Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM November 16, 2017

Subject: **Summary of the Substantive Provisions of S. 2010, the FISA Amendments Reauthorization Act of 2017, and H.R. 3989, the USA Liberty Act of 2017**

From: Edward C. Liu, Legislative Attorney, eliu@crs.loc.gov, 7-9166

This memorandum was prepared to enable distribution to more than one congressional office.

This memorandum summarizes the substantive provisions of:

- S. 2010, the FISA Amendments Reauthorization Act of 2017, as reported by the Senate Select Committee on Intelligence on October 25, 2017, and
- H.R. 3989, the USA Liberty Act of 2017, as ordered to be reported by the House Judiciary Committee on November 8, 2017.[1]

Both bills primarily amend and reauthorize Title VII[2] of the Foreign Intelligence Surveillance Act of 1978 (FISA).[3] FISA generally provides a statutory framework by which government agencies may, when gathering foreign intelligence information, obtain authorization to conduct electronic surveillance[4] or physical searches,[5] utilize pen registers and trap and trace devices,[6] or compel the production of specified business records and other tangible things.[7] Authorization for such activities is typically obtained via a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created by FISA to act as a neutral judicial decision maker in the context of activities authorized by the statute.[8] FISA also created a specialized appellate court known as the Foreign Intelligence Surveillance Court of Review (FISCR) to review decisions of the FISC.[9]

[1] The version of H.R. 3989 ordered to be reported by the House Judiciary Committee includes an amendment in the nature of a substitute offered by Chairman Goodlatte, as modified by additional amendments from Reps. Conyers, Jackson Lee, and Cicilline. *See* House Judiciary Committee, *Markup of H.R. 3989 and H.R. 170* (Nov. 8, 2017), https://judiciary.house.gov/markup/markup-h-r-3989-h-r-170/.

[2] 50 U.S.C. §§ 1881-1881g.

[3] *Id.* §§ 1801-1885c.

[4] *Id.* §§ 1801-1813.

[5] *Id.* §§ 1821-1826.

[6] *Id.* §§ 1841-1846. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular telephone line. *See* 18 U.S.C. § 3127(3)-(4).

[7] 50 U.S.C. §§ 1861-1864.

[8] *Id.* § 1803.

[9] *Id.*

Title VII of FISA, added by the FISA Amendments Act of 2008, provides additional procedures for the acquisition of foreign intelligence information regarding persons who are believed to be outside of the United States. These provisions address both U.S. persons[10] and non-U.S. persons. In particular, the FISA Amendments Act added:

- Section 702, which includes a new procedure for targeting non-U.S. persons abroad without individualized court orders;[11]
- Sections 703, which provides procedures for domestic electronic surveillance that is targeted at U.S. persons who are abroad;[12] and
- Section 704, which provides procedures for other surveillance that is targeted at U.S. persons who are abroad.[13]

All three provisions of Title VII are currently scheduled to expire at the end of 2017.[14] Of these provisions, Section 702 perhaps has received the most attention, likely due to the variance of its procedures from the other authorities under FISA.[15] Traditional FISA orders authorizing electronic surveillance generally require the FISC to find, *inter alia*, that probable cause exists to believe that the particular target of the proposed surveillance is a foreign power or an agent of a foreign power.[16] Under Section 702, however, individual targets of surveillance are not necessarily reviewed by the FISC prior to the U.S. government's acquisition of the targets' communications.[17] Instead, the FISC's role under Section 702 is largely limited to reviewing certifications by the Attorney General (AG) and the Director of National Intelligence (DNI), along with targeting and minimization[18] procedures that the U.S. government proposes to use to target and acquire communications prospectively. Once the targeting and minimization procedures are approved by the FISC, elements of the Intelligence Community (IC) such as the National Security Agency (NSA) may use those procedures to acquire the communications of non-U.S. persons who are reasonably believed to be outside of the United States without the need for additional court orders specific to each target.[19]

The proposed amendments made to FISA Section 702 by S. 2010 and H.R. 3989 generally would not disturb this structure, but layer on additional requirements on the contents of the targeting and minimization procedures to provide greater privacy protections, particularly for U.S. persons.

Summaries of the provisions of S. 2010 and H.R. 3989 are organized by general topic below, along with brief descriptions of current law relevant to the proposed legislation.

---

[10] For purposes of FISA, a U.S. person is defined as a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. *Id.* § 1801(i).

[11] *Id.* § 1881a.

[12] *Id.* § 1881b.

[13] *Id.* § 1881c.

[14] P.L. 112-238, § 2; codified at 50 U.S.C. § 1881 note.

[15] *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 404 (2013) (describing the different character of Section 702 compared to other FISA provisions in the context of assessing a constitutional challenge to Section 702).

[16] 50 U.S.C. § 1805(a)(2). As defined by FISA, the term "foreign power" includes international terrorist organizations. *Id.* §1801(a)(4).

[17] For more detailed information regarding Section 702 procedures, see CRS Report R44457, *Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, by Edward C. Liu.

[18] Minimization procedures generally provide standards governing the circumstances under which particular communications may be acquired, used, and shared. 50 U.S.C. § 1801(h).

[19] *Id.* §§ 1881a(a), (c).

Table of Contents

Reauthorization of Title VII of FISA

Current Law

Title VII of FISA is currently scheduled to sunset on December 31, 2017.[20] Transition procedures would apply to FISA orders authorizing surveillance activities pursuant to Title VII that are in effect on December 31, 2017, permitting the continued effect of such orders until their normal expiration dates.[21]

S. 2010

Section 2 of S. 2010 would extend Title VII of FISA for eight years, until December 31, 2025.

