can be keywords or identifiers such as names of individual people or businesses, e-mail addresses, phone numbers, [redacted], or any other attributes designed to retrieve information from Section 702-acquired information. When one of the terms used to conduct the query identifies a U.S. person or is designed to return information about a specific U.S. person, that query constitutes a U.S. person query. These queries reveal how, when, and where a foreign actor could harm a U.S. person, or co-opt a U.S. person as an accomplice. Queries provide a method by which an intelligence officer or agent can effectively sort data *already lawfully collected*; they do not collect any new data.

[redacted] There are two types of queries: "metadata" queries (which involve the dialing, routing, addressing, or signaling information associated with a communication, but do not include the contents) and "content" queries (which involve the content of communications that were lawfully collected). CIA's, NCTC's, and NSA's U.S. person content queries each constitute a small percentage of their overall queries in the portions of the Section 702 data to which they have access, although these U.S. person queries constitute thousands of queries per year overall. More than 60 percent of NSA's U.S. person query terms are not associated with individual people, but are other entities, such as companies or non-governmental organizations, [redacted], including those associated with critical infrastructure nodes.

(U) With the exception of a series of particularly large batch queries in 2021, FBI's U.S. person content queries account for a quarter to a third of its overall queries. Due to this series of batch queries of presumed U.S. person identifiers in 2021 to identify potential U.S. victims related to one particular cybersecurity investigation, FBI's U.S. person queries in 2021 constituted more than half of its overall queries that year. In light of FBI's domestic mission, its larger percentage of U.S. person queries, compared to other intelligence agencies, is expected.

(U) Warrant Implications

(U) A requirement that an intelligence agency should obtain a warrant or court order prior to

[redacted]

[redacted]

every U.S. person query of Section 702-acquired information would prevent intelligence agencies from discovering threats to the homeland. Importantly, a U.S. person query does not generate new collection on a U.S. person—it is a query conducted within the already lawfully collected communications of foreign intelligence targets. Moreover, except in limited circumstances, a U.S. person query is only permitted when it is reasonably likely to retrieve foreign intelligence information or—in the case of FBI—evidence of a non-national-security-related crime. Therefore, a U.S. person query is the act of purposefully filtering data already collected. A U.S. person query serves as a preliminary exploratory tool to retrieve the most basic data needed to determine whether there is either a threat to a U.S. person or the nefarious involvement of a U.S. person. Once the U.S. person is determined to be involved in a foreign intelligence threat and the government intends to look into the U.S. person, a warrant under other legal processes is required for new collection specifically targeting the U.S. person. A warrant is obtained at the appropriate stage of an investigation. Section 702 queries do not constitute searches, and no court has ever held that a warrant is required for a U.S. person query of information collected under Section 702. Getting a warrant, or any other court order, prior to each U.S. person query conducted by an authorized user of an intelligence agency is not only impractical because there would be too many requests to process, preventing intelligence agencies from detecting threats in a timely manner, it is unjustified. Often, there is not enough information to prove probable cause when a U.S. person query is being conducted—it likely cannot be determined at that point whether the U.S. person is a potential victim or perpetrator involved in a foreign threat to the United States. Moreover, a U.S. person query could retrieve results involving two non-U.S. persons communicating about a U.S. person (rather than communications to or from a U.S. person) which has less implications for U.S. person privacy.

(U) The FBI

(U) The intelligence functions carried out at FBI, which focus on threats to the homeland, cannot be replicated elsewhere in the intelligence community. CIA, NSA, and NCTC properly lack the mission and authority to focus domestically, so eliminating—or even severely constraining—FBI's ability to access Section 702 information for intelligence purposes would make America significantly less safe. FBI must have the tools it needs to do its job, but given FBI's compliance record with respect to its queries of FISA data, there is no question that reforms are needed.

(U) Even though the culture, processes, and resources at FBI do not engender a complete compliance regime, FBI is not lackadaisical in its attitude toward handling sensitive information. FBI receives more than 4,000 tips and leads a day from state and local law enforcement, private companies, intelligence agency partners, foreign governments, and the public. FBI is obligated to pursue all legitimate leads and will often turn to the more than 100 databases of which they

[redacted]

[redacted]

have access, including Section 702, as its first resort, because such checks are considered one of the least intrusive investigative methods the FBI can use. Outside of the national security context, it is commonplace for law enforcement entities at federal, state, and local levels alike to query lawfully-collected information of many different types. No courts require law enforcement entities to obtain warrants to conduct these routine checks. Similarly, the FBI system for running checks is designed to be able to search all of FBI's data repositories, to include Section 702 data, at once. This approach is a direct result of a recommendation from the 2012 Webster Commission's independent investigation into FBI's handling of the 2009 Fort Hood shooting. FBI has been forward-leaning in its mission, changing its practices when directed.

(U) The fact that FBI is involved in the Section 702 program ensures that there is no "gap" between foreign-focused collection and domestic disruption efforts, and that there is no "wall" between its law enforcement and intelligence functions. This was one of the most critical lessons learned after the attacks of September 11 and again after the Fort Hood shooting. The Board believes that FBI can continue to fill this "gap" by exercising the same Section 702 authority used by other intelligence agencies—*for the purposes of foreign intelligence information only*. FBI is the only agency authorized to query Section 702 data for evidence of a non-national security crime (including crimes unrelated to foreign intelligence). Because the purpose of Section 702 is the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information, FBI should be able to restrict its use of Section 702 to its originally-intended objective of identifying foreign intelligence information with minimal risk to its intelligence mission.

(U) Transparency

(U) The Board found that although the Section 702 program is likely to be the most open and publicly-debated surveillance program in the world, extensive misunderstandings about Section 702 persist. The government must communicate more effectively with the public regarding the foreign intelligence threats we face today. Only then can the public more accurately judge the importance of Section 702 in mitigating those threats. One area in which the government can be more transparent is by declassifying the certifications specifying the categories of authorized collection under Section 702. This would allow the public to understand how the government defines the most urgent foreign threats. Separately, the addition of a counternarcotics certification, in particular, would allow the intelligence community to collect more intelligence information about fentanyl threats under Section 702 and to become more effective in supporting the government in its fight against fentanyl. As with the other certifications, the Board recommends that the existence of this category of collection be made public, should it be

[redacted]

[redacted]

authorized.

(U) Another area that has led to misgivings is the government's inability to estimate the amount of incidental U.S. person collection that occurs under Section 702. The Board considered how NSA could be compelled to produce an estimate. We believe that because any effort to do so would involve manually scrutinizing each e-mail address within the data set, the process of counting such collection itself would unduly violate the privacy and civil liberties of U.S. persons. Nonetheless, the Board believes that NSA would increase transparency on this subject if it engaged publicly with experts to examine this question. NSA could also put forth a good faith effort to pursue other metrics to characterize the scale of incidental U.S. person collection.

[redacted]

[redacted]

(U) Recommendations

(U) Based on our research and analysis, we offer you the following recommendations.

(U) **1. Direct the Attorney General to remove FBI's authority to conduct queries for evidence of a non-national security-related crime in its Section 702 data**. FBI's use of Section 702 should be limited to foreign intelligence purposes only and FBI personnel should receive additional training on what foreign intelligence entails. In the event that FBI encounters evidence of a non-national security-related crime while reviewing Section 702 data, existing intelligence community procedures for handling evidence of such crimes uncovered in the course of reviewing intelligence information should be applied.

(U) **2. Direct the DNI and the Attorney General to establish a more rigorous pre-approval standard that is consistent across all agencies for U.S. person content queries.**

(U) A. Institute a common pre-approval standard across all agencies that incorporates, at minimum, a two-person integrity check for U.S. person content queries. (NSA's policy, which already meets this standard, could remain as is.)

(U) B. Require each agency to update its software to require a robust standard for written justifications of U.S. person queries, including a reference citation for the specific factual basis substantiating that the query is reasonably likely to return foreign intelligence information.

(U) C. Require each agency to conduct pre-query due diligence to determine the U.S. person status of the query subject.

(U) D. Require each agency to update its software to include better provisions for record-keeping, auditability, and accountability for U.S. person queries.

(U) E. The DNI and Attorney General should submit a legislative proposal, if needed, to resource these recommendations as required.

