Congressional Research Service
Informing the legislative debate since 1914

FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act

July 8, 2025

Congressional Research Service
https://crsreports.congress.gov
R48592

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48592

July 8, 2025

Andreas Kuersten
Legislative Attorney

FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act

Section 702 of the Foreign Intelligence Surveillance Act (FISA) provides a legal framework under which the U.S. government can conduct electronic surveillance of non-U.S. persons abroad. This surveillance is authorized programmatically rather than individually. That is, the Foreign Intelligence Surveillance Court authorizes the government to carry out this surveillance within approved parameters for up to one year at a time. The government does not have to seek court authorization for every individual it targets. These authorizations also address the procedures pursuant to which the government can search (i.e., query) information collected under Section 702.

Congress enacted Section 702 in 2008 with an automatic repeal date (i.e., a sunset date). Since then, Congress has included a sunset date each time it has reauthorized the section. The last time Congress reauthorized Section 702 was on April 20, 2024, via the Reforming Intelligence and Securing America Act (RISAA), which provides that the section will sunset on April 20, 2026. Section 702 has generated significant debate since its inception. This debate tends to intensify as the sunset dates approach, and reauthorizations have historically been the means by which Congress has amended the section.

In the run-up to Section 702's previous sunset date and the RISAA's enactment, government and private actors shared with Congress a number of concerns about the statute, including the government querying Section 702 data using U.S.-person search terms without warrants, a lack of data on "incidental collection" (i.e., the collection of U.S.-person communications in the course of targeting non-U.S. persons for surveillance under Section 702), and a lack of additional approval procedures for queries potentially targeting politically disfavored individuals or groups.

The RISAA extensively amended Section 702, as well as other portions of FISA relevant to Section 702. For example, Congress expanded the definition of foreign intelligence information to include information on the international production, distribution, and financing of illicit drugs, thereby expanding the types of information that the government has authority to acquire under Section 702. Congress also mandated annual query training for Federal Bureau of Investigation (FBI) personnel and implemented enhanced query oversight for "sensitive queries" involving terms associated with political actors and media and religious organizations, among others. Additionally, under the RISAA, the FBI must establish minimum accountability mechanisms for personnel who conduct improper queries and must facilitate increased oversight by the Department of Justice Office of the Inspector General and Congress.

This report broadly addresses Section 702 in anticipation of its potential sunset or reauthorization. The report proceeds in three parts. First, it provides background on FISA generally and Section 702 specifically. The origins and parameters of each are summarized. Second, the report describes changes that the RISAA made to Section 702 and to other select portions of FISA. The report concludes with some considerations for Congress as it deliberates on Section 702 in light of its impending sunset date.

Contents

Contacts

Introduction

Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes U.S. government surveillance of non-U.S. persons abroad by collecting foreign intelligence information from domestic electronic communications systems.[1] The Foreign Intelligence Surveillance Court (FISC) authorizes the government to carry out this surveillance within approved parameters for up to one year at a time.[2] The government does not have to seek court authorization for every individual it targets. Section 702 surveillance is therefore authorized programmatically rather than individually.[3]

Since its enactment in 2008,[4] Section 702 has been the subject of extensive debate and several amendments.[5] Congress enacted Section 702 with an automatic repeal date,[6] and each reauthorization has included a new sunset provision.[7] Accordingly, Congress has regularly reconsidered and reauthorized the legal framework established by Section 702.[8] These reauthorizations have generally been the vehicles by which Congress has made changes to the statute.

Congress last reauthorized Section 702 on April 20, 2024, via the Reforming Intelligence and Securing America Act (RISAA).[9] The RISAA extensively amended Section 702 and other portions of FISA relevant to Section 702. The RISAA also provides that Section 702 will sunset on April 20, 2026, absent further reauthorization.[10] In anticipation of Congress's deliberation on whether to reauthorize the statute or permit it to lapse, this report provides an overview of FISA generally and Section 702 specifically, outlines changes that Congress made to Section 702 in the RISAA, and discusses some potential considerations for Congress regarding Section 702.

Background on FISA

Congress enacted FISA in 1978, ostensibly as a response to concerns regarding warrantless surveillance of individuals in the United States by the executive branch.[11] Proponents saw FISA as a means to address legal uncertainty surrounding the executive branch's constitutional

[1] 50 U.S.C. § 1881a(a).

[2] *Id*.

[3] CRS In Focus IF11451, *Foreign Intelligence Surveillance Act (FISA)*, by Andreas Kuersten, at 2 (2024).

[4] FISA Amendments Act (FAA) of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, 2438.

[5] *E.g.*, Laura K. Donohue, *The Evolution and Jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review*, 12 HARV. NAT'L SEC. J. 198 (2021); William C. Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, 51 U. RICH. L. REV. 671 (2017); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117 (2015) [hereinafter Donohue 2015].

[6] FAA, Pub. L. No. 110-261, § 403, 122 Stat. at 2473.

[7] *See, e.g.*, Reforming Intelligence and Securing America Act (RISAA), Pub. L. No. 118-49, § 19, 138 Stat. 862, 891 (2024) (providing that section 702 will automatically be repealed "two years after the date of enactment of the [RISAA]").

[8] Congress has reauthorized Section 702 four times. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012); FISA Amendments Reauthorization Act of 2017 (FISA 2017), Pub. L. No. 115-118, 132 Stat. 3 (2018); National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, § 7902, 137 Stat. 136, 1108 (2023); RISAA § 19.

[9] RISAA, Pub. L. No. 118-49, 138 Stat. at 862.

[10] *Id*. § 19.

[11] *Infra* notes 12–16 and accompanying text.

authority to carry out warrantless surveillance of individuals within the United States for purposes of obtaining foreign intelligence information.[12] The Supreme Court had expressly declined to rule on the constitutionality of this practice,[13] though some lower courts had endorsed it.[14] FISA also was viewed as a reaction to revelations in the 1970s of long-running and extensive executive branch abuses of surveillance authority.[15] For example, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activity (the Church Committee) found that the executive branch had consistently and improperly surveilled domestic actors without warrants based on those actors' political views, not genuine national security concerns.[16]

FISA provides a statutory framework under which the federal government can seek and receive court authorization to conduct electronic surveillance to collect foreign intelligence information in the United States.[17] For each target, the government must show probable cause that the target is a foreign power or agent of a foreign power and that the target is using, or is about to use, the facilities or places where the search or surveillance will be conducted.[18] FISA also delineates how collected information can be used and institutes congressional oversight processes.[19]

FISA created the Foreign Intelligence Surveillance Court (FISC) to hear and adjudge government applications to target individuals for surveillance.[20] To review FISC decisions denying government applications, FISA created the Foreign Intelligence Surveillance Court of Review (FISCR).[21] A 1977 Senate report described FISA as a "secure framework by which the Executive

[12] *E.g.*, ACLU Found. of So. Cal. v. Barr, 952 F.2d 457, 460–61 (D.C. Cir. 1991); Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2255–58 (2016); William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1102–10 (2007); Viet D. Dinh & Wendy J. Keefer, *FISA and the Patriot Act: A Look Back and a Look Forward*, 35 GEO. L.J. ANN. REV. OF CRIM. P. iii, iv–ix (2006).

[13] *See* United States v. U.S. Dist. Court for Eastern Dist. of Mich., S. Div. (*Keith)*, 407 U.S. 297, 321–22 (1972) (stating, in relation to a ruling barring warrantless surveillance for domestic security purposes, "[w]e have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents"); *cf.* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013) ("Although the *Keith* opinion expressly disclaimed any ruling 'on the scope of the President's surveillance power with respect to the activities of foreign powers,' it implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible.") (internal citation omitted); United States v. Warsame, 547 F. Supp. 2d 982, 985 (D. Minn. 2008) ("FISA was a congressional response to the Supreme Court's decision in [*Keith*, 407 U.S. at 321–22], which expressly declined to decide whether the Fourth Amendment limits the President's power to conduct electronic surveillance to obtain foreign intelligence information for national security purposes.").

[14] *E.g.*, United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 607–08 (3d Cir. 1974).

[15] *E.g.*, S. REP. NO. 95-604, at 7 (1977); Mondale et al., *supra* note 12, at 2259–62; Funk, *supra* note 12, at 1110–11; Dinh & Keefer, *supra* note 12, at ix.