H.R. 3989

Section 301 of H.R. 3989 would extend Title VII of FISA for approximately six years, until September 30, 2023.

Section 702 Targeting Procedures

Current Law

As noted above, Section 702 of FISA requires the AG and DNI to submit proposed targeting procedures for the acquisition of certain communications.[22] In order to be approved, Section 702 requires the targeting procedures to be reasonably designed to ensure that an acquisition is limited (1) to targeting persons reasonably believed to be located outside the United States and (2) to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[23]

Additional limitations on targeting are provided in FISA Section 702(b). Specifically, an acquisition under Section 702:

- may not intentionally target any person known at the time of acquisition to be located in the United States;
- 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;
- may not intentionally target a U.S. person reasonably believed to be located outside the United States;
- 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
- must be conducted in a manner consistent with the Fourth Amendment to the Constitution.[24]

[20] P.L. 112-238, § 2; codified at 50 U.S.C. § 1881 note.

[21] P.L. 110-261, § 404(b), as amended; codified at 50 U.S.C. § 1801 note.

[22] 50 U.S.C. § 1881a(d).

[23] *Id.*

[24] *Id.* § 1881a(b).

Targeting procedures applicable to the National Security Agency (NSA) were partially declassified by the DNI in 2017.[25] These procedures generally require NSA to consider the totality of the circumstances when determining whether a target is a non-U.S. person reasonably believed to be outside the United States.[26] These targeting procedures also direct NSA to determine whether foreign intelligence is likely to be acquired from the target, based on the totality of the circumstances.[27] The targeting procedures also require NSA analysts to document (1) citations to the information upon which they relied when making targeting determinations and (2) the foreign power or foreign territory about which foreign intelligence information is expected to be acquired.[28]

Presidential Policy Directive 28 (PPD-28), issued by President Obama on January 17, 2014, articulates principles for conducting signals intelligence activities.[29] Among other things, PPD-28 includes a prohibition against the collection of signals intelligence for the purpose of "suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[30]

PPD-28 also acknowledges that "foreign private commercial information or trade secrets is authorized" to be collected, but not for the purpose of affording U.S. companies or sectors a "competitive advantage."[31] The term "competitive advantage" does not include "identifying trade or sanctions violations or [foreign] government influence or direction."[32]

S. 2010

No provision.

H.R. 3989

Section 102(a) would amend FISA Section 702 to additionally require intelligence personnel implementing the targeting procedures to exercise due diligence when determining whether the target of an acquisition meets the criteria of being a non-U.S. person who is reasonably believed to be abroad. Specifically, the determination must be based on the totality of the circumstances, including after resolving any conflicting information regarding the proposed target. Agencies must also document the determination process and document the rationale for why targeting such person will result in the acquisition of foreign intelligence information.

Section 108 of H.R. 3989 appears intended to provide that the amendments made by Section 102(a) of the House bill would apply to applications, certifications, and procedures submitted to the FISC beginning

[25] DNI, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (Mar. 30, 2017) [hereinafter NSA Targeting Procedures], https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf.

[26] *Id.* at 1.

[27] *Id.* at 4.

[28] *Id.* at 8.

[29] WHITE HOUSE, Presidential Policy Directive – Signals Intelligence Activities (Jan. 17, 2014) [hereinafter PPD-28], https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[30] *Id.* at § 1(b).

[31] *Id.* at § 1(c).

[32] *Id.* at n.4.

120 days after the date of enactment of H.R. 3989.[33] However, the actual text of Section 108 of H.R. 3989 references the applicability of amendments made by Sections 101 and 102 of the original FISA statute. Given the structure and language of Section 108, the reference to the original FISA appears to be a clerical error.

Section 109 of H.R. 3989, as modified by an amendment offered by Representative Jackson-Lee, would provide a sense of Congress that the acquisition of communications by the NSA under FISA Section 702 should be conducted within the bounds of treaties and agreements to which the United States is a party, and there should be no targeting of non-U.S. persons for any unfounded discriminatory purpose or for the purpose of affording a commercial competitive advantage to U.S. companies and business sectors. Section 109 of the bill also provides a sense of Congress that the authority to collect intelligence conferred by FISA Section 702 is meant to shield the United States, and by extension, the allies of the United States, from security threats.

"About" Communications Collection

Current Law

Declassified opinions from the FISC indicate that the NSA, acting pursuant to FISA Section 702, acquired communications that were either to or from a particular targeted identifier (such as an email address or telephone number), but also acquired additional communications between untargeted persons if the communications were "about" the targeted identifier (i.e., a reference to the targeted identifier is present in the body of the communication).[34] Because "about" collection can capture communications to which the Section 702 target is not a party, concerns about the potential breadth of such collection have been raised by government entities including the FISC.[35] In 2017, the NSA announced that collection of "about" communications had ceased.[36]

S. 2010

Section 3 of S. 2010 addresses "abouts communications," a term defined as communications that contain a *reference* to a facility, place, premise, or property at which an acquisition under FISA Section 702 is directed or conducted, if such communication is not actually sent to or from such facility, place, premise, or property.[37]

Section 3 of S. 2010 would prohibit the use of FISA Section 702 to intentionally acquire "abouts communications" with one exception. Under this exception, the intentional acquisition of "abouts communications" could be implemented 30 days after written notice of the intent to conduct such acquisition is provided to Congress by the AG and DNI. If, during the 30-day period, Congress enacts legislation disapproving of the proposed collection of "abouts communications," such collection may not

[33] The text of Section 108 governs the applicability of amendments made by Sections 101 and 102 of the original FISA enacted in 1978. CRS assumes that Section 108 actually intends to reference the amendments made by Sections 101 and 102 of H.R. 3989.