(U) **3. Direct the FBI Director to improve FBI compliance efforts by designating and training a compliance officer responsible for ensuring appropriate use of Section 702 in each field office and at FBI Headquarters.**

(U) A. This person could serve as the second person in a two-person pre-approval process for U.S. person queries.

(U) B. FBI should submit a legislative proposal, if needed, to appropriately resource this recommendation.

[redacted]

[redacted]

(U) **4. Direct all agencies to submit an implementation plan for recommendations 1, 2, and 3 to the DNI and the Attorney General within two months of your directive, to be executed within six months of approval.** Upon the accomplishment of the recommendations as set forth in each agency's implementation plan, which will be released to the public, the DNI and the Attorney General would certify to Congress that the actions are complete. Within the implementation plans, each agency should include clear milestones and timelines for how each recommendation will be met. Each agency will provide a quarterly status update of its progress in addressing recommendations 1, 2, and 3 to the Intelligence Oversight Board.

(U) **5. Create a common culture of compliance across the FBI workforce that employs Section 702 authorities through senior personnel exchanges**. Charge the Director of FBI and the Director of NSA with creating Joint Duty Assignments where senior (GS-15 and Senior Executive Service) NSA officers who are subject matter experts in FISA are placed in appropriate positions at FBI for three-year tours; additionally, create similar Joint Duty Assignments for senior FBI officers at NSA.

(U) **6. Establish within the Executive Office of the President (under the auspices of the Intelligence Oversight Board) a centralized, external, independent review mechanism to assess the effectiveness of the entire compliance and oversight system on a regular basis, to ensure that corrective executive action is taken when required.**

(U) **7. Direct the DNI and the Attorney General to research potential technology enhancements to the current oversight framework and report findings to the President, Congress, and Intelligence Oversight Board.** Current Section 702 oversight and compliance processes are complex, resource intensive, and unable to allow for timely detection of noncompliance incidents. The implementation of modern technology enhancements such as machine learning tools, systems that enable near real-time access to Section 702 user compliance data, or other automated processes could improve compliance and the timely enforcement of rules.

(U) **8. Direct the Attorney General to submit a legislative proposal to Congress that would fund the expanded capacity needed to achieve 100 percent oversight of FBI U.S. person queries of Section 702 information.** The Board assesses that other FBI-specific recommendations made herein would decrease the volume of U.S. person queries requiring DOJ oversight, which would mitigate the cost of this recommendation.

(U) **9. Enhance transparency by declassifying, to the greatest extent possible, the certifications specifying the categories of authorized collection under Section 702.** This would increase the public's awareness of 21st century national security risks, the vital

[redacted]

[redacted]

contributions of signals intelligence for understanding and countering those risks, and the safeguards that protect privacy and civil liberties.

[redacted] **10. Direct the DNI and the Attorney General to submit a new counternarcotics certification under Section 702 to the FISC.** Such a certification would allow the intelligence community to collect against [redacted] Inclusion of this new certification would not expand Section 702 authorities to any additional agencies.

(U) **11. Direct the DNI and the Attorney General to agree upon a common set of standards that would hold Section 702 users and agencies accountable in performing querying.** Zero tolerance policies for willful misconduct and escalating consequences for unintentional noncompliance should be instituted at both the user and supervisory levels.

(U) **12. Direct DNI and DOJ to submit legislative proposals that would codify in statute Section 702's adherence to the principles articulated in Executive Order (EO) 14086, Enhancing Safeguards for United States Signals Intelligence Activities**. The principles include permissible objectives of signals intelligence collection and prohibited uses of signals intelligence collection. This recommendation would scope Section 702 collection to one of the authorized uses in EO 14086 (to include EO 14086's explicit recognition of the President's authority to update the list in light of new national security imperatives, with any updates publicly released unless doing so would pose a risk to U.S. national security) and prohibit Section 702 collection from occurring for unauthorized purposes such as suppressing the free expression of ideas or political opinions by individuals or the press and disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion. This should be implemented via an additional attestation requirement as part of the annual certification to the FISC.

(U) **13. Direct the DNI and the Attorney General to submit a legislative proposal to require the participation of *amici curiae* in all annual Section 702 certification processes to the FISC, so as to better protect privacy and civil liberties**. This approach allows those with the necessary security clearances to engage in adversarial representation in normally-closed proceedings.

[redacted]

[redacted]

(U) Conclusion

(U) Section 702 is a relatively new authority that was enacted by Congress when the nation determined that it would not allow foreign threat actors to communicate freely on U.S. networks while plotting against America. The Board concludes that Section 702 is essential to generating the intelligence necessary to protect the United States from a host of threats, such as terrorism, cyber attacks (including potentially catastrophic attacks on infrastructure), influence by foreign actors on our democracy, illegal export of critical technology, and importation of deadly fentanyl and other substances that are killing so many Americans. Section 702 will also be critical to meeting emerging threats whose full impact has yet to materialize.

(U) The Board concludes that jettisoning Section 702 over compliance errors made in its first 15 years would be a tremendous mistake. The Board believes implementation of its proposed legislative and executive branch recommendations will improve compliance and oversight, and thus public confidence, in Section 702, without increased risk to the intelligence community's collective ability to protect the American people. Congress should be aware that failing to renew Section 702 would immediately expose the nation to the threats set forth above.

[redacted]

[redacted]

(U) Appendix I – FISA Section 702 Overview

(U) What is FISA Section 702?

(U) Section 702 of FISA is a law that authorizes members of the U.S. intelligence community to collect electronic communications, such as e-mails and phone calls, of non-U.S. person targets who are located overseas to acquire foreign intelligence information. Under Section 702, the government is able to obtain these electronic communications by compelling U.S. telecommunications companies to provide the requested information to the government. Prior to the establishment of Section 702, the government was required to obtain a Title I FISA warrant to conduct electronic surveillance for both U.S. persons and non-U.S. persons alike.

(U) Section 702 does not permit "reverse targeting," or targeting a non-U.S. person located outside the United States for the ultimate purpose of targeting a U.S. person or a person inside the United States. Section 702 also does not allow for the collection of bulk data, including the indiscriminate collection of metadata. All collection under Section 702 is targeted collection.

(U) FISA Title I versus Section 702

(U) FISA Title I authorizes the government to conduct electronic surveillance of, among others, a U.S. person or a person located in the United States. In order to conduct such surveillance, the government must obtain an order from the FISC by demonstrating probable cause to believe that the target is an "agent of a foreign power," like a spy or international terrorist. This is similar to getting a court order to conduct a wiretap in a criminal case. A key difference between Title I and Section 702 is that Title I authorizes electronic surveillance of a foreign power or agent of a foreign power, which can include a U.S. person or a person located inside the U.S., under an individual FISC order specific to that foreign power or agent of a foreign power, while Section 702 only allows the targeting of a non-U.S. person outside the United States to collect foreign intelligence information and does not require an individual FISC order specific to that non-U.S. person. The querying procedures required by Section 702 only permit post-surveillance queries of information, which might include incidentally-collected U.S. person communications, to retrieve foreign intelligence information or, in the case of FBI, evidence of a non-national security-related crime. Notably, any direct collection on the U.S. person that may be desired by the government as a result of information obtained by querying Section 702-acquired information would require other legal processes, such as a FISC order or criminal warrant.

[redacted]

[redacted]

(U) Incidental Collection

(U) The focal point of the Section 702 debate centers on how the government should treat incidental collection of U.S. person information, such as when the government comes across an e-mail in Section 702 data between two foreign terrorists talking about a U.S. person. FISA defines a "U.S. person" as a U.S. citizen, a lawful permanent resident of the United States, a U.S. corporation, or other U.S. entity (such as a non-governmental organization) located anywhere in the world. While FISA does not define all individuals located in the United States as U.S. persons, Section 702 nonetheless cannot be used to target anyone in the United States. Because Section 702 can only be used to intentionally target non-U.S. persons outside the United States, any collection of U.S. person communications is considered "incidental." In other words, it is not intentional, but it is unavoidable.

(U) Other collection methods aligned to foreign intelligence threats, such as human intelligence, also encounter incidental collection and have procedures in place to handle that information appropriately. Within the Section 702 program, minimization procedures govern the retention, dissemination, and use of incidentally-collected U.S. person information.