[16] SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS, U.S. SENATE, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 5–6 (1976)

[17] Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1806–1885c). Electronic surveillance directed solely at communications transmitted by means exclusively used by foreign powers or property under the exclusive control of foreign powers does not require judicial authorization as long as collecting U.S.-person communications is unlikely and procedures meant to avoid collecting U.S.-person communications are followed. 50 U.S.C. § 1802(a)(1).

[18] Kuersten, *supra* note 3, at 1.

[19] 50 U.S.C. §§ 1806–1808.

[20] *Id.* § 1803(a).

[21] *Id.* § 1803(b).

Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights."[22]

Over time, Congress has amended and expanded FISA to cover additional surveillance methods. FISA now addresses domestic surveillance for the purpose of collecting foreign intelligence information carried out by means of (1) electronic surveillance, (2) physical searches, (3) pen registers and trap and trace (PR/TT) devices (i.e., devices that record or decode dialing, routing, addressing, or signaling information), or (4) the production of certain business records.[23] FISA also now contains provisions governing methods for acquiring foreign intelligence information domestically by targeting U.S. and non-U.S. persons abroad,[24] as discussed below.

Background on Section 702

Congress added Section 702 to FISA in 2008 as part of the FISA Amendments Act of 2008 (FAA).[25] Similar to FISA's enactment in 1978, commenters have described Section 702 as a response to new surveillance technology, government surveillance practices, and court decisions.[26] Following the terrorist attacks on the United States on September 11, 2001, the George W. Bush Administration initiated bulk telecommunications data collection practices by government intelligence agencies targeting communications in which at least one party was located abroad and one party was reasonably believed to be affiliated with a terrorist organization.[27] This initially occurred outside of the FISA legal framework because the Bush Administration believed that FISA procedures were overly burdensome, and the executive branch asserted authority for these collections under alternative legal theories.[28] After this government surveillance came to light in 2005, the Bush Administration sought FISC authorization under FISA.[29] In January 2007, the FISC authorized the government to target communications when the government (1) reasonably believed that at least one communicant was abroad and (2) had probable cause to believe that at least one communicant was associated with Al Qaeda or an affiliated terrorist organization.[30] In May 2007, when the government sought to renew the earlier order, the FISC authorized surveillance procedures where the court, not the government, made the probable cause determination as to the target's terrorist affiliation, requiring the government to

[22] S. REP. NO. 95-604, at 15 (1977).

[23] *See* 50 U.S.C. §§ 1801–1813 (addressing electronic surveillance); *id*. §§ 1821–1829 (addressing physical searches); *id*. §§ 1821–1829 (addressing PR/TT devices); *id*. §§ 1861–1864 (addressing the production of certain business records). For a succinct overview of FISA, see CRS In Focus IF11451, *Foreign Intelligence Surveillance Act (FISA)*, by Andreas Kuersten (2024).

[24] 50 U.S.C. §§ 1881–1881h.

[25] FAA, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. at 2438; 50 U.S.C. § 1881a.

[26] *E.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 403–04 (2013); THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2014) [hereinafter PCLOB REPORT 2014], https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf; Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH. L. REV. 401, 405–11 (2019); Donohue 2015, *supra* note 5, at 124–42.

[27] *Clapper*, 568 U.S. at 403; Adams, *supra* note 26, at 407.

[28] Adams, *supra* note 26, at 407; Donohue 2015, *supra* note 5, at 126.

[29] PCLOB REPORT 2014, *supra* note 26, at 17; Adams, *supra* note 26, at 407.

[30] *Clapper*, 568 U.S. at 403; PCLOB REPORT 2014, *supra* note 26, at 17; Adams, *supra* note 26, at 408.

seek FISC approval for each target and acquisition.[31] This transformed the program from being programmatically authorized to requiring individual authorization for each target.

During this period, the government was also undertaking surveillance operations under FISA in which it sought FISC orders compelling private telecommunications service providers (TSPs) "to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States-based communication service providers."[32] This process required individualized court orders for each acquisition.[33]

The Bush Administration contended that the aforementioned processes, by requiring individualized court orders for each target and TSP collaboration, required "considerable resources" and created an "intelligence gap."[34] It submitted a proposal to Congress to modify FISA to ease collecting foreign intelligence information when a target is located abroad.[35]

In August 2007, Congress responded by enacting the Protect America Act (PAA) of 2007, a temporary measure set to expire in 180 days.[36] In broad terms, the PAA allowed the Attorney General (AG) to authorize, for up to one year, acquiring foreign intelligence information from targets reasonably believed to be abroad so long as the AG and the Director of National Intelligence (DNI) determined that

> (1) Reasonable procedures were in place for determining that the acquisition concerned persons reasonably believed to be located outside the United States; (2) The acquisition did not constitute electronic surveillance (it did not involve solely domestic communications); (3) The acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to communications; (4) A significant purpose of the acquisition was to obtain foreign intelligence information; and (5) Minimization procedures outlined in FISA would be used.[37]

The AG had to submit the government's targeting procedures to the FISC and certify that no purely domestic communications would be intercepted.[38] If the court determined that the government was not "clearly erroneous" in assessing that its procedures for avoiding intercepting purely domestic communications were reasonable, then the court had to approve the procedures.[39] The PAA expired in February 2008.[40]

Congress enacted the FAA in July 2008.[41] Among other things, the FAA added to FISA Title VII, "Additional Procedures Regarding Certain Persons Outside the United States," which includes Sections 702, 703, and 704.[42] Title VII "addresses methods of acquiring foreign intelligence information targeting persons outside of the United States."[43] Sections 703 and 704 govern

---

[31] *Clapper*, 568 U.S. at 403; PCLOB REPORT 2014, *supra* note 26, at 17; Adams, *supra* note 26, at 408.

[32] PCLOB REPORT 2014, *supra* note 26, at 17.

[33] Adams, *supra* note 26, at 408.

[34] PCLOB REPORT 2014, *supra* note 26, at 18.

[35] Adams, *supra* note 26, at 409; Donohue 2015, *supra* note 5, at 135.

[36] Protect America Act of 2007 (PAA), Pub. L. No. 110-55, 121 Stat. 552 (repealed 2008); *see* PCLOB REPORT 2014, *supra* note 26, at 19 (describing the interactions leading to the PAA).

[37] Donohue 2015, *supra* note 5, at 136; PAA § 2.

[38] PAA, Pub. L. No. 110-55, § 3, 121 Stat. at 555 (repealed 2008).

[39] *Id*.

[40] *Id*. § 6(c).

[41] Pub. L. No. 110-261, 122 Stat. 2436.

[42] *Id*. § 101(a)(2).

[43] Kuersten, *supra* note 3, at 2.

targeting U.S. persons abroad with methods aimed at collecting foreign intelligence information domestically and internationally, respectively.[44] Section 702 establishes procedures for targeting non-U.S. persons abroad by collecting foreign intelligence information from communications that may travel through domestic communications infrastructure.[45] Whereas other sections of FISA require individualized FISC authorizations to target individuals and acquire foreign intelligence information, collections under Section 702 are authorized programmatically.[46]

In general terms, Section 702 requires the AG and DNI to compose a certification specifying the surveillance procedures that the government will use to target non-U.S. persons abroad and submit this to the FISC for approval.[47] The AG and DNI must also affirm to the FISC that these procedures align with statutory requirements concerning targeting individuals for surveillance, minimizing the collection and incorrect handling of information, and when and how the government can search collected information.[48] The FISC must review the aforementioned submission and either (1) order the government to remedy any shortcomings in the certification or (2) approve the certification and authorize surveillance and collections under it for up to one year.[49] If the certification is approved, the government can then direct electronic communication service providers (ECSPs) to assist in targeting non-U.S. persons reasonably believed to be abroad.[50] An ECSP is any of the following: (1) a provider of telecommunications services;[51] (2) a service that provides users the ability to send or receive wire or electronic communications;[52] (3) a provider of public computer storage or processing services using an electronic communications system;[53] (4) a communication service provider with access to wire or electronic communications as such communications are transmitted or stored;[54] (5) a communication service provider with access to equipment used to transmit or store wire or electronic communications, except in certain circumstances;[55] or (6) an officer, employee, custodian, or agent of any entity previously listed.[56]

The AG and DNI's certification must also contain querying procedures governing how and when government agencies can search (i.e., query) information collected under Section 702.[57] The FISC must ensure that these procedures are consistent with the Fourth Amendment's protections against

[44] 50 U.S.C. §§ 1881b, 1881c. A "United States Person" under FISA is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence . . . , an unincorporated association a substantial number 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).

