OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act

LEADING INTELLIGENCE INTEGRATION

Office of Civil Liberties, Privacy, and Transparency

November 2017

-- Page left intentionally blank. --

Contents

EXECUTIVE SUMMARY

The Foreign Intelligence Surveillance Act (FISA) establishes an extensive legal framework under which the government can collect vital foreign intelligence while also protecting privacy and civil liberties. Questions about how the Intelligence Community (IC) protects privacy when it disseminates information arose in a recent public hearing on FISA.[1] In that hearing, the Director of National Intelligence (DNI), Daniel Coats, stated that the civil liberties and privacy officers for the relevant members of the IC would conduct a review of the policies and procedures that protect the privacy of U.S. persons in FISA disseminations.

The civil liberties and privacy officers for the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA), have carried out those reviews, in coordination with the ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT).[2] Their reports—attached as Annexes to this report—collectively document the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations.[3]

To begin with, individuals may be subject to FISA surveillance only if certain specific conditions are met. For example, to conduct electronic surveillance targeting someone inside the United States, FISA Title I[4] requires that the government submit an application for review and approval by the Foreign Intelligence Surveillance Court (FISC) demonstrating, among other things, probable cause to believe that the target is a foreign power or an agent of a foreign power. Section 702 of FISA may be used only to target non-U.S. persons reasonably believed to be located outside the United States, who are expected to possess, receive, and/or are likely to communicate foreign intelligence information responsive to a FISC-approved certification executed by the Director of National Intelligence and the Attorney General.[5] Section 702 may *not* be used to target anyone in the United States; nor may it be used to target a U.S. person anywhere in the world.

In addition to such limitations, FISA specifically requires agencies to follow procedures designed to minimize the collection, retention, and dissemination of information concerning unconsenting U.S. persons. These are known as "minimization procedures," and FISA requires that they be adopted by the Attorney General and approved by the FISC. The FISC has

---

[1] The hearing was on the reauthorization of Section 702 of FISA, and took place before the Senate Select Committee on Intelligence. It is currently set to sunset on December 31, 2017.

[2] This report also includes a review of the FISA dissemination procedures for National Counterterrorism Center (NCTC).

[3] As discussed in the attached reports, this framework is consistent with the Fair Information Practice Principles as applicable to intelligence activities.

[4] Title I, addressing electronic surveillance for foreign intelligence purposes, is codified at 50 U.S.C. §§1801-1812. Title III, addressing physical searches for foreign intelligence purposes, is codified at 50 U.S.C. Sections 1821-1829. Both require probable cause findings from the FISC and are sometimes referred to as "traditional FISA."

[5] Title VII, including Section 702, was enacted in 2008 as the FISA Amendments Act (FAA). It is codified at 50 U.S.C. §1881a. Throughout this report, this legal authority will be referred to as Section 702 of FISA or simply Section 702.

specifically approved NSA, FBI, CIA, and NCTC to directly receive unminimized information collected under FISA authorities. These agencies must in turn abide by minimization procedures directly applicable to each (further described in the attached reports). The specifics of each agency's minimization procedures vary based on the unique mission and operational environment of each agency.

As illustrated in the Annexes, there are many layers of protections prior to the dissemination of information, such as collection restrictions, training requirements, retention limitations, and access controls. In addition, agencies may disseminate information only to authorized recipients. In general, for non-public information concerning an unconsenting U.S. person, agencies may only include the identity of the U.S. person if it itself constitutes foreign intelligence, is necessary for the recipient to understand the foreign intelligence being transmitted, or is evidence of a crime.[6] Agency minimization procedures generally provide for the substitution of a generic phrase or term, such as "U.S. person 1" or "a named U.S. person" when including the identity of the U.S. person does not meet dissemination criteria. This is informally referred to as "masking" the identity of the U.S. person.