(U) When an intelligence agency encounters U.S. person information while reviewing intentionally-collected Section 702 data, it has an interest in determining whether that U.S. person is a potential victim of, or a potential accomplice to, the threat that was the original purpose of the Section 702 collection. In the former case that the U.S. person is a potential victim, the government will seek to warn and protect the U.S. person. In the event that the U.S. person is an accomplice, the government will attempt to thwart any nefarious activity carried out by that U.S. person.

(U) In many cases, one agency will likely need to share pertinent information with another agency. For example, NSA only focuses on foreign intelligence threats overseas, so it would need to pass the relevant information about these U.S. persons to FBI for the Bureau to take appropriate action.

(U) In the event that the U.S. person is neither an accomplice nor a victim (perhaps the U.S. person is simply a friend or acquaintance of the terrorist but not involved in any nefarious activity), and the information does not contain foreign intelligence information, the government is required to purge any Section 702-acquired U.S. person information it has incidentally collected after a set period of time.

[redacted]

[redacted]

(U) U.S. Person Queries

(U) Typically, in order to reach a conclusion about whether the U.S. person is an accomplice, a victim, or neither, the intelligence agency will need to conduct more research. For example, if an intelligence officer is reviewing the e-mails of an international terrorist and discovers an e-mail that indicates that this terrorist has plans to attack a specific school in the United States, the intelligence officer will want to gather more information about any potential attack against the school. The intelligence officer may choose to execute a query in the Section 702 database using the U.S. school's name as a search term to determine if there is additional information pertinent to this potential attack. This is a U.S. person query. Prior to conducting the query, the intelligence officer must ensure that he or she has satisfied the query standard outlined in the querying procedures.

(U) Absent an exception, every query of Section 702 information, whether involving a U.S. person or not, must meet the baseline standard: the query must be reasonably likely to retrieve foreign intelligence information or, in the case of FBI, and only in the case of FBI, the query could also be conducted to retrieve evidence of a non-national security-related crime. There are publicly released, FISC-approved rules for querying Section 702 data for all four agencies that can access "unminimized" or raw Section 702 information. For FBI specifically, in addition to each query of Section 702 data meeting the baseline query standard, 1) the person conducting the query must have purpose for retrieving foreign intelligence information or evidence of a crime, 2) the person conducting the query must have a specific factual basis to believe that it is reasonably likely to retrieve foreign intelligence information or evidence or a crime; and 3) the query must be reasonably tailored to retrieve foreign intelligence information or evidence of a crime without unnecessarily retrieving other information.

(U) In the example above, the government would seek additional information to determine the timing and method of a potential attack on the school and conduct queries in the Section 702 database to attempt to address those information needs. Conducting a query does not collect new information – it filters the information that has already been collected.

(U) A user may choose to conduct a Section 702 query to retrieve content or metadata. Content refers to any information about the substance or meaning of a communication while metadata refers to the routing or addressing information associated with a communication.

[redacted]

[redacted]

(U) Appendix II – NSA's Use of FISA Section 702

(U) NSA uses Section 702 information to produce foreign intelligence information in support of policymakers, the military, and cybersecurity personnel. NSA is the primary agency involved with Section 702 and only the NSA may initiate Section 702 collection. NSA collects on non-U.S. persons on behalf of itself and as requested by the CIA and FBI. NCTC does not nominate new foreign intelligence targets for collection, but it can request access to already-collected Section 702 information that meets its mission need. All NSA analysts accessing Section 702 data are trained to do so.

(U) NSA collects information through "downstream" collection, which is acquired through the compelled assistance of U.S. electronic communications service providers. NSA also collects information through upstream collection, which is acquired through compelled assistance of the providers that control the U.S. "telecommunications backbone." While downstream collection is shared with CIA, FBI, and NCTC, only NSA may access upstream collection.

[redacted] When an NSA analyst discovers a new identifier of interest, the first step is to conduct some research. In our hypothetical example, an NSA analyst identifies a foreign state-sponsored hacker who uses an e-mail address serviced by an electronic communications service provider. The NSA analyst starts by researching this hacker to verify that the individual is a non-U.S. person, located outside of the United States, and related to a foreign intelligence purpose authorized under an existing Section 702 certification. In this case, the analyst knows through other intelligence sources that this hacker plans to attack a piece of U.S. critical infrastructure, namely [redacted]. The analyst prepares a request to initiate collection of this foreign hacker's e-mail address.

(U) To pursue collection, NSA analysts must draft a targeting request that includes the hacker's name (if known), the hacker's e-mail address, a justification explaining the expected foreign intelligence information to be gained, and evidence demonstrating the hacker is reasonably believed to be a non-U.S. person outside the United States. In this request process, NSA analysts examine the totality of information available to them to build their case. If an analyst finds information that does not support use of the Section 702 authority, the analyst must address this issue before proceeding with the request.

(U) After the NSA analyst submits the targeting request, it passes through two additional levels

[redacted]

[redacted]

of review: peer review and final adjudication, each of which is performed by a different person who has been trained for that additional function. The adjudicator—a person who has specific additional training certifying them to evaluate Section 702 targeting requests for approval—will review the request and complete a separate set of database checks to ensure the information in the request is accurate. If approved, the e-mail address is sent via FBI to the compelled provider to initiate collection. Additionally, analysts are required to conduct post-targeting reviews to ensure targeted identifiers (in this case, the foreign hacker's e-mail address) continue to meet Section 702 requirements.

(U) The key details from all targeting records, including the target identifier (such as an e-mail address or phone number), target, justification, and supporting details, undergo subsequent checks by NSA's Office of Compliance and after-the-fact review by DOJ. This extensive process is in place to ensure the integrity and legality of collection even on a foreign entity.

(U) Once data is returned from providers and available in NSA databases, analysts can only access the collected information by running a query. Queries are searches of Section 702 data that has already been lawfully collected; they are not requests for new collection. The information is held in NSA databases and labeled specifically, distinguishing it from data collected using other authorities.

(U) NSA queries of Section 702 data are subject to the query standard mentioned previously. NSA has two approaches to querying data: pre-structured queries and custom queries.

(U) Pre-structured queries simplify adherence to the Section 702 querying procedures. Pre-structured queries use details from the Section 702 targeting records (such as the target's e-mail or phone number) and the current targeting status (whether it is still in an authorized state or not) to help inform whether a Section 702 query is authorized to be executed by the analyst. Pre-structured queries require action by an analyst to execute. The pre-structured nature simplifies the compliant retrieval of data by minimizing the possibility of typographical errors.

(U) Custom queries allow analysts to design their own query terms and structure. In addition to providing terms, analysts must opt into the specific authorities' datasets that their queries will run against and provide foreign intelligence justifications.

(U) In this example, the NSA analyst queries into the lawfully-collected Section 702 data using the e-mail address of the foreign hacker as the search term. The returned results include the communications sent to and from the foreign hacker's e-mail address available in the already-collected data, as well as any other communications in the Section 702 database that contain the e-mail address used in the search term.

[redacted]

[redacted]

(U) The vast majority of NSA's queries into Section 702 data use non-U.S. person query terms; however, there are situations in which NSA uses a U.S. person query term (e.g., a U.S. person name or telephone number used by a U.S. person) to expeditiously search the Section 702 data already legally acquired and in NSA holdings for foreign intelligence purposes. The basis for that U.S. person query could be derived from information previously gleaned from Section 702 data, information from other intelligence reporting, or other sources.

(U) In this example, the U.S. person query term is connected to U.S. critical infrastructure. In 2022, most of NSA's U.S. person query terms used to retrieve content from Section 702 data were terms associated with non-human beings, used to identify foreign threats to those entities. Whether a query term is related to a human being or not, the query standard remains the same. NSA recognizes the sensitivities associated with U.S. person queries of Section 702-acquired content. Accordingly, NSA has put into place extensive safeguards in addition to those required by its querying procedures.

(U) All NSA U.S. person queries of Section 702 content must first be pre-approved by NSA's Office of Compliance and Office of General Counsel before that query may be executed. In some circumstances, the U.S. person query requires additional safeguards, including additional specialized training of personnel; approval by NSA's Civil Liberties, Privacy, and Transparency Office; various levels of NSA leadership pre-approval; and increased oversight of the queries.