[34] Redacted, 2011 U.S. Dist. LEXIS 157706, at *19 (FISA Ct. Oct. 3, 2011).

[35] *Id.* at *57 (finding that "about" collection may result in NSA's acquisition of "tens of thousands of additional communications of non-targets each year, many of whom have no relationship" to the Section 702 target). *See also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 88 (July 2, 2014), https://pclob.gov/library/702-Report.pdf.

[36] NSA, *NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702* (Apr. 28, 2017),https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml.

[37] S. 2010 uses the plural "abouts" rather than "about" when referring to these communications.

be implemented. Expedited procedures for consideration of such disapproving legislation would be provided for both the House and the Senate.

The written notice to Congress would be required to include (1) copies of certifications and supporting material that have been submitted to the FISC in support of the proposed acquisition of "abouts communications;" (2) decisions, orders, or opinions of the FISC approving such certifications; (3) a summary of the protections in place to detect any significant non-compliance under the proposed collection; and (4) a certification that the proposed collection will not occur until the 30-day period has lapsed, except where the AG and DNI determine that exigent circumstances exist and that intelligence information important to the national security either may be lost or not timely acquired. Notice of the invocation of exigent circumstances must be provided to the House and Senate Intelligence and Judiciary Committees within seven days.

The head of any agency involved in the proposed collection of "abouts communications" would be required to report any material breaches to the House and Senate Intelligence and Judiciary Committees.

H.R. 3989

Section 102(a) of H.R. 3989 would provide that the targeting procedures adopted under FISA Section 702 must limit communications collection to those communications sent to or from the targeted person, effectively prohibiting collection of "about" communications. This limitation would apply until September 30, 2023. The AG is directed to submit an annual report to the Intelligence and Judiciary Committees regarding the effect of this limitation, including any difficulties relating to the limitation and the technical feasibility of ensuring that incidental acquisitions of U.S. person information complies with applicable minimization procedures.

Use of Information Acquired Under Section 702

Current Law

Information acquired under FISA Section 702 regarding any U.S. person may be used and disclosed in accordance with the minimization procedures approved by the FISC.[38] FISA defines minimization procedures to allow for evidence of crimes that has been acquired under Section 702 to be shared with law enforcement agencies.[39] Privileged communications (such as attorney-client communications) do not lose their privileged character simply because they may have been acquired pursuant to FISA.[40] Information acquired under Section 702 may only be used in a criminal proceeding with the advance authorization of the AG.[41] The government shall notify any person of information acquired under Section 702 when the government intends to enter the information into evidence or otherwise use it against such

[38] 50 U.S.C. §§ 1881e(a), 1806(a). Minimization procedures declassified by the DNI permit the use of Section 702 acquired information for law enforcement purposes. DNI, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 10, 12-13 (Mar. 30, 2017) [hereinafter NSA Minimization Procedures], https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf at 10, 12-13.

[39] 50 U.S.C. § 1801(h)(3).

[40] *Id.* §§ 1881e(a), 1806(a).

[41] *Id.* §§ 1881e(a), 1806(b).

person in a trial, hearing, or other proceeding.[42] Such information may be suppressed if unlawfully acquired.[43]

S. 2010

Section 6 of S. 2010 would amend FISA Section 706(a) to apply additional restrictions on the use of communications collected under Section 702 of FISA when such communications contain a reference to a U.S. person. Specifically, such communications could not be used in evidence against the referenced U.S. person in any criminal proceeding unless the AG determines that the proceeding (1) involves death; kidnapping; serious bodily injury; certain offenses against minors; certain offenses against critical infrastructure; cybersecurity; trans-national crime; human trafficking; or (2) affects, involves, or is related to national security. The AG's determinations would not be subject to judicial review.

H.R. 3989

Section 101(c) of H.R. 3989 would place additional restrictions on the use of information obtained through the querying mechanism added by H.R. 3989 (described in the following section). Specifically, such information could be used in evidence only with the AG's approval, and the information also must be directly related and necessary to address a specific threat of terrorism, espionage, proliferation of weapons of mass destruction, cybersecurity, incapacitation or destruction of critical infrastructure, or a threat to the armed forces or personnel of the United States or a U.S. ally.

Section 304 of H.R. 3989 would express the sense of Congress that, in carrying out FISA Section 702, the United States should ensure that barriers to sharing critical foreign intelligence among the intelligence community (IC) that existed before September 11, 2001, are not reimposed. The sense of Congress would further provide that information vital to national security should be shared among the IC in a manner that is consistent with applicable provisions of law and the Constitution.

Section 305 of H.R. 3989 would express a sense of Congress that, consistent with the protection of sources and methods, when lawful and appropriate, the President should share information learned by acquiring communications under FISA Section 702 with allies of the United States to prevent and defend against terrorism.

Queries Using U.S. Person Identifiers

Current Law

Once information has been acquired under FISA Section 702, the minimization procedures adopted by the AG and approved by the FISC govern the retention and dissemination of such information by the government.[44] For example, the minimization procedures may set forth the circumstances under which the government may "query" (search) information previously acquired under Section 702 for the presence of specific U.S. person identifiers (such as a telephone number or email address). In general, FISA requires these procedures to restrict the acquisition, retention, and dissemination of non-public information concerning U.S. persons (including identities).[45] However, if the collected information is evidence of a

[42] *Id.* §§ 1881e(a), 1806(c).

[43] *Id.* §§ 1881e(a), 1806(e), (g).

[44] *Id.* § 1881a(e).