Agency policy and practice can include additional protections. For example, NSA, as a matter of policy, in many cases requires that U.S. person identities be masked, with the identity provided only after a request by an authorized recipient and approval by a senior official. This is true even if including the identity in the original report would have been permitted by the minimization procedures. Moreover, an IC Directive mandates additional protections for the inclusion of information identifying a member of Congress or congressional staff in an intelligence report (these so-called "Gates Procedures" are further described in this report). In addition, the IC applies important protections to information about non-U.S. persons as well, pursuant to Presidential Policy Directive-28 on Signals Intelligence (PPD-28) (also further described below).

A robust and multi-layered compliance and oversight framework, involving all three branches of the government, ensures that the minimization procedures are followed. The attached reviews included examination of a sample of disseminations, and no significant compliance issues were identified. Information collected under FISA is classified, and the unauthorized disclosure of that information is prohibited and may result in criminal liability.

Although the current procedures, processes, and practices described in these reports provide robust privacy protections for U.S. person information in intelligence disseminations, the IC continues to seek ways to improve privacy protections and transparency. These reviews provide additional transparency so that the public can better understand how these protections work.

[6] *See* FISA §§ 1801(h), 1821(4), and 1881a(e). As further discussed in the Annexes, some procedures list particular dissemination criteria.

I. Introduction

A. Purpose and Scope of Report

On June 7, 2017, during a public hearing on Section 702 of the FISA before the Senate Select Committee on Intelligence (SSCI),[7] DNI Coats stated that the civil liberties and privacy offices for the Office of the DNI (ODNI) and certain IC elements would review procedures relating to protecting U.S. person identities in intelligence disseminations. Pursuant to the DNI's direction, the civil liberties and privacy offices for the NSA, FBI, and CIA, each conducted a review of their agencies' dissemination procedures and practices under certain FISA authorities.[8] These reviews were conducted in coordination with CLPT. Each office prepared a report detailing their reviews.[9] Those reports are attached.[10] These reports have been prepared for public release, consistent with the *Principles of Intelligence Transparency*.[11] Many of these processes have been discussed in previously released documents, including the actual procedures approved and opinions issued by the FISC.[12] Those documents should be reviewed for further information on the applicable protections as those processes will not be detailed in this report.

B. FISA Background

Title I and Title III of FISA apply respectively to the conduct of electronic surveillance and physical searches for foreign intelligence purposes of persons, facilities, or property. Both require that the government file an application asking the FISC to authorize (a) the electronic surveillance of a facility (e.g., telephone number, email account) or place being used or about to be used by the by a target for Title I or (b) the search of premises or property that is or is about to be owned, used, possessed by, or in transit to or from a target for Title III. For such an application to be approved, the FISC must issue an order finding there is probable cause that (i) the targeted individual is a foreign power or an agent of a foreign power and (ii) the facility, place, premises, or property is being used or is about to be used by that individual. Additionally, prior to granting the request, the FISC must agree that the government's proposed collection

---

[7] The SSCI, the House of Representatives Permanent Select Committee on Intelligence (HPSCI), the Senate Judiciary Committee (SJC) and the House of Representatives Judiciary Committee HJC) have statutory oversight authority over FISA, including Section 702. *See* FISA §§ 1808, 1826, 1871, 1881a(l)(1), and 1881f.

[8] The specific FISA authorities covered by each review are identified in the reports. All reviews cover Title I and Section 702 of FISA.

[9] The reviews cover general agency practices and processes in applying protections, but does not include any information about specific individuals, investigations, or cases.

[10] This report also includes a review of NCTC's FISA minimization procedures concerning the protection of U.S. person information during dissemination.

[11] The IC's *Principles of Transparency* are available on the ODNI's Tumblr website *IC on the Record* at https://www.dni.gov/index.php/how-we-work/transparency.