[redacted] In our example, the NSA analyst performing a query in which the analyst seeks to learn more about the foreign hacker's intention to disable a specific U.S. [redacted] will design the parameters of the query to retrieve information about the foreign hacker's planned attack against the U.S. [redacted]. At a minimum, the analyst will likely use the foreign hacker's e-mail address and the name of the U.S. [redacted], and select the time frame for the query. The analyst will also select the specific sets of data the analyst intends to query against and will seek pre-approval before the analyst runs the query. Because the query contains the name of a U.S. asset, this is considered a U.S. person query.

(U) Now that the NSA analyst has received approval to run the query and has done so, the analyst retrieves and reviews the results for foreign intelligence. The analyst will often review many pieces of collection, such as e-mails, to determine which communications satisfy foreign intelligence requirements.

(U) As mentioned above, even when querying using foreign query terms, NSA analysts might come across U.S. person information, such as when a Section 702 target is communicating with a U.S. person. NSA analysts receive training on how to handle communications in which a U.S. person is a communicant (and part of the incidentally-collected U.S. person information) or

[redacted]

[redacted]

when U.S. person information is otherwise included in a communication (such as when a foreign intelligence target is discussing a U.S. person).

(U) Once the analyst has identified one or more communications meeting a valid foreign intelligence requirement, the analyst may craft an intelligence report to disseminate the information to NSA's intelligence customers. When authoring a dissemination based on a communication involving a U.S. person (either as an incidental communicant or as a subject of the communication), the analyst must determine whether any information about the U.S. person is required in order to understand the foreign intelligence. If information about the U.S. person is not needed to understand the foreign intelligence, then the analyst will write the intelligence report without any reference to the U.S. person.

(U) When information about the U.S. person is needed to understand the foreign intelligence, the analyst will limit references to the U.S. person to only what is necessary to understand the foreign intelligence. The analyst will also evaluate whether, based on NSA's Section 702 minimization procedures and dissemination policy, the analyst is authorized to identify the U.S. person in the report or whether the identity of the U.S. person must be "masked" (in generalized wording such as, "named U.S. person"). This protects the identity of the U.S. person to readers of the intelligence report. Intelligence consumers who have a need to know the U.S. person identity can submit a written request to NSA to have the identity "unmasked." This means the identity is released to the requester (not all consumers), but only if the identity is needed to understand the foreign intelligence

(U) NSA must conduct an initial review of tasking shortly after this action and then routinely thereafter. Generally, NSA may retain Section 702 information for up to five years, with exceptions based on whether the information is determined to be foreign intelligence, or other factors, such as requiring additional time for decryption.

[redacted]

[redacted]

(U) Appendix III – CIA's Use of FISA Section 702

(U) CIA uses Section 702 information to support its operations worldwide, to include protecting CIA officers from threats posed by hostile intelligence services and non-state actors. While CIA can access Section 702 data, the agency cannot directly collect the data itself. Instead, CIA must submit a request to NSA to initiate the collection. When CIA identifies a foreign person with intelligence information of national security interest, a CIA officer will try to identify accounts used by this person, such as an e-mail address and phone number. In a hypothetical scenario, a person of interest (or "target") might be someone who has volunteered to be a CIA source and claims to have information about an adversary country's military plans and intentions. The CIA officer would research this target and might discover that the target uses a U.S.-based e-mail provider. The CIA officer would assess whether the target fell under one of the categories on which the FISC had approved collection; then, the officer would prepare a request to NSA to initiate collection on that e-mail address.

(U) This request by CIA includes such information as the target's name (if known), e-mail address, evidence about why this target is likely to have information about the adversary government's military plans, the foreign intelligence information that the government expects to collect as a result of tasking the e-mail address, evidence that this target is not a U.S. person, and justification that the target is located overseas. The CIA officer's request would then be reviewed and approved by a supervisor and CIA's FISA program office before being submitted to NSA.

(U) When NSA receives CIA's request for collection, an NSA analyst then uses other resources at NSA's disposal to confirm that the target is not in the United States, in addition to verifying the information in CIA's original request. In this example, NSA would review CIA's information indicating that the target is likely to possess, receive, or communicate foreign intelligence information about the adversary government's military plans. NSA is required to cite specific documents supporting its determination that the target is not in the United States. Then, the information is peer-reviewed by another NSA analyst and adjudicated by a more senior NSA analyst before the request is approved. This is the same process NSA applies to its own targeting requests to initiate Section 702 collection. NSA documents all of this information, which is later reviewed by DOJ.

(U) At this point, NSA sends the request to FBI, which provides it to the appropriate

[redacted]

[redacted]

communications service provider to initiate collection on this e-mail address requested by CIA. The authorized collection is then sent to CIA. In this hypothetical, the requested communications are e-mails sent to and from the target's e-mail address. CIA stores its FISA information in a standalone database that requires a user login and password. CIA's Section 702 information is compartmented into "bins" so that an officer with access to CIA's Section 702 data can only access those "bins" that are applicable to the officer's job. In this present instance, the CIA officer might only have access to Section 702 data that pertains to a subset of intelligence information, such as an adversary's military affairs. Only designated CIA officers with the appropriate training and certifications are given access to Section 702-acquired data.

(U) When reviewing the collected emails, the CIA officer can view the data manually, by clicking on each e-mail to read its contents. The officer may also choose to use search terms to "query" or filter the information to find pertinent information. This is a process very similar to someone searching their own e-mail inbox for a relevant e-mail. Returning to our example, the officer might input as a search term the name of a high-ranking foreign military official who the CIA officer has reason to believe is in communication with the target.

(U) In this example, after volunteering, the target meets with a CIA field officer overseas and mentions being friends with a senior foreign military officer, handing the CIA field officer the foreign officer's business card as proof. The CIA officer could use the e-mail address listed on the business card to run a query within the target's e-mails. This query would meet the standard of being "reasonably likely to retrieve foreign intelligence information" because the target told the CIA they were friends and, separately, the CIA officer knows that the officer is in fact, a key figure in that country's military. CIA's Section 702 database logs each query conducted, to include recording the query terms used, the date of the query, and the officer who conducted the query.

(U) It is possible that this particular query returns several e-mails between the target and the military officer (only e-mails from the authorized "bins" will appear). In reading these e-mails, the CIA officer discovers that the communications mention a particular advanced U.S. technology—produced by only one U.S. company—that would critically enhance the adversary's military capabilities. At this point, the CIA officer wants to query the target's e-mails using the U.S. company name as a query term in order to gain foreign intelligence about how the adversary government plans to gain access to the technology. This is considered a U.S. person query.

(U) There are additional rules for querying Section 702 data using terms that contain U.S. person identifiers. In these instances, the officer must enter a statement of facts showing that the U.S. person query terms are reasonably likely to retrieve foreign intelligence information. Before

[redacted]

[redacted]

running the query, the officer documents the justification for conducting a U.S. person query using the same query standard described previously. All of these justifications are logged in a database, along with the query terms, date of the query, and officer who conducted the query.

(U) CIA users of Section 702 data are required to review their holdings every 30 days to determine whether the data contains information of foreign intelligence value and confirm the target remains an appropriate one for collection pursuant to Section 702. For any specific information that the CIA officer deems necessary to transfer outside of the restricted FISA repository that contains U.S. person information, the officer must either redact the U.S. person information from the product or write a justification explaining why the U.S. person information is necessary to understand the foreign intelligence or assess its importance. All data determined to contain information of foreign intelligence value must be marked as such within this database or transferred out of the database for use in operational or analytic products. All other data neither marked as containing information of foreign intelligence value nor transferred out of the database will, in general, automatically be purged from the database after five years from the expiration of the certification authorizing the collection.

(U) CIA shares the Section 702 data it acquires when there is a need to notify another U.S. government agency or a foreign government of pertinent information. For example, CIA would share information about an adversary's plans to steal U.S. technology with FBI so the FBI could warn the U.S. company in the hope of preventing any potential theft.