[45] *Id.* § 1801(h).

crime, FISA allows for the retention and dissemination of such information for law enforcement purposes.[46]

Minimization procedures adopted by various agencies may differ with regard to an agency's ability to query information. For example, minimization procedures declassified in 2017 appear to allow the NSA and the Central Intelligence Agency (CIA) to query information collected under FISA Section 702 using U.S. person identifiers only when reasonably likely to return foreign intelligence information.[47] In contrast, Federal Bureau of Investigation (FBI) minimization procedures appear to allow that agency to query information acquired under Section 702 using U.S. person identifiers to additionally determine if such information is evidence of a crime.[48] The minimization procedures require the FBI to maintain records of all searches, including search terms used.[49]

S. 2010

Section 7 of S. 2010 would amend FISA Section 702 to require separate querying procedures, in addition to the targeting and minimization procedures required under current law. The querying procedures, to be adopted by the AG in consultation with the DNI, would apply to instances in which already acquired data is subsequently searched using a specific term or terms for the purpose of discovering or retrieving content or metadata that has not previously been viewed by IC personnel. The querying procedures required by S. 2010 would require records of all queries using a known U.S. person identifier to be kept by the relevant element of the IC. The querying procedures would be subject to judicial review by the FISC to ensure compliance with the statutory requirements. The AG and DNI would assess agencies' compliance with the querying procedures in a semi-annual assessment provided to the FISC and the House and Senate Intelligence and Judiciary Committees. The Inspectors General of the Department of Justice and relevant IC elements would also have jurisdiction to conduct oversight of compliance with the querying procedures by their respective agencies.

Section 8 of S. 2010 would further amend FISA Section 702 to require the FBI Director to notify the FISC within one business day after a query of information acquired under Section 702 returns responsive information concerning a known U.S. person. As part of this notice, the FBI Director would be directed to submit the query, the responsive information, and the FBI's justification for the query. Within two business days after receiving this submission, the FISC would review the query for consistency with the Fourth Amendment and notify the FBI of the court's findings. If the FISC determined that a query was not consistent with the Fourth Amendment, the information could not be used in any court proceeding. The FISC would also be directed to submit an annual report on its reviews of query submissions in the previous year to the House and Senate Intelligence Committees, including the total number of queries and the number of queries determined to be inconsistent with the Fourth Amendment.

---

[46] *Id.* § 1801(h)(3).

[47] NSA Minimization Procedures, *supra* note 38, at 4-5; DNI, Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 3 (Sept. 26, 2016),https://www.dni.gov/files/documents/icotr/51117/2016_CIA_Section_702_Minimization_Procedures_Se_26_2016.pdf.

[48] DNI, Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, at 11 (Sept. 26, 2016), https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf at 11.

[49] *Id.*

Section 8 also includes a rule of construction stating that it shall not be construed to require any action to determine the nationality of an individual that would not have been required prior to the enactment of S. 2010. The query submission requirement would take effect 90 days after the date of enactment of S. 2010.

H.R. 3989

Section 101 of H.R. 3989 would amend FISA Section 702 to impose additional requirements before accessing information acquired under Section 702 that is returned in response to a query. If a query seeks the contents of a communication, the AG would be required to apply to the FISC for a court order finding that:

- probable cause exists to believe that the contents of the communication include evidence of one of the crimes that is a predicate crime to support a wiretap under the Electronic Communications Privacy Act;[50]
- the communication is relevant to an authorized investigation or assessment that is not conducted solely on the basis of First Amendment protected activities; and
- any use of such communications by the government will be consistent with the requirements of H.R. 3989.

A denial of the application for such an order by the FISC could be reviewed by the FISCR, and potentially thereafter by the Supreme Court.

A lower standard would apply to queries that seek non-content information such as dialing, routing, addressing, or signaling information. For this type of information or metadata, a supervisor would be required to approve of the query, but a court order authorizing the query would not generally be required. As with queries for content information, the information could not be sought solely on the basis of activities protected by the First Amendment. If a court order based on probable cause would have been required to obtain such metadata as part of a federal criminal investigation, the government would also be required to apply to the FISC for a court order before submitting a query of FISA Section 702 information. Under Section 101 of H.R. 3989, neither requirement to obtain a FISC order nor supervisory approval would apply to a query if:

- the query is reasonably designed to return foreign intelligence information (notwithstanding the fact that such information may describe activities that are also federal crimes);
- the AG determines that the person identified by the queried term is already the subject of a wiretap or electronic surveillance order under federal law;
- the AG reasonably determines that an emergency situation requires access to the information before either a court order or supervisory approval can be obtained;
- the AG reasonably determines that the person identified by the queried term is communicating with another person who is reasonably believed to be engaged in, or preparing to engage in, international terrorism or material support for terrorism;[51] or
- the person identified by the queried term has consented to the query.

[50] 18 U.S.C. § 2516.

[51] The AG must also reasonably believe that the factual basis for the issuance of the order exists and must contemporaneously inform the FISC of the exercise of this authority to access the contents of communications. If the FISC subsequently determines that these criteria were not met, the contents of communications may not be used by the government.

Before making this determination, the AG would be required to conduct a review of the relevant metadata that causes him to (1) reasonably suspect that the third party is engaged in international terrorism or material support for terrorism, and (2) conclude that a failure or delay to access or disseminate the contents of the communications would harm the national security. The AG would be required to notify the FISC as soon as practicable (but at most within seven days) of the invocation of this exception and the factual basis for it. If the FISC finds that the determination was not appropriate or the factual basis was erroneous, the government could not use such communications in any hearing, trial, or proceeding.

If the AG determines that it is necessary to conduct electronic surveillance on a known U.S. person whose communications have been acquired under FISA Section 702, the AG could only conduct such surveillance using other provisions of law. Section 101 of H.R. 3989 also instructs the FBI Director to ensure that all available investigative or intelligence databases are queried simultaneously. The AG would be instructed to delegate authority to authorize queries under this provision to the fewest number of officials practicable.

