Federal Bureau of Investigation

Privacy & Civil Liberties Officer, Office of the General Counsel

Protections for United States Person Information Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act

MEMORANDUM FOR Office of Civil Liberties, Privacy, and Transparency, Office of the Director of National Intelligence (ODNI)

FROM: Federal Bureau of Investigation (FBI) Privacy and Civil Liberties Officer (PCLO)

SUBJECT: FBI Review of Title I and Section 702 of Foreign Intelligence Surveillance Act (FISA) Dissemination Protections for U.S. Person Information

I. Executive Summary:

In response to the Director of National Intelligence's request for the ODNI, National Security Agency (NSA), Central Intelligence Agency (CIA), and FBI Privacy and Civil Liberties Offices to review the procedures relating to the privacy protections afforded to U.S. persons in relation to disseminations of finished intelligence information collected under Title I and Section 702 of FISA, the FBI's PCLO and the Privacy and Civil Liberties Unit (PCLU) in the Office of General Counsel (OGC) submit this report examining the FBI's procedures and practices. As set forth below, the FBI incorporates privacy and civil liberties protection into all stages of intelligence activities in accordance with the Constitution, U.S. statutes, executive orders, presidential directives, federal regulations, and civil liberties and privacy policies such as the Fair Information Practice Principles (FIPPs).[1]

In preparing this report, the PCLO and PCLU reviewed: applicable privacy protections governing the acquisition, retention, and dissemination of U.S. person information acquired under Title I and Section 702 of FISA; FBI policies, procedures, and practices; Department of Justice (DOJ) guidance, training, oversight, and compliance activities associated with the dissemination of FISA-acquired information; and a sample of disseminated information.

As detailed below, this review[2] of the FBI's procedures and practices with respect to the dissemination of FISA-acquired information concerning U.S. persons found:

- The FBI adheres to specific Foreign Intelligence Surveillance Court (FISC)-approved procedures to minimize the dissemination of U.S. person information. Consistent with the definition of "minimization procedures" in FISA, these procedures limit the dissemination of U.S. person information to three categories: (1) information that reasonably appears to be foreign intelligence information; (2) information which is necessary to understand foreign intelligence information or assess its importance; or (3)

[1] The FIPPs are a set of principles that are rooted in the Privacy Act of 1974, and include: transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; accountability; and auditing. In addition to all of the FISA-specific provisions contained here, the Privacy Act of 1974 also governs the dissemination of all U.S. person information from an FBI System of Records. *See* Privacy Act of 1974, 5 U.S.C. § 552a, as amended. The FIPPs are the standard by which the government and many in the private sector assess privacy impacts and develop mitigations. Given ODNI's mandate with regard to this report, the pertinent FIPPs are discussed in the context of the FBI's FISA minimization procedures; internal policies and practices; training; compliance and oversight; and transparency.

[2] Information used for this review was current as of July, 2017.

evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

- Dissemination of FISA-acquired information regarding U.S. persons is only permitted after removing, or substituting a characterization for, information of or concerning a U.S. person. Such dissemination must receive multiple levels of approval before the information may leave the FBI in finished intelligence.
- If U.S. person information does not meet one of the above three categories, it is not disseminated.
- Consistent with prior DOJ/ODNI oversight reviews, the PCLO and PCLU found no intentional violations of FBI's procedures governing the handling and dissemination of U.S. person information.
- The FBI has extensive and effective training for all those with access to raw or "unminimized" FISA-acquired information regarding how to access, handle, or use that FISA-acquired information in any way.
- Compliance and oversight activities are carried out internally by the FBI Inspection Division, FBI Office of Integrity and Compliance (OIC), FBI OGC's National Security and Cyber Law Branch (NSCLB), FBI PCLO, PCLU, DOJ Office of Intelligence (OI), and DOJ Office of the Inspector General. External compliance and oversight activities are conducted by ODNI, the Privacy and Civil Liberties Oversight Board (PCLOB), Congress, and the FISC.

II. FBI Mission to Protect the American People and Uphold the U.S. Constitution:

The FBI's mission is to protect the American people and uphold the Constitution of the United States. The FBI shares this mission with other elements of the Intelligence Community, but the Bureau's role is unique for several reasons. First, the FBI has both foreign intelligence and law enforcement responsibilities and authorities. In addition, the FBI operates mainly within the U.S. and 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. Because of the domestic focus, the FBI interacts primarily with U.S. citizens and other people in the United States. The FBI is accustomed to that, and all of its internal policies and procedures are designed to appropriately protect the privacy and civil liberties of the substantial number of U.S. persons with whom it comes into contact. With respect to terrorism, the FBI is expected to prevent all terrorist attacks from happening – not merely investigate terrorism crimes after they occur – by leveraging all of the FBI's intelligence and investigative resources.