[redacted]

[redacted]

(U) Appendix IV – NCTC's Use of FISA Section 702

[redacted] NCTC's Section 702 program focuses on reviewing communications by known and suspected terrorists, conducting international terrorist network development, and garnering insight into international terrorist operations. NCTC first gained approval to access unminimized Section 702 data in April 2017. NCTC does not nominate targets for specific collection. Instead, NCTC requests Section 702 [redacted] information already collected by NSA pertaining to international terrorist targets located outside the United States that NCTC tracks. NSA checks all NCTC [redacted] requests and approves them before NCTC receives the information.

[redacted] NCTC analysts authorized to access Section 702 data receive training required for this access. NCTC analysts review the [redacted] Section 702 collection at least every seven days to ensure there are no indications that the target is a U.S. person, is in the United States, or is intending to travel to the United States or an unidentified location. NCTC analysts must complete a "Mark as Reviewed" action to re-start a seven-day review clock affirming they have reviewed their designated Section 702 data. If the review is not completed within seven days, the selector will turn yellow on the analyst's dashboard. After 14 days, it turns orange and the analyst's supervisor receives an alert e-mail. After 21 days, it turns red and the analyst's supervisor and NCTC compliance office receive alert e-mails.

[redacted] In a typical scenario, an NCTC analyst begins by identifying and requesting [redacted] the Section 702-collected information for a known terrorist overseas whose selector NSA already has tasked for collection. [redacted]. One of the most important questions for NCTC to determine is whether the international terrorist could gain access to and pose a threat to the homeland. Part of NCTC's mission is to map out and understand specific high value terrorist networks.

(U) In this example, the NCTC analyst discovers from reviewing the e-mail communications of the Al-Qa'ida affiliate that he is in communication with a California-based individual. Since the individual is in the United States, unless circumstances give rise to a reasonable belief that this person is not a U.S. person, the individual is presumed to be a U.S. person. The NCTC analyst will first conduct database checks on that U.S. person's e-mail address in counterterrorism data

[redacted]

[redacted]

sets that do not contain Section 702-acquired information to identify any other connections to international terrorism. The NCTC analyst will then evaluate the nature of its findings and determine how often that U.S. person's e-mail address is in contact with known or suspected international terrorists. If the results of these database checks establish a sufficient basis to meet NCTC's query standard for Section 702 data, NCTC may query the presumed U.S. person e-mail address against Section 702 information to identify any additional connections to international terrorists.

(U) In this example, the NCTC analyst further discovers that the above presumed U.S. person has ties to multiple international terrorist networks. Before the NCTC analyst may run a query using this individual's e-mail address as a query term, NCTC's FISA information system requires the analyst to provide a written justification for each query of Section 702-acquired information. In this example, the NCTC analyst provides written justification for the query and runs the search.

(U) If NCTC identifies the presumed U.S. person as having relevant connections to one or more counterterrorism targets sufficient to meet the NCTC Section 702 standard for dissemination, NCTC will issue a FISA dissemination cable to NSA, FBI, and CIA, and then potentially issue a lead cable to mission partners including FBI to further their consideration in connection with counterterrorism investigations and threat determinations.

(U) Since NCTC's ability to access Section 702 data is relatively recent, it has incorporated many compliance measures into its program from inception. NCTC's Compliance and Transparency Group provides internal reviews of its use and handling of FISA-acquired information to provide reasonable assurance that NCTC personnel comply with the FISA requirements and NCTC's Section 702 procedures and to properly identify, address, and report instances of non-compliance. NCTC's Compliance and Transparency Group administers training and conducts monthly reviews of NCTC's Section 702 query and minimization logs, as well as disseminations of Section 702-acquired information.

(U) Section 702 information in NCTC's holdings that has not been reviewed is destroyed five years from the date of expiration of the certification under which the information was acquired, unless specific authority is obtained. Information that has been reviewed but has not yet been determined to meet the minimization standard is accessible for ten years from the expiration date of the certification. After ten years, the information is placed in restricted status, such that users will receive notice of its existence if it is responsive to a query, but executive level approval is required in order to gain full access to it. After fifteen years, information that has not been determined to meet the minimization standard is destroyed, unless specific retention authority is obtained.

[redacted]

[redacted]

(U) Appendix V – FBI's Use of FISA Section 702

(U) FBI uses Section 702 to support its national security investigations, in concert with other authorities. By longstanding FBI policy, the agency only receives Section 702 collection on a particular foreign intelligence target if that target is relevant to an ongoing full FBI national security investigation. This policy decision has not been codified into statute, but it is in place to ensure that FBI's use of Section 702 data is consistent with its role in the intelligence community, namely, to investigate and disrupt threats to the homeland. As a result, in 2022, FBI received collection on 3.22% of the intelligence community's total Section 702 targets.

(U) To give an example of how this works in practice, consider a hypothetical involving FBI's efforts to counter a Chinese intelligence service. FBI has a number of open investigations into Chinese intelligence activities targeting the United States in field offices around the country. Many of these investigations may never result in prosecution because the individual foreign officers involved will never leave China, and the U.S. government may, therefore, never have the opportunity to arrest and charge them. Nevertheless, FBI is responsible for tracking and disrupting these intelligence activities when they affect American citizens or companies.

[redacted] In this example, the foreign intelligence officer, posing as an academic, makes contact with an American [redacted]. This action is consistent with those of other Chinese intelligence officers who, in order to develop relationships with Americans, might ask their targets to write "white papers" that disclose nonpublic information, or to present at a conference or university in China. After making initial contact [redacted], foreign intelligence officers will often try to transition to other communication channels, such as e-mail.

(U) Returning to the example, an FBI agent working an investigation into Chinese intelligence activities receives intelligence information from CIA about an e-mail address that is used by the Chinese intelligence officer posing as an academic. That serves as the initial tip that FBI uses to develop its investigation further.

[redacted] Noticing that the e-mail address resolves to a U.S.-based e-mail provider, the agent then sends a request to NSA to collect the e-mails sent to and from this e-mail address. The request would contain the e-mail address itself, the name of the user (if known), evidence that this user is not a U.S. person or a person in the United States, and justification for requesting

[redacted]

[redacted]

collection of communications to and from this e-mail address. In this example, it turns out that this account had already been targeted for collection under Section 702 by NSA, so FBI requests a [redacted] to receive the collection that the NSA is already receiving.

[redacted] Once NSA approves FBI's [redacted] request, NSA gives FBI a copy of the requested communications for this e-mail address. All FBI personnel who are approved to have access to Section 702 data receive training on the use of Section 702 information as a condition of being granted access.

(U) At this point, the FBI case agent will be able to see exactly what the foreign intelligence officer is saying via that e-mail address and to whom the officer is saying it. Over time, the case agent might see that the Chinese intelligence officer is in contact with dozens or even hundreds of Americans. Some of these people might have ignored the foreign intelligence officer's outreach and never responded. Others might have responded, but they have no idea they are communicating with a foreign intelligence officer. And some of these people might be fully recruited assets of this Chinese intelligence officer now secretly gathering information inside the United States.

(U) To triage this information, the agent can query numerous FBI database holdings using identifiers such as e-mail addresses or phone numbers for those presumed to be U.S. persons in order to obtain a full picture of where they fall on that spectrum and, correspondingly, what kind of intervention is needed. These databases are federated and can access more than 100 different FBI repositories including travel data, immigration data, and Section 702 data. The agent can enter the query terms and select which databases to search. Currently, the default setting is for Section 702 data not to be included. When the agent submits the query, a pop-up window asks whether the agent wants to include a search of Section 702 data. If so, the agent will be prompted to go back and select the Section 702 data to be included in the query (which, in this case, will include communications to and from the foreign intelligence officer's e-mail address).

(U) The agent will then be prompted to fill out a form indicating whether or not the query contains a U.S. person search term. Once this indication is made, the query is run.

(U) The system logs all U.S. person queries. If the U.S. person query returns no results, no further action is taken in the system. If the U.S. person query returns results, the system prompts the agent to identify the purpose and justification for the query prior to accessing any Section 702 collection that is retrieved.

(U) In this example, the FBI agent, who is reviewing the communications of the foreign intelligence officer, can see that this intelligence officer is communicating with many Americans.

[redacted]

[redacted]

In order to distinguish who has been co-opted and who has yet to be co-opted, the agent needs to review these e-mails. Importantly, FBI can only see emails between the U.S. persons and non-U.S. persons already under FISA collection—they cannot see any other emails that the U.S. persons have sent or received.