Under the House bill, the AG and other IC elements would retain records of queries that use a term identifying a U.S. person for at least five years. The records would be maintained in an auditable manner and made available for congressional oversight. The requirements for queries under this provision would not apply to queries made for submitting information to Congress, performing maintenance, or testing information systems. As discussed above, the information received in response to queries under this provision would be subject to additional limitations on use.[52]

Section 106 of H.R. 3989 would also require the FBI Director to submit semiannual reports to the House and Senate Intelligence and Judiciary Committees regarding the total number of query applications made, the number of query applications approved, the number of supervisory approvals made, the number of emergency exceptions made by the AG, the number of emergency exceptions with which the FISC disagreed, the number of terrorism-related exceptions made, and the number of terrorism-related exceptions with which the FISC disagreed.

Section 108 of H.R. 3989 appears intended to provide that the amendments made by Section 101 of the House bill would apply to applications, certifications, and procedures submitted to the FISC beginning 120 days after the date of enactment of H.R. 3989. However, the actual text of Section 108 of H.R. 3989 references the applicability of amendments made by Sections 101 and 102 of the original FISA statute. Given the structure and language in Section 108, the reference to the original FISA appears to be a clerical error.

Emergency Collection Authority

Current Law

Title I and Title III of FISA authorize court orders, supported by probable cause, to conduct electronic surveillance and physical searches, respectively.[53] These titles also permit short-term electronic surveillance and physical searches targeting a U.S. person without a court order in emergency situations.[54]

If an order under Title I or Title III has been issued with respect to a U.S. person, FISA Section 705 permits the AG to authorize the additional targeting of that U.S. person for the purpose of acquiring foreign intelligence information while that person is reasonably believed to be outside of the United

[52] *See supra* "Use of Information Acquired Under Section 702."

[53] 50 U.S.C. §§ 1801-1813, 1821-1829.

[54] *Id.* §§ 1805(e), 1824(e).

States.[55] However, Section 705 of FISA does not include a provision allowing the AG to authorize targeting of U.S. persons reasonably believed to be outside of the United States if they are currently being targeted for *emergency* electronic surveillance or physical searches.[56] FISA Sections 703 and 704, which provide procedures for court orders targeting U.S. persons abroad, permit emergency acquisitions without a court order, but such acquisitions must be followed by an application for a court order within seven days.[57]

S. 2010

Section 9 of S. 2010 would amend FISA Section 705 to address situations where a U.S. person has been subject to emergency electronic surveillance or physical searches under Title I or Title III of FISA. During the applicable emergency period, the AG would be permitted to authorize the targeting of that person for acquiring foreign intelligence while that person is reasonably believed to be outside the United States. If a court order is not issued following the emergency surveillance under Title I or Title III of FISA, the information acquired under FISA Section 705 would not be available as evidence or otherwise disclosed in any trial, hearing, or proceeding, unless the AG determines that the information indicates a threat of death or serious bodily harm to any person.

H.R. 3989

No provision.

FISC and FISCR Procedures

Current Law

The FISC is an Article III court[58] composed of 11 district court judges selected by the Chief Justice of the Supreme Court from at least seven of the regional judicial circuits.[59] The FISCR, is an Article III court which sits as an appellate court above the FISC, comprised of three judges designated by the Chief Justice.[60] While judges of traditional Article III courts are selected via presidential appointment following Senate confirmation,[61] FISC and FISCR judges are "designated" to the court by the Chief Justice.[62] The FISC's jurisdiction is limited to hearing applications and granting orders for "the collection of foreign intelligence by the federal government."[63] This includes applications for (1) electronic surveillance; (2) physical searches; (3) pen register/trap and trace surveillance; and (4) orders to compel the production of tangible things.[64] Under the FISA Amendments Act of 2008 (FAA), the FISC is authorized to review

[55] *Id.* § 1881d(a).

[56] *Id.* §§ 1881b(d), 1881c(d).

[57] *Id.*

[58] *See* United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) (Kennedy, J.).

[59] 50 U.S.C. § 1803(a)(1).

[60] *Id.* § 1803(b).

[61] U.S. CONST., art. II, § 2, cl. 2.

[62] 50 U.S.C. §§ 1803(a)(1), (b).

[63] *In re* Release of Court Records, 526 F. Supp. 2d 484, 487 (FISA Ct. 2007).

[64] *See* 50 U.S.C. § 1803(a) (electronic surveillance); *id.* § 1822(c) (physical searches); *id.* § 1842(a)(1) (pen registers); *id.* § 1861(b)(1) (tangible things).

applications for targeting U.S. persons reasonably believed to be abroad.[65] The government may appeal a denial of a FISA application to the FISCR.[66]

S. 2010

No provision.

H.R. 3989

Section 306 of H.R. 3989 makes a number of amendments relating to the FISC and the FISCR. Specifically, the provision would:

- remove the temporal requirement that the FISCR "immediately" provide a written statement for its decision affirming the denial of a FISA application;
- specify that the FISCR, in addition to the FISC, has the inherent authority to determine or enforce compliance with its orders or rules; and
- specify that denials of applications to extend electronic surveillance, applications for pen registers and trap and trace devices orders, and applications for orders to produce tangible things may be reviewed by the FISCR.

Section 306 of H.R. 3989 also makes a number of technical amendments to the text of FISA to correct grammatical errors and cross-references.