[45] *Id.* § 1881a.

[46] Kuersten, *supra* note 3, at 2.

[47] 50 U.S.C. § 1881a(h).

[48] *Id.*

[49] *Id.* § 1881a(j). The AG and DNI can, if they determine that exigent circumstances exist, authorize surveillance without a court-approved certification, but they must submit a certification to the FISC for approval within seven days of commencing such surveillance. *Id.* § 1881a(h)(1)(B).

[50] *Id.* § 1881a(i). ECSPs can petition the FISC "to modify or set aside such directive" to provide information to the government. *Id.* § 1881a(i)(4).

[51] *Id.* § 1881a(b)(4)(A); 47 U.S.C. § 153(51).

[52] 50 U.S.C. § 1881a(b)(4)(B); 18 U.S.C. § 2510(15).

[53] 50 U.S.C. § 1881a(b)(4)(C); 18 U.S.C. § 2711(2).

[54] 50 U.S.C. § 1881a(b)(4)(D).

[55] *Id.* § 1881a(b)(4)(E).

[56] *Id.* § 1881a(b)(4)(F).

[57] *Id.* § 1881a(f)(1)(A).

unreasonable searches and seizures.[58] Section 702 contains numerous querying restrictions specific to the FBI, given its law enforcement mandate.[59] For example, FBI personnel (1) cannot, except in limited circumstances, use U.S.-person terms to carry out queries aimed solely at investigating criminal activity; (2) must, except in limited circumstances, obtain approval from a supervisor or an attorney before querying Section 702 information using U.S.-person terms; and (3) must, except in limited circumstances, obtain approval from the Deputy Director of the FBI before querying Section 702 information using terms reasonably believed to identify U.S. elected officials, appointees, political candidates or organizations, or media personnel or organizations.[60]

Changes Under the Reforming Intelligence and Securing America Act

The last meaningful changes to Section 702 were enacted via the FISA Amendments Reauthorization Act of 2017 (FISA 2017).[61] The primary changes that Congress made involved regulating the querying of Section 702 information, including requiring the AG to adopt querying procedures consistent with constitutional protections and limiting the FBI's authority to query Section 702 data.[62]

In April 2024, Congress enacted the RISAA, which reauthorized Section 702 and amended FISA.[63] This section addresses changes made by the RISAA to Section 702 and to other parts of FISA that are relevant to Section 702.[64]

Reauthorization

The RISAA extended Section 702 for two years from the RISAA's enactment, meaning that Section 702 will now sunset on April 20, 2026, absent further reauthorization.[65]

In the event that Section 702 sunsets on April 20, 2026, this would not necessarily mean that the government must cease engaging in activities authorized by Section 702 on that date. If a FISC order authorizing government collections and querying under Section 702 is in effect on the date that the section sunsets, the FAA permits the government to continue acquiring foreign intelligence information and querying under that order until the order's expiration date.[66] The FISC may also continue administering previously authorized procedures according to Section 702 until the court's orders authorizing the procedures expire.[67]

[58] *Id.* § 1881a(f)(1)(C).

[59] *Id.* §§ 1881a(f)(2), (f)(3).

[60] *Id.* §§ 1881a(f)(2), (f)(3)(A), (f)(3)(D)(ii). For a definition of U.S.-person, see *supra* note 43.

[61] FISA 2017, Pub. L. No. 115-118, 132 Stat. 3.

[62] *Id.* § 101(a)(1)(B).

[63] Pub. L. No. 118-49, 138 Stat. 862.

[64] For a list of prior reauthorizations, see *supra* note 8.

[65] *Id.* § 19(a).

[66] Pub. L. No. 110-261, § 404(b), 122 Stat. at 2476.

[67] *Id.*

Targeting U.S. Persons

The RISAA articulates the following "sense of Congress" with regard to targeting U.S. persons under Section 702:

> It is the sense of Congress that, as proscribed in section 702(b)(2), section 702 of the Foreign Intelligence Surveillance Act of 1978 has always prohibited, and continues to prohibit, the intelligence community from targeting a United States person for collection of foreign intelligence information. If the intelligence community intends to target a United States person for collection of foreign intelligence information under the Foreign Intelligence Surveillance Act of 1978, the Government must first obtain an individualized court order based upon a finding of probable cause that the United States person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power, in order to conduct surveillance targeting that United States person.[68]

"Sense of Congress" provisions are generally not treated by reviewing courts as establishing legally enforceable rights or obligations.[69] However, such provisions may inform a court's understanding of the legislative intent behind other legally enforceable provisions of the legislative enactment.[70]

Abouts Collections

Between 2018 and enactment of the RISAA, "abouts collection" was, as a general matter, barred under FISA Section 702.[71] However, such collection could be authorized under certain circumstances.[72] Abouts collection entails "acquiring communications that contain a reference to, but are not to or from, a target of an acquisition authorized under [Section 702]."[73] Under Section 103 of the FISA 2017, the FISC could authorize abouts collections pursuant to a certification, and the AG and DNI could implement such an authorization and conduct abouts collections without individual FISC approvals under certain circumstances.[74] In order to carry out such collections, the AG and DNI first had to submit a written notice of their intent to conduct abouts collections, and any supporting materials, to the congressional intelligence and judiciary committees.[75] Beginning on the date that notice was provided, the relevant committees had thirty days to "hold hearings and briefings and otherwise obtain information in order to fully review the written notice."[76] During this review period, the AG and DNI could not implement abouts collections.[77] The aforementioned process was not necessary in the event that the AG and DNI determined that exigent circumstances necessitated conducting abouts collections.[78] The congressional intelligence and judiciary committees had to be notified within seven days of such a

[68] RISAA, Pub. L. No. 118-49, § 4(a), 138 Stat. at 867. For a definition of U.S.-person, see *supra* note 43.

[69] *See generally* CRS Report R46484, *Understanding Federal Legislation: A Section-by-Section Guide to Key Legal Considerations*, by Victoria L. Killion (2002), at 26-27 (discussing caselaw interpreting sense of Congress provisions).

[70] *Id.*

[71] 50 U.S.C. § 1881a(b)(5) (2018).

[72] *Id.*

[73] Redacted, 402 F. Supp. 3d 45, 55 (FISC 2011).

[74] 50 U.S.C. § 1881a(b)(5) (2018).

[75] FISA 2017, Pub. L. No. 115-118, § 103(b)(2)(A), 132 Stat. at 10–11. The written notice's required contents are delineated in section 103(b)(3) of the Act. *Id.* § 103(b)(3).

[76] *Id.* § 103(b)(2)(B).

[77] *Id.* § 103(b)(2)(C).

[78] *Id.* § 103(b)(4)(A).

determination.[79] Finally, the head of each intelligence community element that engaged in abouts collections had to "fully and currently inform" congressional intelligence committees of any "material breach" (i.e., "significant noncompliance with applicable law or an order of the [FISC] concerning any acquisition of abouts communications").[80]

Some observers flagged the government's ability to potentially restart abouts collection as a threat to Americans' privacy and civil liberties because, using such collection, the government could too easily acquire purely domestic communications and communications between individuals unsuspected of wrongdoing.[81] These observers advocated that Congress remove the government's ability to restart abouts collection.[82] An alternative suggestion was that Congress, as a general matter, remove the government's authority to restart abouts collection without congressional approval, except in exigent circumstances.[83]

Under the RISAA, the government is barred from resuming abouts collections under Section 702, with no exceptions.[84]

Foreign Intelligence Information Definition

Prior to the RISAA, FISA defined "foreign intelligence information" as

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[85]

The RISAA amended the definition of foreign intelligence information to include under subsection (1) of 50 U.S.C. § 1801(e) information relating to "international production,

[79] *Id.*

[80] *Id.* § 103(b)(5)(B); 50 U.S.C. § 1881a(m)(4)(A), (m)(4)(B)(ii) (2018).