[12] Many of the applicable documents have been publicly released, in redacted form, on *IC on the Record*. CLPT's *Guide to Posted Documents Regarding Use of National Security Authorities* (posted on the left side on the homepage of *IC on the Record*) at https://www.dni.gov/files/CLPT/documents/Guide_to_Posted_Documents.pdf. This guide helps readers navigate the location of the many relevant documents such as the agencies' Section 702 minimization and targeting procedures, *Summary of Section 702 Oversight*, the *FISA Amendments Act: Q&A*, relevant FISC Opinions, and *Section 702 Joint Assessments of Compliance by the DNI and Attorney General*.

techniques and minimization procedures adequately protect U.S. person information acquired in the course of the collection activity.[13]

Section 702 permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures and minimization procedures that they satisfy the statutory requirements and are consistent with the Fourth Amendment. Instead of issuing court orders that specify particular targets or facilities, under Section 702, the FISC issues an order approving annual certifications submitted by the Attorney General and the DNI after finding that the statutory requirements have been met. These statutory requirements include, among other things, that the Attorney General and DNI have adopted targeting and minimization procedures for the acquisition that meet the statutory standards and are consistent with the Fourth Amendment, and that a significant purpose of the acquisition is to obtain foreign intelligence information.[14]

For historical context, the concept of protecting U.S. person information acquired through surveillance for foreign intelligence is not a new concept nor is it unique to Section 702. Prior to the enactment of FISA in 1978, Congress was aware that *non-targeted* U.S. person information would likely be incidentally collected -- that is when, for example, a target communicates with or about a non-target U.S. person.[15] Anticipating such incidental collection, Congress required that rules known as minimization procedures be statutorily required by FISA so as to protect such U.S. person information that has been incidentally collected.

Specifically, FISA Section 1801(h) defines minimization procedures, to include Section 702, as (in pertinent part) specific procedures, adopted by the Attorney General that are reasonably designed to:

> (1) [m]inimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate *foreign intelligence information*; (2) [prohibit nonpublicly available unconsenting U.S. person information from being disseminated when that information is not

---

[13] For additional information, *see FISA Amendments Act: Q&A*, page 2, posted on *IC on the Record* on April 19, 2017. *See also* the 2016 *Statistical Transparency Report Regarding Use of National Security Authorities (*hereafter the *Annual Statistical Transparency Report)*, pages 2-4, posted on *IC on the Record*.

[14] *See FISA Amendments Act: Q&A*, page 3 and the 2016 *Annual Statistical Transparency Report*, pages 5-7.

[15] As stated in the legislative report that accompanied the FISA bill:

> The minimization procedures of the bill provide vital safeguards because they regulate the acquisition, retention, and dissemination of information about U.S. persons, including persons who are not the authorized targets of surveillance. For example, an entirely innocent American might use a telephone that is tapped to target someone else. Or an American might talk on the phone to a foreign official who is under surveillance for purposes unrelated to the particular conversation. The procedures also protect Americans who are not parties to a communication, but who are referred to in the communication; such information has in the past been disseminated for improper purposes.

H.R. Rep 95-1283, at 54-55 (1978).

> foreign intelligence information but when] such person's identity is *necessary to understand foreign intelligence information or assess its importance*; (3) allow for the retention and dissemination of information *that is evidence of a crime* which has been, is being, or is about to be committed and that is to be retained and disseminated for law enforcement purposes; [.][16]

Minimization procedures must be reviewed and approved by the FISC as part of the government's application pursuant to Titles I or III of FISA, or when approving a Section 702 certification.

Prior to 9/11, when FBI initiated counterterrorism FISA collections under Titles I and III, it could only disseminate such information to CIA and NSA after it had first reviewed and minimized the information. This was a time-consuming process. Following the 9/11 attacks, the government applied to the FISC for FBI's unminimized FISA counterterrorism information to be provided to CIA and NSA directly, so that their counterterrorism analysts could much more quickly and effectively apply their own knowledge and expertise to identify actionable intelligence. In 2002, the FISC approved the request, and required each agency to apply its own set of FISC-approved minimization procedures to the information. In 2012, the FISC further authorized the FBI to share this unminimized counterterrorism information with NCTC provided that NCTC likewise handled, retained, and disseminated such information pursuant to FISC-approved minimization procedures. After Section 702 was enacted in 2008, the FISC approved minimization procedures for NSA, FBI, and CIA. In 2017, the FISC also approved minimization procedures for NCTC to receive unminimized Section 702 information related to counterterrorism.[17]