Appointment of *Amicus Curiae* by the FISC and FISCR

Current Law

The term *amicus curiae*, or "friend of the court," refers to a person who is not a party to a particular lawsuit or proceeding, but who may be heard by a court on a particular issue (via petition to the court or request from the court).[67] *Amici* have been used previously by both the FISC and the FISCR.[68] The role of *amici* in FISA proceedings was codified in 2015 by the USA FREEDOM Act.[69]

Section 103 of FISA, as amended by the USA FREEDOM Act, authorizes the presiding judges of the FISC and FISCR to designate at least five individuals to be eligible to serve as *amicus curiae*.[70] Either court shall appoint *amici* to assist in the consideration of any application that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate.[71] Either court may also appoint an *amicus* in any instance the court deems appropriate or may grant leave for an individual or organization to file an amicus curiae brief.[72]

---

[65] *Id*. §§ 1881b(a), 1881c(a).

[66] *Id*. §§ 1803(b), 1822(d), 1861(f)(3).

[67] BLACK'S LAW DICTIONARY 102 (10th ed. 2014).

[68] *See*, *e.g*., In re Orders of this Court Interpreting Section 215 of the Patriot Act, 2013 U.S. Dist. LEXIS 143060, at n.5 (FISA Ct. Sept. 13, 2013); *and* In re Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

[69] P.L. 114-23, § 401, codified at 50 U.S.C. § 1803(i).

[70] 50 U.S.C. § 1803(i)(1).

[71] *Id.* § 1803(i)(2)(A).

[72] *Id.* § 1803(i)(2)(B).

S. 2010

Section 4 of S. 2010 would amend FISA Section 103 to provide a rebuttable presumption that the first certification proposing to authorize acquisition of "abouts communications" (as described above) pursuant to Section 3 of the Senate bill would present a novel or significant interpretation of the law such that the appointment of an *amicus curiae* would be warranted.[73]

Section 5 of S. 2010 would also amend FISA Section 103 to provide that *amici* appointed by either the FISC or FISCR may be compensated by either court at a rate the court considers appropriate.

H.R. 3989

Section 104 of H.R. 3989 would amend FISA Section 103 to provide that the FISC and FISCR shall appoint an *amicus curiae* with respect to the review of any certification under FISA Section 702, unless the court issues a finding that an *amicus* is unnecessary.

Unauthorized Unmasking and Disclosure of Classified Information

Current Law

The minimization procedures that were adopted under FISA Section 702, and approved by the FISC, generally protect against the retention, use, and dissemination of non-public information concerning U.S. persons.[74] The protection of U.S. persons' identities is expressly included in FISA's statutory definition of requisite minimization procedures.[75] However, disclosure of identifying information is permissible to the extent that "such [U.S.] person's identity is necessary to understand foreign intelligence information or assess its importance."[76] The process by which a U.S. person's identity is disseminated, so that the recipient may better understand the foreign intelligence implications of related information, is typically referred to as "unmasking."

Information collected under FISA is also frequently protected from disclosure as classified information. Several provisions of federal criminal law prohibit the disclosure of sensitive national defense information or classified information.[77] For example, 18 U.S.C. § 1924(a) makes it a misdemeanor for officers, employees, consultants, and contractors of the United States to knowingly remove documents or materials containing classified information without authority and with the intent to keep such documents or materials at an unauthorized location. Violations of 18 U.S.C. § 1924(a) are punishable by fine and up to one year in prison.[78]

[73] *See*, *supra* at ""About" Communications Collection."

[74] 50 U.S.C. § 1801(h).

[75] *Id.* § 1801(h)(2).

[76] *Id.*

[77] *See* CRS Report R41404, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, by Stephen P. Mulligan and Jennifer K. Elsea.

[78] 18 U.S.C. § 1924(a).

S. 2010

Section 12 of S. 2010 would amend 18 U.S.C. § 1924(a) to increase the criminal penalty for violations so that the maximum term of imprisonment would be not more than 10 years.

H.R. 3989

Section 102 of H.R. 3989 would amend FISA Section 702 to impose additional requirements on the minimization procedures specific to unmasking. Specifically, the minimization procedures would be required to include specific procedures for the submission of requests to unmask information in disseminated intelligence reports. These unmasking procedures would require (1) documentation of the reasons for the unmasking and (2) the retention of records relating to each request (such as the identities of the requester and any persons approving such request). "Unmask" would be defined to mean the dissemination of the identity of a U.S. person whose identity had not been previously released. Similar requirements would also be placed on information acquired through traditional electronic surveillance, physical searches, pen registers and trap and trace devices, and orders for the production of tangible things.

Section 102 H.R. 3989 would also require the DNI to submit a report to the House and Senate Intelligence and Judiciary Committees on progress made to ensure (1) incidentally acquired communications of U.S. persons are properly masked and (2) implementation of unmasking procedures as added by this section.

Section 108 of H.R. 3989 appears intended to provide that the amendments made by Section 102 of the House bill would apply to applications, certifications, and procedures submitted to the FISC beginning 120 days after the date of enactment of H.R. 3989. However, the actual text of Section 108 of H.R. 3989 references the applicability of amendments made by Sections 101 and 102 of the original FISA statute. Given the structure and language in Section 108, the reference to the original FISA appears to be a clerical error.

Section 302 of H.R. 3989 would amend 18 U.S.C. § 1924(a) to increase the criminal penalty for violations so that the maximum term of imprisonment would be not more than five years.