[81] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them Before the Subcomm. on Crime and Federal Government Surveillance of the H. Comm. on the Judiciary*, 118th Cong. 6 (2023) (statement of Sharon Bradford Franklin, Chair, Privacy and Civil Liberties Oversight Bd.) [hereinafter Franklin Statement]; *accord Fixing FISA, Part II Before the Subcomm. on Crime and Federal Government Surveillance of the H. Comm. on the Judiciary*, 118th Cong. 11 (2023) (testimony of Elizabeth Goitein, Senior Dir., Liberty and Nat'l Sec. Program, Brennan Ctr. for Just. at N.Y.U. Sch. of Law) [hereinafter Goitein Statement].

[82] Franklin Statement, *supra* note 81, at 5–6; Goitein Statement, *supra* note 81, at 3–4.

[83] THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 203 (2023) [hereinafter PCLOB REPORT 2023], https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf.

[84] RISAA, Pub. L. No. 118-49, § 22, 138 Stat. at 892; 50 U.S.C. § 1881a(b)(5). This amendment was offered and agreed upon during RISAA's consideration on the floor of the House. 170 Cong. Rec. H2351 (Apr. 12, 2024).

[85] 50 U.S.C. § 1801(e) (2018).

distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned."[86] The new definition expands the government's authority to target non-U.S. persons abroad to acquire foreign intelligence information under Section 702.[87]

Definition of Electronic Communication Service Provider

Section 702 only permits information acquisition from or with the assistance of an electronic communication service provider (ECSP).[88] Prior to the RISAA, FISA defined an "electronic communication service provider" (ECSP) to include (1) "a telecommunications carrier"; (2) "a provider of electronic communication service"; (3) "a provider of a remote computing service"; (4) "any other communication provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored"; or (5) "an officer, employee, or agent of an entity" previously described.[89]

The RISAA expanded the definition of an ECSP to include any other service provider that "has access to equipment that is being or may be used to transmit or store wire or electronic communications."[90] This does not include an entity that serves as (1) "a public accommodation facility"; (2) "a dwelling"; (3) "a community facility"; or (4) "a food service establishment."[91]

Querying

Prior to the RISAA, some commenters described FBI noncompliance with Section 702 querying restrictions as a problem,[92] identifying "inadequate supervisory review" of FBI queries as a contributing factor.[93] Commenters suggested that supervisor or attorney review of proposed queries prior to their implementation was a potentially effective way to "help detect and prevent compliance errors before they occur."[94] Some observers also proposed regular, "effective internal oversight" by offices like the FBI Office of General Counsel as a means to "identify and correct compliance errors close in time to their occurrence."[95] The Department of Justice Inspector

[86] RISAA, Pub. L. No. 118-49, § 23, 138 Stat. at 893; 50 U.S.C. § 1801(e)(1)(D). This amendment was offered and agreed upon during RISAA's consideration on the floor of the House. 170 Cong. Rec. H2351 (Apr. 12, 2024).

[87] 50 U.S.C. § 1881a(a).

[88] *Id.* § 1881a(h)(2)(A)(vi).

[89] 50 U.S.C. 1881(4) (2018). The definition of a telecommunications carrier is provided in 47 U.S.C. § 153(51). The definition of an electronic communication service is provided in 18 U.S.C. § 2510(15). The definition of a remote computing service is provided in 18 U.S.C. § 2711(2).

[90] RISAA, Pub. L. No. 118-49, § 25(a), 138 Stat. at 893; 50 U.S.C. § 1881(b)(4)(E). This amendment was offered and agreed upon during RISAA's consideration on the floor of the House. 170 Cong. Rec. H2357 (Apr. 12, 2024).

[91] 50 U.S.C. § 1881(b)(4)(E). The definition of a public accommodation facility is provided in 50 U.S.C. § 1861(4). The definition of a dwelling is provided in 42 U.S.C. § 3602(b). The definition of a community facility is provided in 42 U.S.C. § 1592n(c). The definition of a food service establishment is provided in 7 U.S.C. § 1638(3).

[92] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them Before the Subcomm. on Crime and Federal Government Surveillance of the H. Comm. on Appropriations*, 118th Cong. 7 (2023) (statement of Michael E. Horowitz, Inspector Gen., U.S. Dep't of Justice) [hereinafter Horowitz Statement]; *accord* Goitein Statement, *supra* note 81, at 13–17. In a 2022 opinion, the FISC detailed extensive improper querying of Section 702 data by FBI personnel. Memorandum Opinion and Order 26–34 (FISC Apr. 21, 2022), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.

[93] Horowitz Statement, *supra* note 92, at 7.

[94] *Id.*

[95] *Id.*

General (DOJ IG) also recommended additional oversight by both his office and the Privacy and Civil Liberties Oversight Board (PCLOB), though he noted the limited resources of the DOJ OIG relative to its responsibilities, particularly "resource intensive" national security reviews.[96]

Training

Under the RISAA, FBI personnel must complete training on querying procedures prior to conducting queries.[97] This training must be completed annually.[98]

Information Access Controls

The RISAA mandates certain access mechanisms for FBI information storage systems that store both unminimized information gathered under Section 702 and information gathered by other lawful means.[99] Unminimized data refers to information that has not been subjected to minimization procedures that prevent improper data acquisition, retention, and dissemination.[100] In turn, minimized data is data that has been subjected to authorized minimization procedures and can include, for example, information that has been stripped of U.S.-person identifiers.[101] FBI personnel are required to affirmatively include unminimized information collected under Section 702 in any query.[102] The FBI also must deploy other controls "reasonably expected to prevent inadvertent queries of such unminimized" information.[103]

Queries Unrelated to National Security

Prior to the RISAA, Section 702 barred the FBI, except in certain circumstances, from accessing information collected under Section 702 for use in investigations unrelated to national security "that [was] retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence."[104] The FBI could apply for an exception to this restriction with the FISC.[105] An application had to identify the officer making it and contain "a statement of the facts and circumstances relied upon" to believe that the desired information would provide evidence of (1) "criminal activity"; (2) "contraband, fruits of a crime, or other items illegally possessed by a third party"; or (3) "property designed for use, intended for use, or used in committing a crime."[106] The FISC could grant an application if it found probable cause to believe that Section 702 information would provide the aforementioned evidence.[107] The FBI could conduct the query without applying for and receiving an order from the FISC if the bureau

[96] *Id*. at 8. The PCLOB is an independent agency within the executive branch, headed by a five-member board, that is tasked with reviewing federal counterterrorism programs to ensure privacy and civil liberties are protected. 42 U.S.C. § 2000ee(c).

[97] RISAA, Pub. L. No. 118-49, § 2(d), 138 Stat. at 863; 50 U.S.C. § 1881a(f)(3)(D)(i).

[98] 50 U.S.C. § 1881a(f)(2)(A).

[99] RISAA, Pub. L. No. 118-49, § 2(d), 138 Stat. at 863; 50 U.S.C. § 1881a(f)(3)(D)(iv).

[100] 50 U.S.C. § 1801(h).

[101] *Id*. § 1801(h)(2).

[102] *Id*. § 1881a(f)(3)(D)(iv)(I).

[103] *Id*. § 1881a(f)(3)(D)(iv)(II).

[104] *Id*. § 1881a(f)(2)(A) (2018).

[105] *Id*. § 1881a(f)(2)(A)–(B).

[106] *Id*. § 1881a(f)(2)(C).

[107] *Id*. § 1881a(f)(2)(D).

determined that there was "a reasonable belief" that the information "could assist in mitigating or eliminating a threat to life or serious bodily harm."[108]

Congress amended this subsection through the RISAA to prohibit, absent excepting circumstances, "[FBI] queries of [Section 702] information . . . that are solely designed to find and extract evidence of criminal activity."[109] Exceptions to this restriction include situations in which (1) "there is a reasonable belief that such query may retrieve information that could assist in mitigating or eliminating a threat to life or serious bodily harm" or (2) "such query is necessary to identify information that must be produced or preserved in connection with a litigation matter or to fulfill discovery obligations in criminal matters."[110]

U.S.-Person Queries

Prior to the RISAA, 50 U.S.C. § 1881a barred the FBI, except in certain circumstances, from querying Section 702 data using U.S.-person terms in the context of investigations unrelated to national security and when such terms were not employed in pursuit of foreign intelligence.[111] The FBI could query Section 702 data using U.S.-person terms in the aforementioned situations if it obtained a court order allowing such a query or excepting conditions existed[112] (i.e., if the FBI "determine[d] there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm").[113]

Under the RISAA, FBI personnel must obtain approval from a supervisor or attorney with proper authority to query Section 702 data using a U.S.-person term.[114] Such approval is not required if the person conducting the query "has a reasonable belief that conducting the query could assist in mitigating or eliminating a threat to life or serious bodily harm."[115] Additionally, prior to employing a U.S.-person query term, FBI personnel must "provide a written statement of the specific factual basis to support the reasonable belief that such query meets the" querying requirements that the AG and DNI must adopt under 50 U.S.C. § 1881a(f)(1).[116] The FBI must also, with regard to queries involving U.S.-person terms, record the query term, the date, the individual who conducted the query, and the aforementioned written statement.[117]

Sensitive Queries

Prior to the RISAA, some commenters expressed concern that, under Section 702, the U.S. intelligence community could potentially "be weaponized against politically disfavored

[108] *Id*. § 1881a(f)(2)(E).