II. How is U.S. Person Information Protected in FISA Disseminations

A. What Happens Before Dissemination

Before an agency can disseminate information, it must first obtain it. Each year the President sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process. The DNI is responsible for translating these intelligence priorities into the National Intelligence Priorities Framework, or NIPF.[18] The priorities in the NIPF are at a fairly high level of generality, and apply to all intelligence activities. Through systematic interagency processes, these priorities are translated into more specific information needs and

---

[16] 50 U.S.C. §§1801(h)(1)-(3) and 1821(4)(A)-(C) (emphasis added); *see also* 50 U.S. C. §1881a(e)(1) ("the Attorney General, in consultation with the Direction of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4)").

[17] Previously, NCTC received certain *evaluated* counterterrorism information acquired pursuant to Section 702, to which it applied a more limited set of Section 702 minimization procedures. With the FISC's approval of the 2016 Certifications, the FISC approved minimization procedures for NCTC so that it could start receiving certain unminimized counterterrorism information acquired under Section 702.

[18] Intelligence Community Directive (ICD) 204 provides further guidance on the NIPF, and is available on www.dni.gov.

collection requirements. Agencies determine how to satisfy those needs and requirements based on their capabilities and authorities.

If an agency determines that an intelligence priority can be met through use of FISA authorities, then the multiple legal requirements under FISA must be carefully reviewed and met. For example, for Title I collection, the government must be able to meet the probable cause standard, among other requirements, before collection can be initiated. For Section 702 collection, the government must follow the FISC-approved targeting procedures and conclude that it has a reasonable belief that the target is a non-U.S. person located outside the United States, and that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information that fits within an approved certification.

After information is acquired, then each agency that has access to that information may only retain the information pursuant to the FISC-approved minimization procedures applicable to that information. For example, for Section 702 information, this means that the agencies may only retain unevaluated information for the duration specified in their minimization procedures; that only trained and authorized personnel may access the information; and that certain rules must be followed to query the information.[19]

Thus, information is eligible for dissemination only after it has been collected pursuant to an intelligence priority established by the NIPF, collected in satisfaction of the strict legal requirements imposed by FISA, and retained in accordance with FISC-approved minimization procedures.

B. Dissemination Protections

The basic standard for dissemination of U.S. person information is set forth in FISA's definition of "minimization procedures." This applies across the IC and across the traditional and Section 702 FISA authorities. Information concerning U.S. persons may be disseminated if it is itself foreign intelligence or necessary to understand foreign intelligence or assess its importance, or if it is evidence of a crime.[20] Each agency's attached report provides detailed information about how this general standard is implemented in their procedures and practices. Our review of NCTC's practices is in Annex 4.

As is evident from the attached reports, the minimization procedures adopted by each agency are different, reflecting the different mission and operational environment of each agency. NSA is focused on collecting and analyzing signals intelligence (SIGINT) for foreign intelligence and counterintelligence purposes, to include support to military operations and force protection. Accordingly, it plays a key role in implementing Section 702, which is focused on the collection of foreign intelligence by targeting non-U.S. persons outside the United States. CIA is

[19] Note that CIA, FBI, and NCTC receive only a subset of the Section 702 information that is collected by NSA; thus, their minimization procedures apply only to that subset of unminimized information that they obtain from NSA.