(U) Based on the query results (to potentially include non-Section 702 information), FBI may send leads to the field office where that U.S. person is located for any necessary follow-up — whether that takes the form of a defensive briefing for potential victims or further investigation. For recruited co-optees of the foreign intelligence service, FBI would open a new spin-off investigation, which may include requesting a warrant to surveil the U.S. person who FBI has evidence is acting as an agent of the foreign intelligence service.

(U) FBI must review tasking within five days upon receipt of collection to confirm the correct identifier is under coverage and meets FISA 702 targeting requirements. At minimum, Section 702 information must be reviewed at least once every 30 days thereafter to continue confirming that the target meets FISA 702 targeting requirements. FBI's Section 702 information that has not been reviewed will be purged five years after the expiration of the certification under which it was collected. Information that has been reviewed but not marked as meeting the minimization standard will be restricted ten years after expiration of the certification and purged after fifteen years.

(U) All FBI U.S. person queries are logged and may be subjected to subsequent review by DOJ. With the exception of 2021, FBI's U.S. person queries in its Section 702 data have constituted about a quarter to a third of its overall Section 702 queries for the past three and a half years. FBI's Section 702 U.S. person queries in 2021 accounted for more than half of FBI's overall Section 702 queries because of a series of batch queries that represented 1.9 million U.S. person queries.

[redacted]

[redacted]

(U) Appendix VI – Procedures and Oversight

(U) The Attorney General and DNI may authorize for a period of up to one year the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign intelligence information about topics such as foreign governments, international terrorism, and the proliferation of weapons of mass destruction. The Attorney General and DNI provide the FISC a written certification and any supporting affidavits from the heads of the intelligence agencies prior to the implementation of any such authorization. The FISC, which was created in 1978 to review applications for electronic surveillance in the United States for foreign intelligence purposes, reviews and approves these certifications. The FISC also reviews and approves accompanying affidavits and procedures, including targeting procedures (which describe rules for the collection of a specific electronic communication), minimization procedures (which describe rules for the retention and sharing of the information collected), and querying procedures (which describe rules for conducting queries of the information collected). Each of the four agencies that receives unminimized Section 702 data (NSA, FBI, CIA, and NCTC) has its own procedures governing the minimization, querying, and sharing of Section 702 data tailored to its specific mission. The FISC must review a certification and accompanying procedures and issue an order within 30 days from the date the certification is submitted, unless the court finds that an extension is necessary for good cause in a manner consistent with national security.

(U) The Section 702 program is overseen in some fashion by all three branches of government. In addition to internal intelligence community compliance, the Section 702 program is overseen by DOJ, ODNI, the FISC, and Congress.

(U) DOJ reviews every NSA decision to initiate Section 702 collection. DOJ also reviews 100 percent of CIA's and NCTC's U.S. person queries and 100 percent of NSA's approved U.S. person query terms. Because of the high volume of FBI queries, DOJ reviews only a sampling of FBI's U.S. person queries. DOJ also reviews a sampling of FBI's non-U.S. person queries. To assess compliance with Section 702 program procedures as approved by the FISC, DOJ conducts bi-monthly reviews of NSA's, CIA's, and NCTC's implementation of their targeting, minimization, and querying procedures. DOJ conducts reviews of FBI's implementation of its targeting procedures on at least a bi-monthly basis. In addition, DOJ conducts query audits each year of approximately 23-27 FBI field offices and Headquarters components to assess compliance with the querying and minimization procedures. Since March 2022, DOJ has also periodically reviewed FBI's sensitive query pre-approvals. Finally, DOJ has conducted certain

[redacted]

[redacted]

FBI-wide query audits, focusing on a sample of queries run by multiple FBI offices.

(U) DOJ reports all identified incidents of noncompliance to the FISC and to Congress, including the scope and nature of each incident, its cause, and the remedial actions taken in response. DOJ documents noncompliance in letters and quarterly reports to the FISC, and semi-annual reports to Congress. Jointly with ODNI, DOJ documents compliance trends in assessments transmitted to Congress, as well as the FISC. ODNI publishes the Annual Statistical Transparency Report, redacted versions of DOJ-ODNI joint assessments, and redacted versions of each FISC Memorandum Opinion and Order approving the certifications. ODNI also publicly releases redacted targeting, querying, and minimization procedures, which are the internal rules agencies use to govern how their officers initiate collection, conduct querying, share information, and store information.

(U) Today's Section 702 Oversight Framework

(U) Today, Section 702 is subject to multiple levels of oversight, supervision, and control (see Figure 1 below). In addition to internal compliance mechanisms initiated by the four Section 702 user agencies, there are no fewer than nine additional organizations that play an active role in oversight. All activities carried out pursuant to Section 702 are subject to the jurisdiction of the FISC. In certain instances, the court has issued assessments resulting from analysis of reported non-compliance issues. The FISC relies on mandatory compliance reporting to review and adjudicate the Attorney General and DNI certifications that authorize agency use of this authority. The FISC's referenced oversight role as it pertains to Section 702 is codified in the FISA Amendments Act of 2008. As part of its role, the FISC reviews each agency's targeting, querying, and minimization procedures to determine if they adhere to all statutory requirements and are reasonable under the Fourth Amendment. The FISC sometimes appoints *amici curiae* to review Section 702-related matters, and the FISC may request additional information and hold hearings on Section 702 legal and compliance matters.

(U) Additionally, Section 702 activities are subject to extensive oversight by the executive branch through DOJ and ODNI. DOJ provides oversight to ensure that agencies comply with applicable laws and policy. DOJ and ODNI monitor agency compliance efficacy, identify problem areas, and provide explicit corrective guidance to intelligence agencies. DOJ and ODNI are statutorily required to provide a comprehensive, joint compliance assessment every six months to the pertinent congressional committees. These assessments are also provided to the FISC and the Privacy and Civil Liberties Oversight Board (PCLOB). Lastly, Congress, through the House Permanent Select Committee on Intelligence and the Senate Select Committee on

[redacted]

[redacted]

Intelligence, as well as the Senate and House Judiciary Committees, regularly conducts oversight and receives periodic reports. Each of the named congressional committees also has the authority to request information pertaining to program implementation and compliance issues on an *ad hoc* basis.

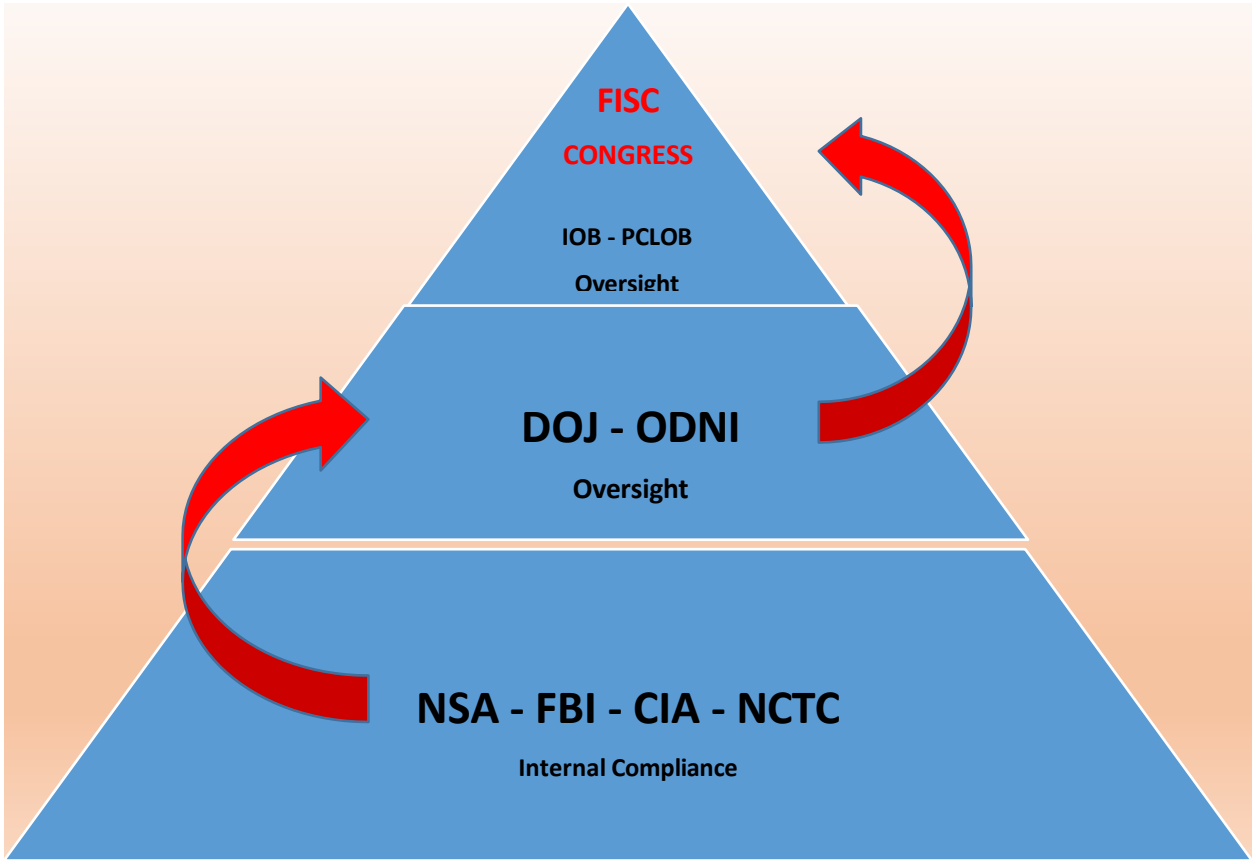
(U) The PCLOB—a congressionally mandated independent agency—was created specifically to ensure that the government's vast counterterrorism activities, including the use of FISA authorities to collect intelligence, can be carried out while effectively protecting privacy and civil liberties. In fulfilling its unique mission, the PCLOB conducts oversight reviews; provides recommendations; and advises the President, Congress, and other executive branch agencies.