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 our 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 before it occurs, 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.

Among other things, since 9/11, the FBI has dedicated considerable time, effort, and money to develop and operate a federated database environment for its agents and analysts to review

information across multiple datasets to establish links between individuals and entities who may be associated with national security and/or criminal investigations. This allows FBI personnel to connect dots among various sources of information in support of the FBI's investigations, including accessing data collected pursuant to FISA in a manner that is consistent with the statute and applicable FISA court orders. The FBI has done this by developing a carefully overseen system that enables its personnel to conduct database checks that look for meaningful connections in its data in a way that protects privacy and guards civil liberties. Maintaining the capability to conduct federated database checks is critical to the FBI's success in achieving its mission.

III. Training:

Pursuant to the FBI FISA and Standard Minimization Procedures (SMP) Policy Guide,[3] all FBI personnel, including contractors, task force officers, and others operating under FBI supervision and control, who will be drafting FISA requests or working with DOJ to draft FISA applications, must complete FISA Accuracy training to learn how to properly draft Title I (and Title III) FISA applications. Additionally, they must complete FISA SMP training and the Section 702 Retention 2011 course concerning how to properly access, handle, or use un-minimized or "raw" FISA-acquired information, as well as how to handle minimized FISA-acquired information. The FISA SMP training also includes specific Section 702 instructions.[4] In addition to the above FISA trainings, authorized FBI employees must successfully complete the FISA 702 Nominations course (and refresher training every two years) before they can nominate facilities for acquisition under Section 702.[5] Those submitting Section 702 requests must also complete the FISA SMP and SMP Policy Implementation Guidelines course and the FISA Section 702 Retention 2011 course.

From a privacy and civil liberties perspective, the FBI's overall FISA training program provides substantial instruction regarding the protection of U.S. person information. For example, FBI employees are given detailed scenarios of what information would and would not meet the Title I and Section 702 minimization procedures' standard for maintaining information concerning U.S. persons. This training is reinforced by various oversight mechanisms, which include executive branch, judicial, and congressional oversight, as discussed in the following sections. Because all FBI employees are cleared at the Top Secret/Sensitive Compartmented Information level, they have mandatory training in the protection of information at every security level to include multiple privacy protection topics. These numerous training safeguards both prevent and mitigate threats to privacy in connection with the disclosure of U.S. person information. The trainings also help the FBI comply with the FIPPs principle of accountability which requires the FBI to provide training to all employees and contractors who use personally identifiable information (PII).

[3] (U) FBI Office of the General Counsel, *FBI FISA and SMP Policy Guide*, 0828 PG at § 4 (August 11, 2016).
[4] (U) *Id.*
[5] (U) *Id.*

IV. FISA Process:

Congress enacted FISA in 1978[6] to regulate the executive branch's use of electronic surveillance against foreign powers or their agents.[7] FISA balanced the President's Article II authorities with the need to protect the rights of Americans. The statute has been amended multiple times, most significantly in 2008, to provide an inclusive statutory vehicle for certain additional types of court-authorized foreign intelligence collection. As described below, the structure of the FISA statute itself contains numerous provisions to protect the privacy and civil liberties of U.S. persons.

a. Title I of FISA

Under Title I or traditional FISA, the FBI must file a detailed application asking the FISC to authorize the electronic surveillance[8] of an agent of a foreign power before any such surveillance may occur.[9] The FBI must demonstrate probable cause that the proposed target is a foreign power or an agent of a foreign power, and the facility or place at which electronic surveillance will be conducted is used by or is about to be used by that target. Moreover, U.S. persons cannot be agents of a foreign power based solely on activities protected by the First Amendment.

FISA limits the type of information the government may seek when targeting U.S. persons because every application for electronic surveillance must certify the information sought is "foreign intelligence information."[10] Thus, the FBI may obtain FISA surveillance authorization against a U.S. person *only*[11] if it can certify that the information it seeks is "necessary to" the government's ability to protect itself against clandestine intelligence gathering, international terrorism, or other actions undertaken by foreign powers or agents of foreign powers.[12]

---

[6] FISA, 50 U.S.C. §§ 1801-1885(c).