[109] RISAA, Pub. L. No. 118-49, § 3(a), 138 Stat. at 866; 50 U.S.C. § 1881a(f)(2)(A). The subsection heading for this restriction states, "Limits on authorizations of United States person queries," though the language of the subsection does not set out specific query terms that must be used in order for this restriction to apply. 50 U.S.C. § 1881a(f)(2)(A) (2024). The RISAA also describes this subsection as "revoking [FBI] authority to conduct queries unrelated to national security." RISAA § 3(a). It is therefore potentially ambiguous as to whether this limitation applies to all queries solely seeking evidence of criminal activity or just such queries that employ U.S.-person terms.

[110] 50 U.S.C. § 1881a(f)(2)(B).

[111] *Id*. § 1881a(f)(2)(A) (2018). For a definition of U.S.-person, see *supra* note 44.

[112] 50 U.S.C. § 1881a(f)(2)(B) (2018).

[113] *Id*. § 1881a(f)(2)(E) (2018).

[114] RISAA, Pub. L. No. 118-49, § 2(a)(2), 138 Stat. at 862; 50 U.S.C. § 1881a(f)(3)(A)(i).

[115] 50 U.S.C. § 1881a(f)(3)(A)(ii).

[116] *Id*. §§ 1881a(f)(3)(D)(iii), 1881a(f)(1).

[117] *Id*. § 1881a(f)(3)(A)(iii).

opponents."[118] These observers recommended that Congress consider codifying "enhanc[ed] pre-approval policies" with regard to "sensitive queries . . . involving elected officials, members of the media, and religious figures," or requiring that the Deputy Director of the FBI or the FISC review these queries before they can be undertaken.[119]

The RISAA provides that, absent exigent circumstances, FBI personnel must receive approval from certain superiors prior to conducting "sensitive queries."[120] FBI personnel must receive approval from

- the FBI Deputy Director to use "a query term reasonably believed to identify" a U.S. elected official, presidential or state governor appointee, U.S. political candidate, U.S. political organization or a prominent U.S. person in such organization, or a U.S. media organization or a U.S. member of such organization;[121]
- an FBI attorney to use "a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization";[122] and
- an FBI attorney to conduct a query "involv[ing] batch job technology (or successor tool)."[123]

Defensive Briefings

The RISAA limits the circumstances under which the FBI can query Section 702 information using the name or restricted information of a Member of Congress "for the exclusive purpose of supplementing the contents of a briefing on the defense against a counterintelligence threat to a member of Congress."[124] Either (1) the Member in question must consent to using the query term(s) or (2) the FBI Deputy Director must determine "that exigent circumstances exist sufficient to justify the conduct of such query."[125] The FBI Director must notify "appropriate congressional leadership" within three days of requesting a Member's consent.[126] The Director must also notify appropriate congressional leadership within three days of conducting a query without a Member's consent in light of exigent circumstances.[127]

Information Access

The RISAA provides that the FBI "may not ingest unminimized [FISA Section 702 information] into its analytic repositories unless the targeted person is relevant to an existing, open, predicated

[118] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them Before the Subcomm. on Crime and Federal Government Surveillance of the H. Comm. on the Judiciary*, 118th Cong. 3 (2023) (Statement of Beth A. Williams, Member, Priv. and C.L. Oversight Bd.).

[119] *Id*. at 3–4.

[120] RISAA, Pub. L. No. 118-49, § 2(d), 138 Stat. at 863; 50 U.S.C. § 1881a(f)(3)(D)(ii).

[121] 50 U.S.C. § 1881a(f)(3)(D)(ii)(I).

[122] *Id*. § 1881a(f)(3)(D)(ii)(II).

[123] *Id*. § 1881a(f)(3)(D)(ii)(III).

[124] RISAA, Pub. L. No. 118-49, § 2(f), 138 Stat. at 865; 50 U.S.C. § 1881a(f)(3)(C).

[125] 50 U.S.C. § 1881a(f)(3)(C)(i).

[126] *Id*. § 1881a(f)(3)(C)(ii)(I). "Appropriate congressional leadership" entails the (1) chairs and ranking members of the congressional intelligence committees; (2) House Speaker and minority leader; and (3) Senate majority and minority leaders. *Id*. § 1881a(f)(3)(C)(iv).

[127] *Id*. § 1881a(f)(3)(C)(ii)(II).

full national security investigation."[128] This restriction does not apply, however, if the FBI Director determines exigent circumstances require analyzing the unminimized information and informs certain congressional committees and leaders within three business days of processing the information.[129] The restriction also does not apply if the FBI "has agreed to provide technical, analytical, or linguistic assistance at the request of another Federal agency."[130]

Vetting Non-U.S. Persons

Prior to the RISAA, the executive branch stated that it was precluded from utilizing Section 702 data for the sole purpose of vetting non-U.S. persons seeking entry into the United States.[131] In the executive branch's view, it was not authorized to query Section 702 data unless the query was "reasonably likely to return foreign intelligence information (or evidence of a crime in the case of the FBI)."[132]

Some observers asserted that the government's inability to utilize Section 702 information to vet individuals for immigration purposes or security clearances was disadvantageous to national security.[133] These commenters advised Congress to consider modifying these restrictions to ensure that people entering the country and those who are entrusted with sensitive information are "thoroughly vetted against information already in the Government's possession."[134] Others, however, worried that allowing Section 702 information to be used for vetting, particularly immigration vetting, could facilitate undesirable actions against those "seeking refuge in the United States."[135]

Pursuant to the RISAA, the AG, in consultation with the DNI, must ensure that the querying procedures that the AG adopts "enable the vetting of all non-United States persons who are being processed for travel to the United States using terms that do not qualify as United States person query terms."[136]

Intelligence Courts

Amicus Curiae

Prior to the RISAA, some commenters suggested that the role of amici curiae in FISC proceedings should be strengthened to provide counterweights to government assertions made before the court in support of requests to authorize surveillance under Section 702.[137] Proposals included expanding the situations in which the FISC must appoint amici curiae, ensuring that

[128] RISAA, Pub. L. No. 118-49, § 3(b), 138 Stat. at 867; 50 U.S.C. § 1881a(n)(1). For a description of minimized and unminimized data, see *supra* notes 100–101 and accompanying text.

[129] 50 U.S.C. § 1881a(n)(2). For a definition of U.S.-person, see *supra* note 44.

[130] *Id*. § 1881a(n)(3).

[131] PCLOB REPORT 2023, *supra* note 83, at B-37.

[132] *Id*.

[133] *Id*. at 4.

[134] *Id*.

[135] H.R. REP. NO. 118-302, at 100 (2023).

[136] RISAA, Pub. L. No. 118-49, § 24, 138 Stat. at 893; 50 U.S.C. § 1881a(f)(6).