An amendment to H.R. 3989 adopted at markup would provide a rule of construction, stating that nothing in the bill may be construed to limit the application or effect of criminal penalties under the Privacy Act of 1974 or 18 U.S.C. § 1924, with respect to offenses relating to the unauthorized access or use of information or the unauthorized disclosure of U.S. person's information acquired under Section 702.[79]

Deletion

Current Law

FISA Section 106 requires that if the contents of any communication are unintentionally acquired by surveillance under circumstances in which a party has a reasonable expectation of privacy and a warrant would be required to intercept the communication for law enforcement purposes, such contents shall be destroyed if both the sender and all intended recipients are located within the United States.[80] Such

[79] Amendment to the Amendment in the Nature of a Substitute to H.R. 3989 Offered by Rep. Cicilline,https://judiciary.house.gov/wp-content/uploads/2017/11/Cicilline.pdf.

[80] 50 U.S.C. § 1806(i).

contents shall be destroyed as soon as they are recognized.[81] Destruction of the contents of the communication is not required if the AG determines that the contents indicate a threat of death or serious bodily harm to any person.[82] This requirement applies to information acquired through electronic surveillance and also applies to information unintentionally collected under FISA Section 702.[83]

S. 2010

No provision.

H.R. 3989

Section 201 of H.R. 3989 would amend FISA Section 702 to require that the NSA Director include an affidavit stating that communications acquired under Section 702 were deleted upon a determination that those communications did not contain foreign intelligence information. This affidavit would be submitted as part of the semiannual assessment required under current law, and could not be delegated by the NSA Director to another person.

Transparency and Congressional Oversight

Current Law

FISA currently requires a number of periodic reports and assessments to be provided to congressional and public audiences, including:

- annual public reports by the DNI providing the total number of individualized electronic surveillance and physical search orders; the total number of Section 702 orders and a good faith estimate of queries and searches of information collected under Section 702; the total number of pen registers and trap and trace device orders; the total number of orders to produce tangible things; and the total number of national security letters issued;[84]
- annual reporting by the AG to the Administrative Office of the U.S. Courts and Congress on the total number of applications made for orders and extensions of FISC orders approving electronic surveillance;[85]
- Semiannual reporting by the AG to the House and Senate Intelligence and Judiciary Committees on the number of applications for pen registers and trap and trace device orders;[86] and
- semiannual reporting by the AG to the House and Senate Intelligence and Judiciary Committees on the implementation of Section 702, including incidents of non-compliance.[87]

[81] *Id.*

[82] *Id.*

[83] *Id.* § 1881e(a).

[84] *Id.* § 1873(b).

[85] *Id.* § 1807.

[86] *Id.* § 1846(b).

[87] *Id.* § 1881f.

S. 2010

Section 6(b) of S. 2010 would require the annual public report from the DNI to include a good faith estimate of (1) the number of U.S. person and non-U.S. person targets of individualized electronic surveillance and physical search orders; (2) the number of FISA Section 702 targets; (3) the number of times that the FBI received FISA Section 702 information in response to a query that was reasonably designed to find evidence of a crime; (4) the number of instances in when the FBI opened a criminal investigation of a U.S. person based in whole or in part on Section 702 information; and (5) the number of criminal proceedings in which the FBI provided notice that the government intended to use FISA-derived information.

H.R. 3989

Section 103 of H.R. 3989 would amend FISA Section 702 to direct the DNI, in consultation with the AG, to conduct a declassification review of minimization procedures adopted under Section 702, and to make such minimization procedures public to the greatest extent practicable (including in redacted form) no later than 180 days after conducting the review.

Section 105 of H.R. 3989 would amend FISA Section 707 to require the DNI's semiannual Section 702 report to include (1) the number of U.S. persons' communications acquired under FISA Section 702, or a detailed explanation if neither a number or good faith estimate can be made; (2) the number of U.S. persons whose identities were unmasked; (3) the number of requests made by an element of the federal government to unmask such information; (4) the number of requests that resulted in the dissemination of U.S. persons' identities; (5) the number of Section 702 communications provided to the FBI for cases unrelated to foreign intelligence; (6) the number of instances when evidence of a crime unrelated to foreign intelligence was shared by the FBI's national security branch to the FBI's criminal investigative division; and (7) the number of individuals to whom the AG has delegated authority related to U.S. person queries.

As noted above, Section 106 of H.R. 3989 would also amend FISA Section 707 to require the FBI Director to semiannually report to the House and Senate Intelligence and Judiciary Committees on statistics of FBI queries of information acquired under FISA Section 702.[88]

Section 107 of H.R. 3989 would amend Section 107 of FISA to require the AG to transmit to the Administrative Office of the U.S. Courts and to Congress a report including (1) the total number of applications for orders and extensions of orders for electronic surveillance; (2) the total number of such orders granted, modified, or denied; and (3) the total number of persons subject to emergency electronic surveillance, rounded to the nearest 500, including the number of U.S. persons in that group, reported to the nearest band of 500, starting with 0-499. This report would be submitted in unclassified form and made publicly available.

Section 107 of H.R. 3989 would further amend Section 406 of FISA to require inclusion of a good faith estimate of the total number of subjects who were targeted by pen registers and trap and trace device orders or emergency authorizations rounded to the nearest 500, including the number of such subjects who are U.S. persons; and the number of persons whose information was reviewed or accessed. These numbers would be reported to the nearest band of 500, starting with 0–499. The report would be submitted in unclassified form and made publicly available.

Section 303 of H.R. 3989 would direct the Comptroller General of the United States to conduct a study of the unauthorized disclosure of classified information and the classification system of the United States

[88] *See* "Queries Using U.S. Person Identifiers."

generally. The study would be required to address (1) insider threat risks; (2) the effect of modern technology; (3) the effect of overclassification; (4) ways to improve the classification system; (5) ways to improve the authorized sharing of classified information; (6) the value of polygraph tests; and (7) the uniformity of standards and proper training across the IC. The report would be submitted within 180 days after the date of enactment of H.R. 3989 to the House and Senate Intelligence and Judiciary Committees.