[7] Since its enactment, FISA has been amended several times, including by the Intelligence Authorization Act of 1995, the Intelligence Authorization Act of 1999, the USA PATRIOT Act, the USA PATRIOT Additional Reauthorization Amendments Act of 2006, the FISA Amendments Act of 2008, the FISA Sunsets Extension Act in 2012, and the USA FREEDOM Act of 2015.

[8] FISA defines "electronic surveillance" to provide greater protection to U.S. persons in the U.S. by requiring the FBI and other government agencies to satisfy the statute before targeting U.S. persons' wire or radio communications, regardless of where the monitoring occurs.

[9] The FISC is a U.S. Federal court that holds nonpublic, *ex parte* hearings (but with the ability to appoint Amicus Curiae) to issue FISA orders authorizing electronic surveillance, physical search, or acquisitions of foreign powers or agents of a foreign power. *See* 50 U.S.C. § 1803(i)(1).

[10] 50 U.S.C. § 1804(a)(6)(A), (E) (electronic surveillance) and § 1823(a)(6)(A), (E) (physical search). While this review focuses on Tile I and Section 702 of FISA, and there are some specific differences, the Title I descriptions generally apply to Title III of FISA.

[11] 50 U.S.C. § 1801(e) (emphasis added).

[12] FISA defines "agent of a foreign power" differently depending on whether the target is a U.S. person. In contrast, any person (including U.S. citizens and permanent residents) are "agents of a foreign power" if they knowingly engage in espionage for a foreign power or intelligence service, and such activities "are about to involve" a violation of any U.S. law. 50 U.S.C. § 1801(b)(2)(B). Section 1801(b)(1) covers non-U.S. persons, while § 1801(b)(2) covers "any person." A non-U.S. person is an "agent of a foreign power" if they:

- act in the U.S. as an officer or employee of a foreign power, irrespective of whether the person is inside the U.S. 50 U.S.C. § 1801(b)(1)(A); or

One of the purposes of FISA's enactment was to protect the privacy of U.S. persons.[13] In accordance with FISA, and as incorporated in the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act (SMP),[14] the definition of what qualifies as U.S. person information serves as a privacy safeguard because any such information that does not meet the minimization standard, as discussed below, will be removed or redacted in finished intelligence. Besides U.S. citizens, the definition of U.S. person[15] includes permanent resident aliens, U.S. companies that are incorporated, and unincorporated associations for which the majority of members are U.S. citizens or lawful permanent residents.[16] Therefore, any target that is a U.S. person has specific FISA protections. For example, all justifications for a proposed U.S. person target must be extensively and thoroughly reviewed by numerous lawyers, supervisors, and senior executive management at the FBI, including by the FBI Director or Deputy Director. The application is then reviewed multiple times at DOJ, including by the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security, before even being submitted to the FISC for its review and approval.

b. Section 702 of FISA

Section 702 permits the government to target the communications of non-U.S. persons located outside the United States for the purpose of acquiring foreign intelligence information. It is not bulk collection or mass surveillance,[17] it cannot be used to target U.S. persons, and the statute can only be employed with the FISC's approval.[18] Section 702 requires the Attorney General, in consultation with the DNI, adopt "targeting procedures" to (1) ensure that Section 702 acquisition is limited to targets reasonably believed to be non-U.S. persons located outside the U.S. and (2) prevent the intentional

- act for or on behalf of a foreign power that engages in clandestine intelligence activities in the U.S. contrary to U.S. interests when (1) the circumstances of such persons' presence in the U.S. "indicate that such person may engage in such activities, or (2) when such person knowingly aids or abets any person, or conspires with any person to engage in such activities." 50 U.S.C. § 1801(b)(1)(B).

[13] *See* H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1, ("FISA House Report") at 63 ("The bill is designed to provide primary protection to 'U.S. persons.'").

[14] "Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act.," Approved by John P. Carlin, Assistant Attorney General for National Security (May 17, 2016) (hereinafter "SMP"), pp. 2-3.

[15] If an individual is known to be located in the U.S., or if it is not known whether the individual is located inside or outside the U.S., the individual is *presumed to be a U.S. person*. If an individual is known or believed to be located outside of the U.S. or there are circumstances that give rise to a reasonable belief that the individual is not a U.S. person, then the individual is presumed to be a non U.S. person. 50 U.S.C. §§ 1801(i).

[16] Entities that also constitute certain foreign powers are excluded from the definition of U.S. person.

[17] If the FBI seeks to nominate a facility to NSA for targeting pursuant to Section 702, the FBI must identify each specific communications facility, such as an email address, based on an individualized assessment that it is used by a foreign intelligence target located abroad who communicates, possesses, or is likely to receive one of the categories of foreign intelligence information authorized for acquisition.