[137] PLCOB REPORT 2023, *supra* note 83, at 212; Franklin Statement, *supra* note 81, at 6–7; Goitein Statement, *supra* note 81, at 30–31.

amici curiae have access to all information before the court, and authorizing amici curiae to appeal decisions of both the FISC and FISCR.[138]

The RISAA requires the FISC and FISCR to designate at least one amicus curiae to assist the court in considering "any certification or procedures submitted for review pursuant to [50 U.S.C. § 1881a(h)]," unless the court finds "that such appointment is not appropriate or is likely to result in undue delay."[139] Amicus curiae must, "to the maximum extent practicable," possess "expertise in both privacy and civil liberties and intelligence collection."[140]

If the FISC or FISCR appoints one or more amici curiae, the court must issue an order ruling on any certification, procedures, or amendments within sixty days of the date on which submissions were made or within sixty days of the court appointing one or more amici curiae, whichever is earlier.[141] The court can take longer if it issues an order finding that "extraordinary circumstances" necessitate additional time and that an extension "is consistent with the national security."[142]

Accountability

Under the RISAA, the FBI Director must ensure that the FBI has measures in place "for holding the executive leadership of each covered component appropriately accountable for ensuring compliance with covered procedures by [FBI personnel] assigned to that covered component."[143] (A "covered component" is an FBI element with personnel who have access to unminimized Section 702 data; a "covered procedure" is any procedure governing the use of FISA authority, including querying and minimization procedures.)[144]

In addition, the FBI Director must institute "minimum accountability standards" with "escalating consequences for noncompliant querying of [U.S.-person] terms."[145] These standards must include (1) "zero tolerance for willful misconduct"; (2) "escalating consequences for unintentional noncompliance," including a threshold for mandatory revocation of access to Section 702 information; and (3) "consequences for supervisors who oversee users that engage in noncompliant queries."[146] These standards must be issued within ninety days of the RISAA being enacted.[147]

[138] PLCOB REPORT 2023, *supra* note 83, at 212; Franklin Statement, *supra* note 81, at 7; Goitein Statement, *supra* note 81, at 30–31.

[139] RISAA, Pub. L. No. 118-49, § 5(b), 138 Stat. at 868; 50 U.S.C. § 1803(i)(2)(A)(iii).

[140] 50 U.S.C. § 1803(i)(2)(B).

[141] *Id*. § 1803(i)(2)(C). Ordinarily, the court must complete review and issue an order within thirty days of a certification, procedure, or amendment being submitted. *Id*. § 1881a(j)(1)(B).

[142] *Id*. § 1803(i)(2)(C).

[143] RISAA, Pub. L. No. 118-49, § 12(b)(1), 138 Stat. at 880.

[144] *Id*. § 12(b)(3)(B)–(C). For a description of minimized and unminimized data, see *supra* notes 100–101 and accompanying text.

[145] *Id*. § 16(a)(1); 50 U.S.C. § 1881a(f)(4).

[146] 50 U.S.C. § 1881a(f)(4).

[147] RISAA, Pub. L. No. 118-49, § 16(a)(2), 138 Stat. at 883.

Congressional and Inspector General Oversight

Targeting U.S. Persons

Under the RISAA, Congress requires mandatory reviews and audits of targeting decisions made pursuant to Section 702.[148] "Not less frequently than annually," the DOJ National Security Division must review each person targeted under Section 702 the previous year to make sure none are known U.S. persons.[149] The results of this review must be submitted to the DOJ OIG and the congressional intelligence and judiciary committees.[150]

The DOJ OIG must also, "[n]ot less frequently than annually," audit a sampling of the targeting decisions reviewed by the DOJ National Security Division and submit a report to the congressional intelligence and judiciary committees.[151]

Additionally, within 180 days of the RISAA's enactment, and annually thereafter, agencies authorized to target non-U.S. persons abroad under Section 702 must certify to Congress that no targeting decision made during the previous year targeted a known U.S. person.[152]

Intelligence Courts

The RISAA mandates that certain congressional leadership and their staff have access to FISC and FISCR proceedings.[153] The chairs and ranking minority members of the congressional intelligence and judiciary committees, Senate Majority and Minority Leaders, and Speaker of the House and House Minority Leader are entitled to attend intelligence court proceedings.[154] Pursuant to procedures established by the AG in consultation with the DNI, each of the aforementioned congressional leaders may designate up to two staff members from their committee or office to attend intelligence court proceedings on their behalf.[155]

The RISAA further requires that FISC and FISCR hearings be transcribed and that records of proceedings "be stored in a file associated with the relevant application or order."[156] Within forty-five days of the government receiving a final transcript or when the given matter is resolved, whichever is later, the AG must submit "a notice of the existence of such transcript" to the congressional intelligence and judiciary committees.[157] The AG must also submit any declassified intelligence court decisions, orders, and opinions.[158]

U.S.-Person Queries

The RISAA requires that the FBI Director submit an annual report to the congressional intelligence committees that includes (1) the number of U.S.-person queries of unminimized FISA

[148] *Id.* § 4.

[149] *Id.* § 4(b)(1). For a definition of U.S.-person, see *supra* note 44.

[150] *Id.*

[151] *Id.* § 4(b)(2).

[152] *Id.* § 4(b)(3).

[153] *Id.* § 5(d).

[154] *Id.*

[155] *Id.*

[156] *Id.* § 8(a); 50 U.S.C. § 1803(c).

[157] RISAA, Pub. L. No. 118-49, § 8(b), 138 Stat. at 874; 50 U.S.C. § 1871(c)(3).

[158] 50 U.S.C. § 1871(c)(4).

Section 702 information; (2) the number of approved queries that utilized batch job technology (or successor technology); (3) the number of queries that utilized batch job technology (or successor technology) that were not preapproved due to exigent circumstances; (4) the number of U.S.-person term queries of unminimized Section 702 data conducted "solely to retrieve evidence of a crime"; (5) an estimate of the number of U.S.-person term queries of unminimized Section 702 data carried out "primarily to protect the [U.S.] person who is the subject of the query"; and (6) an estimate of the number of U.S.-person terms used to conduct queries of unminimized Section 702 data where the U.S. person is the target or subject of an FBI investigation.[159] Each report, subject to declassification review by the AG and DNI, must be publicly available by April following the calendar year that the report covers.[160]

In addition, starting one year after January 1, 2025, the FBI Director must submit a quarterly report to the congressional intelligence and judiciary committees that includes the number of U.S.-person queries carried out during the previous quarter.[161]

Section 2(c) of the RISAA also requires the FBI to audit each query that utilized a U.S.-person term within 180 days of the query being conducted.[162] This requirement will sunset either two years after the RISAA's enactment or on the date that the AG certifies to the congressional intelligence and judiciary committees that the FBI has implemented an internal process for auditing queries that utilize U.S.-person terms.[163]

Sensitive Queries

Under the RISAA, the FBI Director must "promptly notify appropriate congressional leadership" and the lawmaker in question when the FBI conducts a query "using a query term that is reasonably believed to be the name or other personally identifying information of a member of Congress."[164] The FBI Director can waive this requirement if the Director determines that notification would impede an ongoing investigation. A waiver must terminate, however, when the Director determines that notification will no longer impede an ongoing investigation or when a relevant investigation ends, whichever is earlier.[165]

Accountability Measures

Within ninety days of the RISAA's enactment, the FBI Director must submit the minimum accountability standards mandated by Section 16(a)(1) of the Act to the congressional intelligence and judiciary committees.[166] By December 1, 2024, "and annually thereafter for 3 years," the

[159] RISAA, Pub. L. No. 118-49, § 11(a)(1)(C), 138 Stat. at 878. For a definition of U.S. person, see *supra* note 43. For a description of minimized and unminimized data, see *supra* notes 100–101 and accompanying text.

[160] RISAA, Pub. L. No. 118-49, § 11(a)(1)(C), 138 Stat. at 878.

[161] *Id*. This amendment was offered and agreed upon during RISAA's consideration on the floor of the House. 170 Cong. Rec. H2357 (Apr. 12, 2024).

[162] *Id*. § 2(c)(1).

[163] *Id*. § 2(c)(3).

[164] *Id*. § 2(e); 50 U.S.C. § 1881a(f)(3)(B)(i). "Appropriate congressional leadership" entails the (1) chairs and ranking members of the congressional intelligence committees; (2) House Speaker and minority leader; and (3) Senate majority and minority leaders. 50 U.S.C. § 1881a(f)(3)(B)(ii). The FBI Director must "give due regard" to protecting "classified information, sources and methods, and national security" when providing notification. *Id*. § 1881a(f)(3)(B)(iii). This notification requirement is distinct from the restriction on querying section 702 data using lawmaker terms for defensive briefings noted above. *See supra* notes 120–123 and accompanying text.

[165] 50 U.S.C. § 1881a(f)(3)(B)(iv).

[166] RISAA, Pub. L. No. 118-49, § 16(a)(3)(A), 138 Stat. at 883.