Privacy and Civil Liberties Oversight Board

Current Law

The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency established under federal law.[89] Its duties include analyzing and reviewing executive branch actions to protect against terrorism, so as to ensure that appropriate consideration is given to privacy and civil liberties protections.[90] The PCLOB is comprised of a full-time chairman and four additional members, each serving a six-year term.[91] The PCLOB meets upon the call of the chairman or a majority of its members.[92] Three members constitute a quorum.[93] The chairman may appoint and fix the compensation of PCLOB's staff including a full-time executive director.[94]

S. 2010

Section 10 of S. 2010 would exempt the PCLOB from statutory requirements for federal agencies regarding public reporting and public meeting accessibility.

Section 11 of S. 2010 would provide that during periods when the position of chairman is vacant or a quorum is absent, the remaining members of the PCLOB, or a single member if only one member has been appointed, may exercise, through a unanimous vote, the authority of the chairman regarding the appointment of staff.

H.R. 3989

Section 202 of H.R. 3989 would allow the members of the PCLOB, through a unanimous vote, to exercise the authority of the chairman regarding the appointment of staff, if the position of chairman is vacant.

Section 202 would also exempt the PCLOB from statutory requirements regarding public meetings, and allow the PCLOB to meet or deliberate in a manner closed to the public.

Section 202 would also direct the PCLOB to submit a report to the House and Senate Intelligence and Judiciary Committees assessing (1) how communications acquired under FISA Section 702 are used by the United States to prevent or defend against terrorism; (2) whether technological challenges and changes in technology affect the prevention of and defense against terrorism, and how effectively the IC has responded to those challenges; (3) how privacy and civil liberties are affected by the use of communications acquired under Section 702 or by changes in technology; and (4) whether race, religion,

[89] 42 U.S.C. § 2000ee(a).

[90] *Id.* § 2000ee(c).

[91] *Id.* §§ 2000ee(h)(1), (h)(4).

[92] *Id.* § 2000ee(h)(5).

[93] *Id.*

[94] *Id.* § 2000ee(j).

political affiliation, or activities protected under the First Amendment are determinative in targeting or querying decisions made under FISA Section 702. The report would be submitted not later than one year after the PCLOB has a quorum of members.

Privacy and Civil Liberties Officers

Current Law

Section 1062 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the AG, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the DNI, the Director of the CIA, and the head of any other department, agency, or element of the executive branch designated by the PCLOB to designate at least one senior officer to serve as a Privacy and Civil Liberties Officer for the relevant agency.[95]

S. 2010

No provision.

H.R. 3989

Section 203 of H.R. 3989 would amend Section 1062 of the IRTPA to add the NSA and the FBI to the list of agencies required to designate a Privacy and Civil Liberties Officer. Section 203 would further require the Privacy and Civil Liberties Officers of IC elements to review incidentally collected communications of U.S. persons to assess compliance with the minimization procedures adopted under FISA Section 702 and effects on the privacy of U.S. persons.

Intelligence Community Whistleblowers

Current Law

Federal law prohibits retaliation against employees of certain IC elements for the lawful disclosure of information to the DNI, the Inspector General of the IC, the head of the IC element, the inspector general of the particular IC element at which the whistleblower is employed, a congressional intelligence committee, or a member of a congressional intelligence committee. This protection against retaliation applies when the employee reasonably believes the disclosed information either evidences a violation of law; mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.[96] In addition to personnel actions, prohibited retaliation includes revocation of security clearances.[97]

S. 2010

No provision.

[95] *Id.* § 2000ee-1(a).

[96] 50 U.S.C. § 3234(b).

[97] *Id.* § 3341(j).

H.R. 3989

Section 204 would extend the anti-retaliation protections provided under federal law to reach the employees of contractors of certain IC elements, including the FBI. Specifically, such protections would apply to employees of (1) contractors, (2) subcontractors, (3) grantees, (4) subgrantees, and (5) personal services contractors.

Severability

Current Law

When one provision of a law is held unconstitutional, the Supreme Court has held that "[u]nless it is evident that the Legislature would not have enacted those provisions which are within its power, independently of that which is not, the invalid part may be dropped if what is left is fully operative as a law."[98] Congress frequently includes a *pro forma* severability clause in a statute,[99] and this may reinforce a "presumption" of severability.[100] Absence of a severability clause does not raise a presumption *against* severability.[101]

FISA does not contain a severability clause. However, Section 401 of the FISA Amendments Act of 2008, which added Title VII to FISA provides that if any provision of that act, any amendment made by that act, or the application thereof to any person or circumstances is held invalid, the validity of the remaining provisions, amendments, and the application of such provisions to other persons and circumstances shall not be affected.[102]

S. 2010

No provision.

H.R. 3989

Section 307 of H.R. 3989 includes a severability clause, providing that if any provision of the act, or any amendment made by the act, or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the act, and of the application of such provisions to other persons and circumstances shall not be affected.

---

[98] Alaska Airlines, Inc. v. Brock, 480 U.S. 678, 684 (1987) (quoting Buckley v. Valeo, 424 U.S. 1, 108 (1976)).

[99] *See, e.g.*, 2 U.S.C. § 1438 ("If any provision of this Act or the application of such provision to any person or circumstance is held to be invalid, the remainder of this Act and the application of the provisions of the remainder to any person or circumstance shall not be affected thereby.").

[100] *Alaska Airlines*, 480 U.S. at 486.

[101] New York v. United States, 505 U.S. 144, 186 (1992).

[102] P.L. 110-261, § 401.