(U) Finally, the Intelligence Oversight Board (IOB) possesses extensive authorities within the executive branch to review and assess the legality, effectiveness, efficiency, and sufficiency of intelligence activities and associated processes. Although Executive Order 13462, which established the IOB, does not explicitly reference FISA Section 702, the Board is well-positioned to exercise oversight in this area.

[redacted]

[redacted]

(U) Figure 1: Current FISA Section 702 Compliance and Oversight Hierarchy



(U) The Board has observed that each of the organizations that support the Section 702 oversight framework have multiple, often overlapping, reporting mechanisms in place. The evolution of this purposely redundant audit and reporting framework has been largely effective in supporting DOJ and ODNI efforts to identify and report all compliance incidents to the FISC and illuminate those areas most in need of focused remediation. As a consequence of this periodic reporting and investigative framework, we assess that the existing oversight paradigm has largely encouraged implementation of remedial measures and enhanced compliance. While the Board finds that FBI has been slow to improve its compliance regime, it is noteworthy that DOJ and ODNI have metrics demonstrating that remedial measures put in place by FBI have yielded significant compliance improvements.

[redacted]

[redacted]

(U) Appendix VII – FBI's Record of Noncompliance and Reforms

(U) The FISC has taken note of the pervasiveness of FBI's querying noncompliance and attempts to address its pattern of broad, suspicionless queries that are not reasonably likely to retrieve foreign intelligence information or evidence of a non-national security-related crime. In 2018, the Court cited FBI's lack of understanding about what it meant for a query to be reasonably likely to return foreign intelligence information or evidence of a crime as a contributing factor. The Court recommended that FBI require users to document a justification for why they believed a U.S. person query that returned Section 702 collection was reasonably likely to return foreign intelligence information or evidence of a crime. FBI's first attempt to address this recommendation was to offer a drop down tab for FBI users to select their justification subsequent to the query being run but prior to accessing the content of the collection. In 2020, the Court found that FBI's failure to properly apply its query standard was more extensive than previously thought, noting that the queries occurred before FBI implemented reforms, and acknowledging that COVID severely limited DOJ's ability to monitor FBI's query compliance during this time. In 2021, the Court noted continued significant querying violations and questioned the effectiveness of the U.S. person query justification process that FBI implemented.

(U) DOJ and FBI disagreed about whether certain queries met the query standard. For example, multiple FBI field offices ran queries of individuals suspected to be involved in the January 6, 2021 Capitol breach. In some instances, FBI explained that they were determining whether the individuals had foreign ties, and in other instances stated that FBI viewed the situation in general as a threat to national security. DOJ assessed these queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime and were, therefore, noncompliant.

(U) Starting in mid-2021, FBI began to implement a number of reforms to further remedy its querying noncompliance.

- (U) DOJ and DNI added language to FBI's querying procedures to be clearer about the meaning of the query standard.
- (U) DOJ, ODNI, and FBI issued new comprehensive guidance to all FBI FISA users, and FBI instituted new mandatory training on that guidance, requiring all FISA users to have annual re-certification training.
- (U) FBI made a modification in its database requiring that users enter a case-specific justification (rather than use the drop down menu) as to the specific basis for why they

[redacted]

[redacted]

believe their query is reasonably likely to retrieve foreign intelligence information or evidence of a crime before accessing Section 702 content from a U.S. person query.

- (U) FBI changed the default settings in the system where it stores Section 702 data so that FBI personnel with access to Section 702 needed to "opt-in" to query such information.
- (U) FBI instituted a policy requiring FBI attorney approval prior to running any batch job that would result in 100 or more queries. A batch job refers to a capability in FBI systems that allows a user to run large numbers of query terms in sequential queries.
- (U) FBI instituted pre-approval requirements for certain sensitive queries. Sensitive persons include domestic public officials or political candidates, members of the media, members of academia, or religious figures. Under this new policy, an FBI attorney must review the justification for these queries before they are conducted. Proposed queries of domestic public officials and members of the media must also be personally approved by the FBI Deputy Director.

(U) On 12 June 2023, FBI introduced more accountability procedures with disciplinary actions that would take effect in the event of FISA noncompliance. While DOJ and ODNI have seen significant improvements in compliance, the Board concludes that these measures have not gone far enough.

(U) FBI has one of the most difficult jobs in U.S. national security. After every major terrorist attack in the homeland, FBI has sought to learn from its shortcomings, which has driven FBI to become increasingly thorough in its investigative processes. It is charged to defend our homeland, which includes gathering evidence in the most controversial and politically sensitive cases, when required. In the course of an investigation, FBI is constantly in search of evidence. Agents and analysts never want to be responsible for missing what could be the critical piece of information that makes the difference between disrupting a plot before it happens, and investigating an attack after it occurs.

(U) In an independent investigation into FBI's handling of its case on U.S. Army Major Nidal Malik Hasan, who was violently radicalized and killed 13 people and injured 42 others in the 2009 shooting at Fort Hood, Texas, the Webster Commission found that FBI had access to information about Hasan that did not come to light because the FBI personnel who conducted database queries did not include FISA databases in their queries. In other words, the FBI field office would have opened a preliminary investigation of Hasan (and potentially prevented the Fort Hood attack), if FBI had seen all of the communications it lawfully had in its possession, but were missed as a result of not querying FISA data. Thus, one of the changes FBI made to its database searches was to automatically include FISA information as a default query setting. The Commission report noted that the limited searches and a mistaken assumption about what was

[redacted]

[redacted]

included in the database search revealed a "lack of training on FBI's most precious counterterrorism resource – its information."

(U) Since the inception of Section 702, the U.S. government has brought to trial a total of nine cases in which a defendant received notice of the government's intent to use information derived from Section 702—all of them terrorism related. This included the arrest of Najibullah Zazi in 2009, whose planned suicide bombing in the New York City subway system was foiled by FBI, and the 2013 conviction of Mohamed Osman Muhamud, who attempted to detonate a vehicle bomb at a Christmas tree lighting ceremony in Portland. These cases reflect some of the impact that Section 702 brings to bear on FBI's mission of protecting the homeland.

[redacted]

[redacted]

(U) Appendix VIII – Fourth Amendment and Warrant Implications

(U) There is well-established precedent upholding the constitutionality of Section 702. In addition, eight different federal district judges sitting on the FISC and several judges in other federal courts, in criminal cases where information derived from Section 702 was used against defendants, have ruled that the Fourth Amendment does not require a warrant for the government to conduct U.S. person queries.