Director must submit a report to the same committees describing each adverse personnel action taken pursuant to the minimum accountability standards and detailing the conduct in issue.[167]

The FBI Director must also submit an annual report to the congressional intelligence and judiciary committees describing the accountability actions taken during the previous year to address noncompliant Section 702 information querying.[168] This must include the number of ongoing investigations and the outcomes of completed investigations and related adverse personnel actions.[169]

In addition, the DNI, in consultation with the FBI, must conduct a study on potential "technological enhancements" that would allow the FBI to monitor bureau systems containing Section 702 information for compliance in real time.[170] The results must be submitted to the congressional intelligence and judiciary committees within one year of the RISAA's enactment.[171]

Unauthorized Disclosures

Under the RISAA, the DNI must notify the congressional intelligence committees "as soon as practicable" (but not less than seven days) after becoming aware of "an actual or potential significant unauthorized disclosure or compromise of [Section 702 information]."[172]

Inspector General Audit

The RISAA requires the DOJ OIG to submit a report on FBI querying practices to the congressional intelligence and judiciary committees within 545 days of the Act's enactment.[173] The report must contain (1) an assessment of FBI compliance with querying procedures; (2) analysis of each reform "responsible for any identified improvement" in FBI compliance and whether such a reform was statutory, required by the FISC or AG, or voluntarily adopted by the FBI Director; (3) an appraisal of the FBI's implementation of all reforms required by the RISAA; (4) an evaluation of the FBI Office of Internal Auditing's effectiveness at monitoring and improving FBI compliance with querying procedures; (5) recommendations for improving FBI compliance with querying procedures; and (6) anything else that the OIG deems relevant.[174]

Considerations for Congress

As Section 702's sunset date approaches,[175] there are numerous potential considerations for Congress.

[167] *Id*. § 16(a)(3)(B).

[168] *Id*. § 12(a)(2); 50 U.S.C. § 1873(e).

[169] 50 U.S.C. § 1873(e).

[170] RISAA, Pub. L. No. 118-49, § 18(b)(1), 138 Stat. at 884.

[171] *Id*. § 18(b)(2).

[172] *Id*. § 18(a).

[173] *Id*. § 9(a)(1).

[174] *Id*. § 9(a)(2).

[175] *See supra* note 11 and accompanying text.

Instituting a Warrant Requirement for Queries of Section 702 Information Using U.S.-Person Terms

Some government officials and private actors have suggested adding a warrant requirement for the government to query Section 702 information using U.S.-person terms.[176] They contend that allowing the government to conduct these searches without court review permits an end run around the Fourth Amendment's protection against unreasonable government searches and threatens Americans' privacy rights.[177] These critics have suggested that Congress impose "a requirement for FISA court review of U.S. person query terms, to ensure protection of Americans' Fourth Amendment rights."[178] Other government actors have objected to such a requirement, however, and claimed that imposing it could unduly limit government access to information that could be critical to national security.[179] Officials have suggested that this could "force the government to turn a blind eye to threat information that it had lawfully acquired, with potentially grave consequences to our nation's security."[180] Then-FBI Director Christopher Wray further stated that queries using U.S.-person terms are usually conducted early in an investigation before the government can establish probable cause or demonstrate urgency to a court.[181]

A federal district court ruled in February 2025 that, under the Fourth Amendment, the government must obtain a warrant to search Section 702 data using U.S.-person terms, unless a specific, established exception to the warrant requirement applies.[182] The ruling emanated from the defendant's effort to suppress evidence that the government obtained by using terms associated with him to query Section 702 information without a warrant.[183] The defendant is a lawful permanent resident, which means he is a U.S. person under FISA.[184] The U.S. Court of Appeals for the Second Circuit had previously determined that "querying . . . stored [Section 702] data [has] important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable."[185] The appellate court remanded the case and ordered the district court to "conduct an inquiry into whether any querying of databases of Section 702–acquired information using terms related to

[176] PCLOB REPORT 2023, *supra* note 83, at 205; Franklin Statement, *supra* note 81, at 4–5; *Fixing FISA, Part II Hearing Before the Subcomm. on Crime and Federal Government Surveillance of the H. Comm. on the Judiciary*, 118th Cong. 2 (2023) (statement of Gene Schaerr, Gen.Counsel of PPSA and Managing Partner, Schaerr Jaffe LLP) [hereinafter Schaerr Statement]; Goitein Statement, *supra* note 81, at 8.

[177] *Supra* note 176.

[178] Franklin Statement, *supra* note 81, at 5; *accord* PCLOB REPORT 2023, *supra* note 83, at 205; Schaerr Statement, *supra* note 176, at 3–4; Goitein Statement, *supra* note 81, at 23.

[179] *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 12 (2023) (joint statement of Chris Fonzone, Gen. Counsel, Off. of the Dir. of Nat'l Intel., George Barnes, Deputy Dir., NSA, David Cohen, Deputy Dir., CIA, Paul Abbate, Deputy Dir., FBI, and Matthew Olsen, Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Just.).

[180] *Id*.

[181] *Warrant Requirement for FBI's Section 702 Queries Would Impede Investigations, Endanger National Security, Director Says*, FBI (Apr. 9, 2024), https://www.fbi.gov/news/stories/warrant-requirement-for-fbi-s-section-702-queries-would-impede-investigations-endanger-national-security-director-says.

[182] United States v. Hasbajrami, No. 11-cf-623, 2025 WL 447498, at *9 (E.D.N.Y. Feb. 10, 2025); *see id*. at *5 (agreeing with the defendant that "querying a Section 702 database in connection with a U.S. person generally requires a warrant, even where the initial interception was lawfully conducted").

[183] *Id*. at *1.

[184] *Id*. at *4; 50 U.S.C. § 1801(i).

[185] United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019).

[the defendant] was lawful under the Fourth Amendment."[186] The district court, in addition to holding that querying Section 702 information using U.S.-person terms presumptively requires a warrant, also concluded that the "foreign intelligence exception" to the warrant requirement did not apply.[187] This exception entails "the executive proceed[ing] without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants."[188] For this exception to apply, the FISCR has further held that (1) "the purpose behind the surveillances [at issue must go] well beyond any garden-variety law enforcement objective" and (2) there must have been "a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake."[189] The district court ultimately determined that the foreign intelligence exception did not apply, but that the evidence would not be excluded because the "good faith exception" did apply: the "government agents . . . 'acted with an objectively reasonable good-faith belief that their conduct was lawful.'"[190] It remains to be seen how any potential appeal will be decided.

Congress could act in a number of ways on this issue, including (1) leaving procedures for using U.S.-person query terms unchanged; (2) requiring that the FISC review and approve any use of U.S.-person query terms; (3) amending executive branch review procedures concerning such queries; or (4) allowing Section 702 to sunset.

Giving Amici Curiae Authority to Appeal Intelligence Court Decisions

Some commenters have recommended giving amici curiae authority to appeal FISC and FISCR decisions as a means to increase adversariality in FISA proceedings and potentially facilitate increased appellate review of intelligence court determinations.[191] As it stands, targeting proceedings before the FISC and FISCR are ex parte (i.e., they only involve one party: the government),[192] and only the government can appeal adverse FISC and FISCR decisions.[193]

There are potential constitutional issues with Congress giving amici curiae authority to appeal intelligence court decisions. To appeal a court determination, an individual must have standing, which entails having suffered "(1) a concrete and particularized injury; (2) that is traceable to the allegedly unlawful actions of the opposing party; and (3) that is redressable by a favorable judicial decision."[194] Amici curiae satisfy none of these conditions and, therefore, despite any

[186] *Id*. at 673.

[187] *Hasbajrami*, 2025 WL 447498, at *16.

[188] United States v. Hung, 629 F.2d 908, 916 (4th Cir. 1980); *see Keith*, 407 U.S. 297, 315 (1972) ("If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and the free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.").

[189] In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISC Rev. 2008).

[190] *Hasbajrami*, 2025 WL 447498, at *20 (quoting Davis v. United States, 564 U.S. 229, 238 (2011)).

[191] PLCOB REPORT 2023, *supra* note 83, at 212; Franklin Statement, *supra* note 81, at 7.

[192] *E.g.*, 50 U.S.C. § 1805(a).

[193] *Id*. § 1803(b), (c).