[20] Note that for NSA, CIA, and NCTC, any dissemination of U.S. person information as "evidence of a crime" must be made pursuant to applicable crimes reporting procedures.

a human intelligence agency that conducts clandestine intelligence activities outside the United States. In general, CIA does not conduct electronic surveillance or physical searches inside the United States. Instead, CIA receives and analyzes unminimized FISA information collected by NSA and FBI in support of its foreign intelligence mission. FBI has both foreign intelligence and law enforcement responsibilities and authorities, and operates mainly within the U.S. It is expected to be the last line of defense against the full range of threat actors, including terrorists, spies, international criminal organizations, and malicious cyber actors. Its operations routinely bring it into contact with U.S. persons. NCTC is the primary organization within the U.S. government responsible for analyzing and integrating all terrorism and counterterrorism information possessed or acquired by U.S. government agencies. The attached reports provide further information on each agency's mission and minimization procedures.

That said, the minimization procedures share key elements in common. As a general matter, a U.S. person's actual identity may be included in an intelligence report at the time it is first prepared and disseminated if such inclusion meets the agency's minimization standard (e.g., whether the identity is foreign intelligence, necessary to understand foreign intelligence or assess its importance, or is evidence of a crime).[21] If the standard is not met, agencies substitute a generic term or phrase for the U.S. person identity, such as "U.S. Person 1" or "a named U.S. person." This is informally referred to as "masking" the identity.[22] However, in some instances, even when the standard is met, an agency may "mask" as U.S. person identity for additional protections. In addition, only authorized recipients may receive disseminated reports. Agency personnel undergo extensive training on the rules for disseminating U.S. person identities. Records of disseminations are maintained for compliance and oversight purposes.

While the requirements for including—or masking—U.S. person identities are generally the same across agencies, internal policies and practices may result in additional protections.

1. NSA

For example, as described in the NSA report, NSA collects, analyzes and disseminates signals intelligence to other government agencies that need that information to carry out their duties. NSA has adopted additional protective measures to safeguard U.S. person information in its disseminations. In general, when U.S. person information is referenced it is masked, often because only a subset of the authorized recipients have a "need to know" to perform their official duties. If the U.S. identity is masked to protect the privacy of the individual or entity, it will be referenced using a generic term, such as "a named U.S. company" or "a named U.S. person." NSA provides its analysts with comprehensive guidance on how to properly reference masked U.S. identities in SIGINT. This guidance emphasizes the need to avoid contextual identification, which occurs if the identity of a U.S. person is masked, but so many other pertinent details are included that the authorized recipient can identify the U.S. person from the context. NSA also responds to customer initiated, post-publication "identity release" requests to approve the unmasking and dissemination of U.S. person identity information originally shared as masked in

[21] Note that agency minimization procedures may include lists of more detailed criteria.

[22] Note that if the standard is not met for including the identity of the U.S. person, the report may well be written without even any reference whatsoever to the fact that a U.S. person was involved, thus obviating the need for masking.

a serialized report. Recipients can request that NSA provide the identity of a masked U.S. person referenced in a serialized SIGINT report if the recipient has a legitimate need to know the identity and has the appropriate security clearances, and if the dissemination would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence or counter intelligence information or assess its importance.) Requesters must include a justification for access to U.S. person information. Only designated NSA officials may approve requests pursuant to NSA policy.

2. CIA

As described in the CIA report, CIA produces and disseminates to policymakers and partners all-source analysis in order to provide tactical and strategic advantage to the United States. In determining what information is to be disseminated to policymakers and partners, including but not limited to U.S. person information, CIA must assess whether the specific U.S. person information is necessary to understand the foreign intelligence information in light of the information that is to be disseminated and the needs and authorities of the recipients of the information. Consistent with CIA's foreign intelligence mission, this means that, for strategic-level reporting, U.S. person identifying information is often not just deleted or replaced with a generic term, but instead never referenced in the first place. On the other hand, particularly in instances regarding more "tactical" information that is disseminated to a limited number of individuals or entities directly involved in countering the foreign intelligence threat at issue, CIA personnel may make the determination at the time of dissemination that the U.S. person's information and identity are necessary to understand the foreign intelligence information and will therefore disseminate this identifying information in the first instance, as opposed to deleting the U.S. person information or replacing the U.S. person identity with a generic term.