[18] The FISC approves the annual certifications submitted by the Attorney General and DNI, after which the Attorney General and DNI are authorized to approve the acquisition of FISA 702 collection for one year. However, the FISC does not approve individual target applications for acquisition of information under Section 702 like it does for traditional FISA.

acquisition of any communication in which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[19] The targeting procedures also must be approved by the FISC. Only non-U.S. persons reasonably believed to be located outside the U.S. who are assessed to communicate or receive certain categories of foreign intelligence information are authorized for targeting by the DNI and the Attorney General.[20]

Under Section 702, the FBI may nominate a facility (such as an email address) to NSA for coverage, but the FBI must assess that the target is eligible for Section 702 coverage before providing the potential target to NSA. Before targeting, the NSA must assess that the facility to be tasked for collection is a non-U.S. person reasonably believed to be located outside the United States.[21] Based on the totality of the circumstances, NSA must also reasonably assess that the subject is expected to possess, receive and/or is likely to communicate foreign intelligence information concerning a foreign power or territory.[22] FBI may nominate targets to NSA for Section 702 collection, but the ultimate decision rests with NSA.

If the target is not assessed to be a non-U.S. person outside the U.S., NSA will not pursue collection under Section 702. Targets under Section 702 collection who are subsequently found to be U.S. persons, or non-U.S. persons located in the U.S., must be detasked immediately.[23] As this demonstrates, even once the initial targeting decision is made, the FBI's due diligence continues for the entire time the facility is under collection. The targeting procedures require post-targeting analysis for all tasked facilities, including regular review to ensure that the tasked facility is used by the intended target.[24] In addition, post-targeting analysis helps ensure that if the individual enters the U.S., collection ceases.

The Attorney General has also adopted, and the FISC approved, targeting procedures (Section 702 Targeting Procedures)[25] specific to the FBI. The FBI Targeting Procedures govern the FBI's direct targeting of "electronic communication accounts/addresses/identifiers designated by the NSA"[26] as being used by a non-U.S. person reasonably believed to be located outside the United States. Before sending a request to the FBI, the NSA will follow its targeting procedures and provide an explanation to the FBI of its conclusion that the user of the facility to be tasked for collection is a non-U.S. person reasonably believed to be located outside the United

[19] 50 U.S.C. § 1881a(d)(1).
[20] 50 U.S.C. § 1881a(a), (g).
[21] *Id.* § I.
[22] *Id.*
[23] *Id.* § II.
[24] 2015 Summary of Notable Section 702 Requirements § II.
[25] Procedures Used by the FBI for Targeting non-United States Persons Reasonably Believed to Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter, "Section 702 Targeting Procedures"). A declassified version of the FBI's Section 702 Targeting Procedures, dated September 26, 2016, is available at ODNI's website, entitled IC on the Record: http://icontherecord.tumblr.com.
[26] Section 702 Targeting Procedures.

States.[27] The FBI, in consultation with NSA, will review and evaluate the sufficiency of NSA's explanation, providing additional assurances that the users of tasked accounts are non-U.S. persons located outside the U.S., in accordance with the FBI's Section 702 Targeting Procedures.[28] If the FBI concludes that the facility is not appropriate for tasking under Section 702 (i.e., the user is a U.S. person or is located in the U.S.), the FBI will inform NSA.[29] The acquisition will be terminated without delay if the NSA concludes that a subject, who at the time of targeting was believed to be a non-U.S. person, is later determined to be a U.S. person.[30] The incident will also be reported to DOJ.

Reverse targeting is specifically prohibited under Section 702.[31] "Reverse targeting" is defined as targeting a non-U.S. person who is reasonably believed to be located outside of the U.S. with the true purpose of acquiring communications of either (1) a U.S. person or (2) any individual reasonably believed to be located inside of the U.S. with whom the non-U.S. person is in contact.[32]

V. Standard Minimization Procedures:

Title I of FISA and Section 702 require that the Attorney General adopt minimization procedures that will govern access, retention, and dissemination of the information acquired pursuant to these authorities. These minimization procedures, which are specific to each agency, are approved by the FISC. In accordance with the provisions of FISA, these standard minimization procedures are reasonably designed, in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination of, information concerning unconsenting U.S. persons consistent with the need to obtain, produce, and disseminate foreign intelligence information.[33]