[194] Cong. Rsch. Serv., *Overview of Standing*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/artIII-S2-C1-6-1/ALDE_00012992/ (last visited Jun. 25, 2025); *see* (continued...)

legislation, are unlikely to satisfy constitutional standing requirements to appeal an intelligence court decision.[195]

Draft legislation introduced in 2023 included provisions giving amici curiae authority to petition the FISC and FISCR to certify questions of law for review by the FISCR and Supreme Court, respectively.[196] These provisions, if enacted, could also raise constitutional issues by giving amici curiae an unfettered right to be heard during litigation, a right generally reserved for parties to a dispute who have constitutional standing.[197] Requiring courts to hear and rule on matters brought before them by amici curiae could be interpreted as requiring courts to adjudge issues outside of the case and controversy before them, and thus beyond federal courts' jurisdiction under Article III of the Constitution.[198]

Another potential avenue for facilitating non-government appeals of intelligence court decisions entails authorizing the FISCR to review FISC decisions sua sponte (i.e., at its own discretion).[199] FISA currently authorizes the FISC to certify certain questions of law for FISCR review.[200] Congress could amend FISA to allow the FISCR to review FISC decisions either in certain circumstances or at its discretion.[201] Congress could additionally authorize an avenue or mechanism for amici curiae to present FISC decisions to the FISCR that they think should be reviewed, with the FISCR deciding whether to consider any such submission and whether to review a decision.[202]

Acquiring Information from Third Parties

Numerous media outlets have reported that government agencies, including intelligence agencies, have acquired information on U.S. persons by purchasing information from data brokers and other third parties.[203] Critics of such practices characterize them as enabling the government to

---

Diamond v. Charles, 476 U.S. 54, 71 (1986) (dismissing an appeal because the individual seeking to appeal the lower court's decision "lack[ed] any judicially cognizable interest" in the case and therefore did not have standing to appeal).

[195] *E.g.*, Aaron X. Sobel, *Procedural Protections in a Secret Court: FISA Amici and Expanding Appellate Review of FISA Decisions*, 172 U. PA. L. REV. ONLINE 13, 19–20 (2023); *see* Transunion LLC v. Ramirez, 594 U.S. 413, 429 (2021) (determining that Congress cannot give an individual standing via legislation when the individual lacks a cognizable legal interest in a given matter under the Constitution).

[196] H.R. 6570, 118th Cong. § 5(b)(2) (2023).

[197] *See, e.g.*, United States v. Michigan, 940 F.2d 143, 166 (6th Cir. 1991) ("Only a named party or an intervening real party in interest is entitled to litigate on the merits.").

[198] *Cf. Diamond*, 476 U.S. at 62 ("The exercise of judicial power . . . can so profoundly affect the lives, liberty, and property of those to whom it extends . . . that the decision to seek review must be placed in the hands of those who have a direct stake in the outcome.") (internal quotation marks and citations omitted); *Michigan*, 940 F.2d at 165 ("Historically, there has been a bright-line distinction between amicus curiae and named parties/real parties in interest in a case or controversy.").

[199] Sobel, *supra* note 195, at 20.

[200] 50 U.S.C. § 1803(j).

[201] Sobel, *supra* note 195, at 20–21.

[202] *Id.*

[203] *E.g.*, Alfred Ng, *Data Brokers Raise Privacy Concerns—But Get Millions From the Federal Government*, POLITICO (Dec. 21, 2022), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600; Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It*, THE WASH. POST (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/; Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 22, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Sara Morrison, *A Surprising Number of Government Agencies Buy Cellphone Location Data. Lawmakers Want to Know Why*, VOX (Dec. 2, 2020), https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

circumvent constitutional protections and FISA requirements.[204] These critics argue that what they call the "data broker loophole" should be closed.[205] The Office of the DNI, for its part, has stated that "commercially available information," including information that is "sold, leased, or licensed," is "increasingly important" to intelligence agencies.[206]

In 2023, the 118th Congress considered the Fourth Amendment is Not for Sale Act, which sought to prohibit law enforcement and intelligence agencies from purchasing U.S.-person information from third parties.[207] The Act passed in the House but did not pass in the Senate.[208] Congress could pursue similar legislation, limit or promote government purchases of U.S.-person data from third parties in other ways, or take no action on this matter.

Definition of Electronic Communication Service Provider

As described above, the RISAA expanded the FISA definition of an ECSP that can be directed to provide foreign intelligence information to the government.[209] An ECSP now includes any service provider that "has access to equipment that is being or may be used to transmit or store wire or electronic communications," not including any entity that serves as (1) "a public accommodation facility"; (2) "a dwelling"; (3) "a community facility"; or (4) "a food service establishment."[210] Commentators believe this was done in response to decisions by the FISC and FISCR finding that a certain entity was not an ECSP and that the government therefore could not direct it to provide foreign intelligence information.[211]

[204] *E.g.*, Goitein Statement, *supra* note 79, at 23; Jake Laperruque, *With the Passage of RISAA, FISA 702 Reform has Been Delayed but not Denied*, CTR FOR DEMOCRACY & TECH. (May 16, 2024), https://cdt.org/insights/with-the-passage-of-risaa-fisa-702-reform-has-been-delayed-but-not-denied/; Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, THE BRENNAN CTR. (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

[205] *Supra* note 204 and accompanying text.

[206] *Intelligence Community Policy Framework for Commercially Available Information*, OFF. OF THE DIR. OF NAT'L INT. (last visited June 30, 2025), https://www.intelligence.gov/commercially-available-information.

[207] Fourth Amendment is Not for Sale Act, H.R. 4639, 118th Cong. (2023).

[208] *All Actions: H.R.4639 – 118th Congress (2023-2024)*, CONGRESS.GOV (last visited June 30, 2025), https://www.congress.gov/bill/118th-congress/house-bill/4639/all-actions.

[209] *Supra* notes 87–89 and accompanying text.

[210] 50 U.S.C. § 1881(b)(4)(E).

[211] David Aaron, *Unpacking the FISA Section 702 Reauthorization Bill*, JUST SEC. (Apr. 18, 2024), https://www.justsecurity.org/94771/unpacking-the-fisa-section-702-reauthorization-bill/. For the FISC and FISCR opinions, see In re Petition to set Aside or Modify Directive Issued [Redacted] (FISC 2022), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf; In re Petition to Set Aside or Modify Directive Issued to [Redacted] (FISC Rev. 2023), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf.

Critics of this expanded definition contend that it too greatly enlarges the number of individuals and entities that are potentially subject to directives to provide the government with foreign intelligence information.[212] They argue that any actor that merely has access to certain equipment can now be a vehicle for government surveillance; the target of a government directive no longer needs to be a telecommunications carrier or service provider.[213] Others, however, do not believe that the change is substantial and note exceptions to the definition and the fact that an entity must still be able to acquire non-U.S. person communications overseas in order to be subject to a government directive.[214] In light of the aforementioned concerns, Congress could further amend the definition of an ECSP or leave it as is.

Information on Incidental Collections

Prior to the RISAA, some commenters identified as a concern the lack of information on the volume of "incidental collection" carried out under Section 702.[215] Incidental collection entails U.S.-person communications that are collected in the course of targeting non-U.S. persons for surveillance under Section 702.[216] Estimating the volume of incidental collection could, in certain individuals' estimation, aid Congress in assessing whether and what safeguards against incidental collection are needed.[217] The PCLOB recommended that Congress require the government to provide regular estimates of the volume of incidental collection carried out under Section 702 or require the government to undertake a pilot project for estimating this volume.[218]

Congress could take no action in this regard, require the government to study the feasibility of and methods for gathering data on incidental collection, or require the government to craft methods for estimating the volume of incidental collection and begin collecting and reporting information on incidental collection.

Author Information

Andreas Kuersten
Legislative Attorney

[212] *E.g.*, John Miller, *Expansion of FISA Electronic Communications Service Provider Definition Must be Removed*, INFO. TECH. INDUS. COUNCIL (Apr. 16, 2024), https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed; Laperruque, *supra* note 203.

[213] *Supra* note 212.

[214] Aaron, *supra* note 211.

[215] PCLOB REPORT 2023, *supra* note 83, at 209; Franklin Statement, *supra* note 81, at 2–4.

[216] Rachel G. Miller, *FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?*, 95 NOTRE DAME L. REV. REFLECTION 139, 148 (2020). For a definition of U.S.-person, see *supra* note 43.

[217] PCLOB REPORT 2023, *supra* note 83, at 210; Franklin Statement, *supra* note 81, at 4.

[218] PCLOB REPORT 2023, *supra* note 83, at 211; Franklin Statement, *supra* note 81, at 4.

Disclaimer