3. FBI

As described in the FBI report, in order to disrupt foreign threat actors and their plans and activities, it is critical that the FBI collect foreign intelligence information that is timely, accurate, and informative within the bounds of their legal authorities and with due regard for the rights of Americans. Importantly, the FBI must be able to effectively and efficiently "connect the dots" in order to prevent terrorist attacks, stop espionage, and interdict malicious cyber data. Through rigorous analysis of lawfully acquired data, the FBI must find links between threat actors, understand their plans, and disrupt their activities. For dissemination of U.S. person information in finished intelligence products, the products undergo multiple layers of review depending on the particular product and recipient. If classified information about a U.S. person is to be given to a foreign government, there are several additional levels of approval required, including legal approval, and must be reported to the Attorney General, or designee, on a quarterly basis.

4. NCTC

As described in the NCTC report, NCTC receives certain unminimized FISA information related to counterterrorism. NCTC began receiving certain unminimized FBI counterterrorism information (collected under Titles I and III) in 2012, and just recently was authorized to receive

unminimized information under Section 702 relating to counterterrorism. NCTC's minimization procedures are further described in Annex 4.

C. Gates Procedures.

In addition, the IC has implemented a specific process to govern the dissemination of "congressional identity information." This process was first established by former Director of Central Intelligence (DCI) Robert Gates (hereafter the "Gates Procedures") in a 1992 letter which memorialized commitments previously made to Congress. In January 2017, the DNI incorporated the Gates Procedures into the formal IC policy framework as an annex to Intelligence Community Directive (ICD) 112.[23]

The Gates Procedures provide that, unless a specific exception applies, prior approval must be obtained from ODNI if information identifying Members or their staff by name or by individually identifying titles or characteristics (congressional identity information) is included in disseminated intelligence reports outside of the requesting IC element within the Executive Branch. IC elements must submit these requests for approval to ODNI on a case by case basis, including, among other things, the officials to whom the element seeks to disseminate the congressional identifying information to and the element's reasons for requesting the unmasking of congressional identity information. The Gates Procedures also provide detailed rules for subsequent congressional notifications concerning any disseminations of congressional identity information.

D. Non-U.S. Person Protections

Non-U.S. persons also benefit from many of the protective rules proscribed by FISA and the minimization procedures. As a baseline, a significant purpose of collection pursuant to Titles I and III or Section 702 of FISA must be the acquisition of foreign intelligence information, as defined by FISA, regardless of U.S. person status. For traditional FISA authorities, if the non-U.S. person is located *inside* the United States, the government must seek FISC approval based upon a probable cause finding. For Section 702, collection is targeted (not bulk), and must be limited to non-U.S. person targets located outside the United States who are likely to possess, receive, and/or are likely to communicate foreign intelligence information that is linked to one of the FISC-approved certifications.

Moreover, PPD-28 requires agencies to establish policies and procedures reasonably designed to minimize the retention and dissemination of personal information collected from signals intelligence activities. NSA, FBI and CIA have completed those policies and procedures, which are publicly posted.[24] Under PPD-28 §4(a), "[p]ersonal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333."

---

[23] The *Gates Procedures* were posted on *IC on the Record* on July 10, 2017; ICD 112 was posted on www.dni.gov.
[24] Links to these documents can be found on the *Guide to Posted Documents*, which is available on *IC on the Record*.

III. Oversight & Compliance

The IC's use of FISA is subject to robust oversight regime that begins with each agencies' internal oversight offices (e.g., compliance, legal, civil liberties and privacy, and inspector generals), continues with oversight by the DOJ, and extends to outside the executive branch with oversight by the FISC and Congress. Significantly, both the FISC and Congress are notified of every identified compliance incident. For example, as required by FISA, Congress is kept fully informed of IC's implementation of FISA Titles I and III and Section 702 authorities through semiannual reports and through copies of FISC opinions that relate to significant interpretations of law. Additionally, certain formal entities, like the Privacy and Civil Liberties Oversight Board (PCLOB), may choose to further examine and make recommendations regarding FISA (regardless of the FISA provision) as it pertains to counterterrorism matters. The following describes the compliance and oversight of Section 702 collection.