The FISC has approved FBI-specific "minimization procedures" for electronic surveillance as well as specific to Section 702 to ensure the FBI is handling and using lawfully collected U.S. person information. Additionally, the FISC conducts oversight to ensure these procedures meet the objectives identified by the statute.[34]

---

[27] *Id.* at §§ I(1), (2)*; see also* Memorandum Opinion at 22 [*Caption Redacted*] [*Docket No. Redacted*] 2011 WL 10945618 at *7 (FISA Ct. Oct 3, 2011) ("Bates October 2011 Opinion"). *Available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.
[28] Section 702 Targeting Procedures § I(3); Bates October 2011 Opinion at p. 22.
[29] Section 702 Targeting Procedures at § I(8).
[30] NSA Targeting Procedures §§ II, IV.
[31] *FBI FISA and SMP Policy Guide*, *supra* note 3, at § 7.3.3.1 (*citing 50 U.S.C. § 1881(a)(b)(2)*; The Attorney General's Guidelines for the Acquisition of Foreign Intelligence Surveillance Information Pursuant to the Foreign Intelligence Surveillance Act of 1978 (as amended)).
[32] *FBI FISA and SMP Policy Guide*, *supra* note 3, at § 7.3.3.1.
[33] 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A).
[34] This includes receiving and reviewing reports from DOJ about potential violations and holding hearings or issuing orders.

a. Title I of FISA

In 2016, pursuant to FISA, the Assistant Attorney General for National Security adopted, and the FISC approved the most recent "SMP for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act." These SMPs will be reviewed within five years (no later than June 1, 2021) or earlier by the Attorney General or designee, in coordination with FBI OGC to determine whether they remain appropriate.[35] Per the SMP, generally, the FBI may retain FISA-acquired information that reasonably appears to be foreign intelligence information, to be necessary to understand information or assess its importance, or to be evidence of a crime.[36]

The SMPs require, for example, FISA-acquired information to be kept under appropriately secure conditions that limit access to only those people who require access to perform their official duties or assist in a lawful and authorized governmental function.[37] The SMP also impose an auditing requirement for the FBI to "maintain accurate records of all persons who have accessed FISA-acquired information in electronic and data storage systems and audit its access records regularly to ensure that FISA-acquired information is only accessed by authorized individuals."[38]

b. Section 702 of FISA

In addition, the FISC must approve specific minimization procedures for information collected under Section 702. "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" ("Section 702 MP") were most recently signed by the Attorney General in 2016 and approved by the FISC in 2017.

As mentioned above, as soon as the FBI recognizes that the acquisition of a communication under Section 702 is inconsistent with any of the limitations set forth in

[35] "SMPs for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act," Approved by John P. Carlin, Assistant Attorney General for National Security (May 17, 2016) (hereinafter "SMP"), at 54. "A written report of such review shall be provided to the FISC within six months of the completion of the review." *Id*.
[36] *Id.* at 39.
[37] *Id.*, IIIA1, at 9.
[38] *Id.* at 17.

> Section 702(b),[39] the FBI must purge the communication.[40] Such removal will occur unless the FBI Director or Deputy Director specifically determines, in writing, on a communication-by-communication basis, that such communication is reasonably believed to contain significant foreign intelligence information; evidence of a crime that has been, is being, or is about to be committed; or contains information that should be retained for cryptanalytic, traffic analytic, or signals exploitation purposes.[41]

The instant privacy review found that the FBI's SMP and Section 702 MP, which are subject to judicial review, protect the privacy rights of U.S. persons by limiting the acquisition, retention, and dissemination of their nonpublicly available information without their consent. In addition, both sets of minimization procedures require that FISA-acquired information only be used for lawful purposes.[42] Since the FBI refers any significant minimization procedure interpretation questions to DOJ's National Security Division (NSD), this provides an added privacy protection. Ultimately, the SMP and Section 702 MP help safeguard U.S. person information at every phase of the intelligence process, including the dissemination of finished intelligence. With respect to the FIPPs, its purpose specification has been satisfied, which requires organizations to specifically articulate the authority that permits the collection of PII and the purpose(s) for which the PII is intended to be used. The information outlined above describes the statutory authority for the FBI's foreign intelligence surveillance and also explains the protections afforded to U.S. persons. This information is further contained in the FISA statute itself, the FISC-approved SMP and Section 702 MP, and other publicly released information. The data minimization FIPP states that organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s). In light of the above judicially-reviewed minimization procedures, the FBI's minimization practices satisfy this principle.