(U) Targeting non-U.S. persons located outside the United States pursuant to Section 702 does not require a warrant for two independent reasons. First, Section 702 targets only non-U.S. persons located abroad who are not protected by the Fourth Amendment. Second, according to multiple court decisions, Section 702 collection falls within the foreign intelligence surveillance exception to the warrant requirement in the Fourth Amendment. Additionally, a query of lawfully collected Section 702 data is not a separate search under the Fourth Amendment. Even if the query were a Fourth Amendment search, U.S. person queries properly and exclusively used to gain foreign intelligence do not require a warrant because courts have long held that the Fourth Amendment does not require a warrant for foreign intelligence collection.

(U) The following examples underscore why a warrant requirement to conduct U.S. person queries in which the government must show probable cause that the query terms belong to a foreign power or agent of a foreign power would have serious implications for national security. The probable cause standard for a FISA warrant is that the target must be a foreign power or agent of a foreign power.

[redacted] 1. From its Section 702 database derived from lawful collection on foreign state cyber actors, FBI observed these actors scanning U.S. [redacted] for vulnerabilities. FBI did not at this point know which [redacted] were compromised or breached by the foreign cyber actors. FBI queried selectors associated with the U.S. network infrastructure and saw that a small number of them had a high volume of data communications with the foreign state cyber actor, indicating that they were potentially compromised. These U.S. person queries helped FBI identify where the foreign hackers had achieved successful compromises of U.S. network infrastructure, and FBI was able to warn the network operators so they could mitigate the intrusion. A warrant requirement with a probable cause standard would have precluded this U.S. person query because there would have been no probable cause that the user of the U.S. selector

[redacted]

[redacted]

was a foreign power or agent of a foreign power. In this world, the victim would likely never have known that they had been hacked and the government would never close the vulnerability.

(U) 2. In 2021, after receiving a tip from another intelligence 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 FBI's Section 702 collection. The queries returned results that confirmed contact with officers from the threat country. FBI subsequently determined that the U.S. person was unaware they were being targeted and obtained important intelligence on the threat country's attempts to acquire sensitive information relating to proliferation of weapons of mass destruction. A warrant requirement would have precluded the U.S. person queries because there would have been no probable cause at the time that the U.S. person in contact with the foreign intelligence officers was a foreign power or agent of a foreign power. The purpose of the queries was to help FBI quickly make that determination before deciding whether to treat the U.S. person as a suspect or a victim.

(U) 3. U.S. person queries are critical to FBI's efforts against Chinese intelligence officers regularly reaching out to hundreds of Americans to try to recruit them as assets. When FBI sees contacts between these U.S. persons and Chinese intelligence officers, queries of those U.S. persons' identifiers in the Section 702 collection enables FBI to quickly identify who might be unwitting in their communication with a Chinese intelligence officer and in need of a defensive briefing, versus those who might be all the way through the recruitment cycle and already working as an asset for a foreign intelligence service inside the United States. In the latter case, FBI then transitions to other authorities, such as the traditional FISA Title I authority or criminal legal authorities, to investigate the U.S. person. In one such case, U.S. person queries of Section 702-acquired information from the targeting of a Chinese intelligence officer helped FBI to quickly identify a former U.S. clearance holder who was recruited by, and working with, a Chinese intelligence service. Based on results of these U.S. person queries of Section 702 data, FBI identified a need to conduct an independent investigation of this U.S. person and obtained a warrant in order to do so.

(U) A warrant, or any other court order, required for every U.S. person query conducted would undoubtedly slow down FBI and the intelligence agencies' ability to do their jobs. The FISC is also not resourced to process the volume of warrants that would be required. FBI conducted over 119,000 unique U.S. person queries from December 2021 to November 2022. The highest volume of FISA Title I and/or Title III applications the FISC ever processed in a year was 2,370 in 2007. More importantly, many of the instances in which FBI and the intelligence community conduct U.S. person queries would not meet the standard of probable cause required for obtaining a Title I warrant. Additionally, U.S. person queries could retrieve communications

[redacted]

[redacted]

between non-U.S. persons outside of the United States—who do not have Fourth Amendment rights—discussing a U.S. person. The claim to U.S. person privacy rights is further weakened when U.S. persons, particularly those that are not individual people, are the subjects of non-U.S. persons' communications lawfully-collected by the government.

(U) Outside the context of FISA and national security investigations, querying lawfully collected information is a common practice for investigators, and courts have not required that the government obtain a warrant to conduct these kinds of routine database checks. For instance, an FBI agent conducting a criminal investigation of a U.S. person suspected of money laundering can simply query that person's identifiers in FBI's non-FISA data, which include information FBI has previously collected in other investigations using, for example, criminal search warrants; witness interviews; or information provided by other federal agencies, foreign governments, or a human source. There is no requirement to go back to a court for authorization to conduct those queries. Among the various tools FBI is permitted to use in its investigations, conducting a database check to examine existing government records is considered to be among the least intrusive investigative steps FBI can take. A requirement to establish probable cause and obtain a warrant before querying Section 702 data with a U.S. person query term would effectively prevent the government from protecting the American people in many situations because the information is incomplete and, thus, not sufficient to meet the probable cause standard. In addition, in many cases, the purpose of the query is to protect a U.S. person, not to connect a U.S. person to a foreign plot.

[redacted]

[redacted]

(U) Appendix IX – Transparency

(U) Some members of the public have objected to the lack of transparency with which the government administers the Section 702 program, to include NSA's inability to provide an estimate of the volume of incidental U.S. person collection, the restricted use of the *amici curiae*, and not disclosing every instance in which Section 702 information is used to build a criminal case. The Board found that Section 702 is the least secretive surveillance program in the world. The reports published and released by the government about the Section 702 program and all of its compliance issues may not be an effective means of communication with the public, but they are nonetheless transparent. No other country in the world allows its surveillance programs to be debated this publicly. The program overseers, namely ODNI and DOJ, have carried out their duties in monitoring compliance, enforcing the rules, assisting in reformations, and being open with the FISC, Congress, and the public. While FBI has also been transparent about its noncompliance, it has been too slow to demonstrate accountability. As a consequence, the actions of FBI have cast doubt on the integrity of FBI and the intelligence community writ large. To build trust with the public, the intelligence community needs to have more meaningful public engagements, not just about Section 702, but about today's threat landscape and how to protect Americans from foreign malign influence.

(U) Another issue that has eroded the public's trust is the government's inability to provide the public with an estimate of the scope and scale of incidental U.S. person collection. The government has not provided a satisfactory explanation to the public for why this task is impossible nor has it offered what it could in fact estimate to help provide context for the public about the scale of U.S. person communications being incidentally-collected in this surveillance program intended to target foreigners located outside the United States.

(U) NSA's inability to count incidental U.S. person communications stems from its inability to determine the location and nationality of every person associated with a target's communications collected under Section 702. It might, for example, be possible for NSA to count the number of e-mail addresses associated with each target's collected e-mail communications; however, it would take an exhaustive effort to even attempt to identify which of those e-mail addresses belonged to a U.S. person. An NSA analyst would need to manually review each e-mail as well as every e-mail address contained in each e-mail. An analyst must then examine each e-mail address in an effort to make a determination about the U.S. person status of each e-mail address. In 2015, NSA undertook several studies and estimated how large of a sample size was required to undertake this type of counting effort. NSA calculated that it would require thousands of

[redacted]

[redacted]

analysts working over a year full-time to estimate the volume of incidental U.S. person collection in this sample size. Even then, this number would contain errors because NSA simply lacks reliable locational data.

(U) Those are the technical difficulties and do not account for privacy concerns. In fact, the act of trying to identify whether the e-mail address belonged to a U.S. person would constitute a violation of privacy. As a matter of practice, NSA does not look at every e-mail in a foreign intelligence target's inbox. Allowing the e-mails that are not of foreign intelligence value to remain dormant in NSA's data repositories would better preserve U.S. person privacy.

(U) NSA spent considerable time and effort attempting several approaches to counting incidental U.S. person collection in Section 702 data, and reported its findings to Congress concluding that none of these options would provide reliable results.

[redacted]