A. Agency Compliance and Training

As detailed in ODNI's *FISA Amendments Act: Q&A* background paper and as further described in these reviews, the intelligence agencies themselves carry out compliance and oversight of activities conducted under FISA. For instance, all IC personnel who work with Section 702-acquired information must be trained in their agencies' Section 702 minimization procedures, and are also trained in how to report potential compliance issues to their agency's respective FISA program managers and other offices with oversight responsibilities. Additionally, internal bodies at the IC elements involved in implementing Section 702, such as compliance officers, civil liberties and privacy officers, and inspectors general, are involved in monitoring their agencies' compliance with FISA and the Section 702 targeting and minimization procedures.

B. DOJ and ODNI Oversight

Section 702 requires ODNI and DOJ to jointly conduct oversight of Section 702 activities. Agencies using Section 702 authority must report any potential incidents of noncompliance promptly to DOJ and ODNI. At least once every 60 days, DOJ and ODNI conduct oversight of the agencies' activities under Section 702. These reviews are normally conducted on-site by a joint team from DOJ's National Security Division (NSD) and ODNI. The team evaluates and, where appropriate, investigates each potential incident of noncompliance, and conducts a review of agencies' targeting and minimization decisions. DOJ reports any identified incidents of noncompliance to the FISC.

C. FISC and Congressional Oversight

Section 702 requires the FISC to review the government's 702 certifications, targeting procedures, and minimization procedures for compliance with statutory and Fourth Amendment requirements. NSD reports any identified Section 702 compliance incidents to the FISC, which often asks follow-up questions and holds hearings on Section 702 related compliance matters.

The FISC takes those incident reports into consideration when making determinations on any subsequent certifications and targeting and minimization procedures submitted by the government.

Additionally Section 702 requires that Congress receive regular reports describing IC elements' use of Section 702 and any identified instances of noncompliance. Specifically, the statute requires the Attorney General and the DNI to provide the Intelligence and Judiciary Committees with semiannual assessments of compliance with key requirements under FISA Section 702 (these reports are often referred to as "Joint Assessments"). These Joint Assessments discuss trends in compliance and may include recommended changes to help reduce compliance incidents. Several of these past reports are available on *IC on the Record*. In addition, the statute requires the Attorney General to report twice per year on every identified incident of noncompliance relating to Section 702 that occurred during the applicable reporting period; requires certain inspectors general and certain heads of agencies to report on compliance with Section 702; and requires that Congress receive copies of the Section 702 certifications submitted to the FISC and copies of certain significant FISC opinions and related pleadings. Finally, FISA requires declassification review and public release of certain FISC opinions, including those related to Section 702, and the public reporting of certain statistics related to the government's use of Section 702.

D. Strong Compliance Record

As reported in the Joint Assessments, ODNI and DOJ have consistently found that the agencies continue to implement the Section 702 procedures and follow the Section 702 Attorney General guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702, including the minimization procedures and the rules regarding disseminating U.S. person information. As DNI Coats explained on June 7, 2017, during an open hearing in front of the SSCI, ODNI and DOJ's audits have revealed an extremely low incident rate. The DNI explained that, while mistakes have occurred, "any system with zero compliance incidents is a broken compliance system, because humans make mistakes." The DNI emphasized that when the government finds compliance incidents, those incidents are reported and corrected. ODNI and DOJ assesses that the consistently low compliance incident rate is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures.