As a matter of policy and as another protection of U.S. person information, the FBI has conducted a privacy assessment of the FISA management system and the main repository that holds FISA collected information in accordance with Section 208 of the E-Government Act of

---

[39] 50 U.S.C. § 1881a(b) or Subsection 702(b) provides that "[a]n acquisition authorized under subsection (a)--
(1) may not intentionally target any person known at the time of acquisition to be located in the United States;
(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

[40] Section 702 MPs § II (A)(2). A declassified version of the FBI's Section 702 Minimization Procedures, dated September 21, 2016, is available at ODNI's website, entitled IC on the Record: http://icontherecord.tumblr.com. *See also FBI FISA and SMP Policy Guide*, *supra* note 3, at § 7.12.1.

[41] Section 702 MPs § III (A). Notwithstanding the above, if any such communications indicates that a person targeted under Section 702 has entered the U.S., nothing in the Section 702 MPs shall prevent the FBI from retaining and providing to the NSA and CIA technical information derived from such communication for collection avoidance purposes. Section 702 MPs § III (A).

[42] Section 702 MPs at p. 2.

2002,[43] Office of Management and Budget directives, DOJ policy, and specific FBI guidance.[44] Each of these requirements incorporates the FIPPs (*e.g.*, transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing) in assessing how privacy and other protections are assimilated into the two systems. We note, however, that a privacy assessment is not required by law because both systems have been designated as national security systems, as defined by the Clinger-Cohen Act.[45] However, DOJ and FBI conducted a review for internal purposes to ensure that all relevant privacy issues are addressed. These reviews ensure that U.S. person information is protected from potential misuse and/or improper dissemination.

VI. Dissemination Protections:

Under FISA, the SMP, and the Section 702 MP, the FBI may not disseminate nonpublicly available information concerning unconsenting U.S. persons[46] unless the information is reviewed and determined to meet one of three requirements: (1) it reasonably appears to be foreign intelligence information; (2) it is necessary to understand foreign intelligence information or assess its importance; or (3) it is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.[47] Before U.S. person information may be disseminated in finished intelligence products, the products undergo multiple layers of review depending on the particular product and recipient. This review helps ensure that the information in the finished intelligence product adheres to minimization procedures, classification rules, and other FBI policies. For example, 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 the disseminations must be reported to the Attorney General, or designee, on a quarterly basis.

Moreover, the both sets of minimization procedures provide that before disseminating FISA-acquired information, the FBI shall remove, or substitute a characterization for, information of or concerning a U.S. person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand or assess the importance of foreign intelligence information, or to be evidence of a crime. While the redaction of U.S. person information may commonly be referred to as "masking," the FBI does not generally use that term.

In addition, disseminations or disclosures of FISA-acquired information must be accompanied by a caveat. All caveats must contain, at a minimum, a warning that the information may not be used in a legal proceeding without the advanced authorization of the FBI or Attorney General.[48] This helps ensure the information is properly protected.

---

[43] *See* 44 U.S.C. § 3501 (note).
[44] The privacy analysis was approved by the DOJ Acting Chief PCLO.
[45] Clinger-Cohen Act of 1996, 40 U.S.C. § 11101, et seq.
[46] FISA requires the minimization procedures to not merely apply to information that *identifies* U.S. persons, but more expansively to the dissemination of "information *concerning* unconsenting U.S. persons." *702 Compliance Decision*, 2011 WL 10945618, p. 22 (FISA Ct. 2011) (emphasis added).
[47] 50 U.S.C. § 1801.
[48] *FBI FISA and SMP Policy Guide*, *supra* note 3, at §§ 7.13.4., 7.13.8.

Before disseminating FISA-acquired information, the FBI shall determine whether the information of or concerning a U.S. person meets the standards for dissemination under the applicable minimization procedures (here, either Title I or Section 702 MP), and if not, shall appropriately remove the U.S. person's identity in a manner sufficient to ensure the U.S. person's privacy.

The SMP restricts the FBI's dissemination of U.S. person information to federal, state, local, and tribal officials and agencies. The U.S. person information must reasonably appear to be necessary to the national defense or the security of the U.S., or the conduct of U.S. foreign affairs to be included. However, that information cannot identify a U.S. person unless such person's identity is necessary to understand foreign intelligence information or assess its importance.[49]

Like the SMP for Title I of FISA, the Section 702 MP permits the FBI to disseminate Section 702-acquired U.S. person information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information or assess its importance to federal, state, local, and tribal officials and agencies with responsibilities relating to national security that require access to intelligence information.[50] The FBI is also permitted to disseminate U.S. person information that reasonably appears to be evidence of a crime to law enforcement authorities.[51] In addition, the Section 702 MP provides guidelines that must be met before dissemination of U.S. person information to foreign governments is allowed.[52] The dissemination of Section 702 information to a foreign government requires legal review by the NSCLB attorney assigned to the case.[53]

In light of the above judicially-reviewed minimization procedures for the dissemination of FISA acquired information, the FBI's current implementation satisfies the data minimization and transparency FIPPs. It also satisfies the purpose specification FIPP because the 702 procedures are contained in the FISA statute itself, the FISC-approved minimization procedures, and other publicly released information.

VII. Oversight and Compliance:

From a programmatic standpoint, the FBI's handling of U.S. person information in FISA and other frameworks is subject to review by the FBI's Inspection Division, FBI's OIC, DOJ's OI, DOJ's Office of the Inspector General, and the PCLOB. The SMP and the Section 702 MP also require the Attorney General through the Assistant Attorney General for National Security to conduct periodic minimization reviews, including reviews at FBI Headquarters, field offices, and

[49] *Supra* note 35 at § IV; Section 702 MPs § V(A).
[50] Section 702 MPs § V(A).
[51] *Id*. at § V(B).
[52] *Id*. at § V(C).
[53] Foreign Dissemination of Classified Information Corporate Policy Directive and Policy Implementation Guide §§ 3.1, 3.2.

U.S. Attorney Offices that receive raw FISA-acquired information.[54] Minimization reviews must consist of reviews of documents, communications, audit trails or other information.[55]

Under Rule 13 of the FISC Rules of Procedure, the government must report non-compliance incidents to the FISC of any FISC-approved authorities that were "implemented in a manner that did not comply with the Courts authorization or approval or with applicable law." This is required for all FISA authorities, including Title I and Section 702.

As another oversight and compliance measure, the FBI's main systems that manage FISA applications and collect FISA information are National Security Systems maintained on a classified network, which is subject to strict training, audit, and access procedures. This further helps regulate the handling of U.S. person information. Additionally, the systems are subject to review by the FBI PCLO and PCLU, which occurred in the instant report.

a. Title I of FISA

At the FBI operational level, there is a multi-level review and approval process for FISA applications before they are presented to the FISC. As previously mentioned, all justifications for a proposed target must be extensively and thoroughly reviewed by numerous lawyers, supervisors, and senior executive management at the FBI, including by the FBI Director or Deputy Director. The draft application is then reviewed multiple times at DOJ, including by the Attorney General, Deputy Attorney General, or Assistant Attorney General of National Security, before even being submitted to the FISC for review and approval.

The FISC provides further oversight of this process because the federal FISC judges determine whether each Title I application meets the statutory requirements for approval. As mentioned earlier, it also approves the SMPs that protect U.S. person information collected under FISA.

In accordance with the FBI FISA and SMP Policy Guide, NSCLB is required to submit to the Attorney General, through DOJ OI, on a quarterly basis, a report of the accounting of the number of disseminations of FISA-acquired information concerning U.S. persons that are made to foreign governments.[56] DOJ also conducts regular reviews of FISA U.S. person disseminations. These reviews serve as another level of oversight by DOJ regarding the FBI's handling of U.S. person information.

b. Section 702 of FISA

As with Title I, several groups within the FBI are responsible for conducting internal oversight over Section 702 activities. For example, several attorneys in the FBI's NSCLB are responsible for providing legal advice regarding the application of the

[54] Section 702 MPs § VI (A).
[55] *Id*.
[56] *FBI FISA and SMP Policy Guide*, *supra* note 3, at §3.10.

Section 702 Targeting Procedures and MP.[57] The FBI Inspection Division is required to conduct oversight of the FBI's exercise of the Section 702 Targeting Procedures.[58] This oversight includes periodic reviews to evaluate the implementation of the procedures and the training given to relevant personnel. Such reviews must occur at least once every calendar year.[59]

The Section 702 MP require FBI to implement policies and procedures to ensure "good faith" compliance as necessitated by Section 702 MP requirements.[60] The FBI must report any incidents of non-compliance with the Section 702 Targeting Procedures by FBI personnel within five business days of learning of the incident to NSD and ODNI.[61] The FBI must also ensure that NSD and ODNI receive all appropriate information with regard to the required periodic reviews of FBI's targeting procedures.[62] In addition, the FBI must report annually to Congress the number of disseminations of U.S. person identities made, the number of U.S. person identities that were subsequently unmasked, and the number of Section 702 targets that were subsequently determined to be located in the United States.[63] Moreover, the FBI must evaluate whether foreign intelligence information is being acquired under Section 702 and whether the minimization procedures adequately minimize the acquisition, retention, and dissemination of U.S. person information consistent with U.S. foreign intelligence needs.[64]

Furthermore, both the 702 targeting procedures and 702 minimization procedures are subject to judicial review by the FISC and approval under 50 USC § 1881a(d), (e), and (i). In accordance with 50 U.S.C. § 1881a(e)(1), Section 702 MP must follow the requirements for Title I minimization procedures, which require judicial review. These procedures are required to ensure that acquisition is limited to targeting persons reasonably believed to be located outside the U.S., and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.