As it pertains to reviewing dissemination of Section 702 information, ODNI and DOJ's National Security Division (NSD) review many of the agencies' disseminations as part of the oversight reviews to assess compliance with each agency's respective minimization procedures and with statutory requirements.[25] NSD and ODNI examine the disseminations to assess whether

[25] For example, as it pertains to NSA, NSD currently reviews all of the serialized reports (with ODNI reviewing a sample) that NSA has disseminated and identified as containing Section 702-acquired U.S. person information. For CIA and NCTC, NSD currently reviews all dissemination (with ODNI reviewing a sample) of information acquired under Section 702 that the agency identified as potentially containing U.S. person information. For FBI, both NSD and ODNI currently review a sample of disseminations of information acquired under Section 702 that FBI identifies as potentially containing U.S. person information.

any information contained therein that appears to be of or concerning U.S. persons meets the applicable dissemination standard found in the agency's minimization procedures; whether other aspects of the dissemination requirements (to include limitations on the dissemination of attorney-client communications and the requirement of a FISA warning statement as required by 50 U.S.C. § 1806(b)) have been met; and whether the information disseminated is indicative of reverse targeting of U.S. persons or persons located in the United States.

The findings regarding these dissemination reviews are included in reports specific to each agency, and any compliance incidents discovered in the course of the NSD and ODNI oversight reviews are reported to the FISC pursuant to Rule 13(b) of the FISC's Rules of Procedure and to Congress in semiannual reports required under 50 U.S.C. §1881f.

E. Preventing Unauthorized Use and Improper Disclosure.

FISA provides that information acquired pursuant to FISA concerning any U.S. person may be used and disclosed only in accordance with applicable minimization procedures. It adds that no FISA information may be used or disclosed by Federal officers or employees except for lawful purposes.[26] Disseminating FISA information in a manner that violates the minimization procedures would, therefore, be a violation of the statute, as would use or disclosure of the information for unlawful purposes. As noted above, identified incidents of non-compliance with the minimization procedures, to include improper disseminations, are reported to the FISC and to the congressional intelligence committees and those incidents are remediated.

Information collected under FISA authorities is classified in order to protect intelligence sources, methods, and activities or otherwise protect the U.S. from damage to national security. Federal law criminalizes the unauthorized disclosure of classified information in certain circumstances.

The IC takes seriously its obligation to protect civil liberties and privacy through careful adherence to applicable rules and safeguards, including those embodied in the minimization procedures. In addition, the IC is firmly committed to the protection of classified information from unauthorized disclosure.

V. Conclusion

As stated in the Principles of Professional Ethics for the IC, intelligence professionals are committed to complying with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy and civil liberties. Nowhere is this more important – nor more evident – than in the scrupulous care taken to implement the rigorous legal and policy requirements that apply to the collection, retention, and dissemination of information under FISA. In particular, information that is disseminated under FISA has already undergone layers of controls, restrictions, and safeguards, and must then satisfy the strict dissemination requirements established in FISC-approved minimization procedures.

[26] *See* 50 U.S.C. §§1806, 1825, and 1881e.

The IC must continue to provide intelligence to officials who need the information to protect the security of the nation and its allies, and must do so within the framework of protections and oversight that has been established to protect privacy and civil liberties. This framework is complex and multi-faceted. Minimization procedures vary by agency, and different procedures may be approved by the FISC for different activities within an agency. This is by design. Congress stressed the need for procedures to be tailored for different circumstances. The resulting complexity, however, raises challenges for both those implementing these authorities and those overseeing them. The IC must continue to work on consistency and harmonization, as appropriate, including with respect to how oversight is conducted. At the same time, the IC must continue to seek ways to improve protection of privacy and civil liberties.

These reviews by civil liberties and privacy officials at ODNI, NSA, FBI, and CIA, also reflect the important roles those officials play within the IC. IC elements should continue to fully support these officials in the performance of their duties, particularly with regard to the exercise of FISA authorities, which directly implicate privacy and civil liberties concerns.

These reviews also illustrate the importance of transparency. Historically, many of the documents establishing this framework were classified and not available to the public. In recent years, much progress has been made in releasing information from these documents, and providing context and explanations to make them more readily understandable. We trust that these reviews are a further step in enhancing public understanding of these key authorities. It is important to continue with transparency efforts like these on issues of public concern, such as the protection of U.S. person information in FISA disseminations.