The FBI has extensive compliance and oversight processes with regard to FISA from the executive, judicial, and legislative branches. Many of the requirements within the FBI FISA and SMP Policy Guide are mandated by the SMP and Section 702 MP so they cannot be changed without a revision to the SMP by the Attorney General and the approval of the FISC.[65] As an added protection, the FBI and DOJ PCLOs also review the management system and the main repository of FISA collected information.

---

[57] August 2013 Semiannual Assessment of Compliance with Procedures and Guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act at A-12.
[58] Section 702 Targeting Procedures § III (13).
[59] *Id*.
[60] Section 702 MPs § VI (A).
[61] Section 702 Targeting Procedures § III (15).
[62] August 2013 Semiannual Assessment of Compliance with Procedures and Guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act at A-12.
[63] 50 U.S.C. §§ 1881a(I)(3).
[64] *Id*. at §§ 1881a(I)(3)(A), (B).
[65] *FBI FISA and SMP Policy Guide*, *supra* note 3, at §1.1.

VIII. Public Transparency:

Redacted versions of certain FISC opinions that relate to Title I and Section 702 matters are available on the IC on the Record website as well as on the FISC's website.[66] Maintained by ODNI, the website provides the public "[d]irect access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community."[67] Additionally, Section 602 of the U.S. Freedom Act of 2015[68] added provisions to FISA that have enhanced the government's transparency concerning FISA matters, including making a report publicly available that identifies, for the preceding 12-month period, the total number of FISC orders issued for electronic surveillance and physical searches.

Furthermore, certain redacted versions of the FBI's 702 Targeting Procedures and Section 702 MP are available on IC on the Record.[69] In addition, several documents that relate to FBI's Section 702 policies and practices are available on that website, including a redacted version of the 2015 Summary of Notable Section 702 Requirements, which references court opinions, agency targeting and minimization procedures, hearing transcripts, and other relevant documents regarding the operation of certain aspects of Section 702. Other pertinent documents include, but are not limited to, a transcript of certain FISC proceedings regarding the FBI's use of Section 702 information containing evidence of a crime, and a Semiannual Assessment of Compliance with Procedures and Guidance issued pursuant to Section 702. The assessment discusses oversight by ODNI and DOJ, including compliance trends identified by the joint oversight team.

Lastly, the FBI provided the PCLOB with information regarding its activities pursuant to Section 702 that informed the PCLOB's July 2, 2014 report and subsequent Section 702 implementation assessment reports. The FBI has accepted all of the PCLOB's recommendations.

Given the classified nature of the information, the release of FISC opinions and redacted minimization procedures, on the IC on the Record, adequately notify the public regarding acquisition, retention, and dissemination, and maintenance of U.S. person information.

IX. Conclusion:

As described above, there are multiple provisions in the statute, the annual certifications, and the FBI's targeting and minimization procedures that explicitly protect the privacy and civil liberties of U.S. persons and others located in the United States. These numerous provisions ensure that collection activities are limited to acquiring information needed to protect national security and privacy interests. Some of the protections include oversight by DOJ, ODNI, the FISC, and Congress. Moreover, the FBI PCLO and PCLU's review found the FBI diligently follows these provisions and protects all U.S. person information in the acquisition, retention, and dissemination of FISA information. This is in accordance with the Constitution, U.S. statutes, presidential directives, executive orders, federal regulations, and civil liberties and privacy

[66] *See* IC on the Record, available at http://icontherecord.tumblr.com (last visited August 9, 2017); the FISC website is available at http://www.fisc.uscourts.gov.
[67] *Id.*
[68] U.S. Freedom Act of 2015, Pub.L. 114-23.
[69] *See* IC on the Record, available at http://icontherecord.tumblr.com (last visited August 9, 2017).

policies. Finally, the instant review found no indication of noncompliance with the required authorities governing dissemination of U.S. person information in finished intelligence.