FISA REAUTHORIZATION: HOW AMERICA'S MOST CRITICAL NATIONAL SECURITY TOOL MUST BE REFORMED TO CONTINUE TO SAVE AMERICAN LIVES AND LIBERTY

Report of the Majority FISA Working Group of the
House Permanent Select Committee on Intelligence

U.S. House of Representatives

November 2023

Executive Summary

"There is nothing so likely to produce peace as to be well prepared to meet an enemy."[1]

- *George Washington, January 29, 1780, Letter to Elbridge Gerry*

If Congress fails to act, Section 702 of the Foreign Intelligence Surveillance Act (FISA) will expire. Section 702 of FISA is one of the most effective tools used by the Intelligence Community to protect our nation. If it sunsets, so too will our ability to identify, prevent, and mitigate threats to our democracy. We will go "blind" to many critical national security risks that threaten our homeland and our military interests abroad.[2] Our allies around the world, many of whom depend upon information acquired under Section 702 to circumvent threats of their own, will also be compromised.[3] Although the reauthorization of Section 702 is imperative for protecting our national security, recent disturbing abuses of Section 702 and other provisions of FISA impacting U.S. persons require a complete review of Section 702 authorities and the enactment of meaningful reforms.

This report will provide a detailed explanation of what FISA is and is not, who uses it and how, why it is such a critical tool in need of reauthorization, the problems with the law in its current form, and what reforms Congress should consider during the reauthorization process. The information contained within is provided in a declassified format for public consumption. There is no need for Section 702 to be shrouded in mystery. The American people have a right to know about the tool that silently protects them 24 hours of the day, 365 days a year.

Congress enacted FISA (50 U.S.C. §§ 1801 *et seq*.) in 1978 to provide a statutory framework for government agencies to gather foreign intelligence information through electronic

---

[1] Letter from George Washington to Elbridge Gerry (Jan. 29, 1780).

[2] Nomaan Merchant & Eric Tucker, *Congress' Anger at FBI Shapes Surveillance Program's Future*, ASSOCIATED PRESS (Apr. 28, 2023) (quoting Rep. Jason Crow, "If we lose this program, we just go blind overnight in a lot of critical areas."); Remarks by Assistant Att'y General Matthew Olsen at Brookings Inst. on Section 702 (Feb. 28, 2023) ("At this moment, when China is ramping up its aggressive efforts to spy on Americans, it would be a grievous mistake to blind ourselves to that threat by allowing this critical authority to expire."); *see also* President Donald J. Trump, Remarks at the White House on the FISA Amendments Reauthorization Act of 2017 (Jan. 19, 2018) ("It has enabled our Intelligence Community to disrupt numerous plots against our citizens at home and our warfighters abroad, and it has unquestionably saved American lives.").

[3] *See "Section 702" Saves Lives, Protects the Nation and Allies*, NAT'L SEC. AGENCY (Dec. 12, 2017); Brett Holmgren, Assistant Sec'y, Bureau of Intel. & Research, U.S. Dep't of State, Remarks at the Center for Strategic and Int'l Studies (May 30, 2023) ("In INR, it is hard to overstate the centrality of 702 collection to providing the Secretary of State and U.S. diplomats with objective, timely analysis. . . . Another way that INR and the State Department have benefitted from 702 is by sharing downgraded or declassified intelligence with allies and partners—a critical tool to strengthen U.S. leverage at the negotiating table, expose disinformation, or galvanize partners and allies. U.S. diplomats abroad routinely rely on 702 data for formal demarches, to pass threat information, or to engage counterparts on sensitive matters. Last year, many of the requests by U.S. diplomats to downgrade or declassify intelligence for sharing with foreign partners was sourced to 702 information.").

surveillance.[4] These provisions are often referred to as Title I or "Traditional FISA." FISA also established the Foreign Intelligence Surveillance Court (FISC), a specialized court which considers applications submitted by intelligence agencies requesting the legal approval needed to gather such information.[5] The judges that preside over the FISC are Senate-confirmed, Article III judges that rotate onto the bench, generally a week at a time, from their home federal districts.[6]

When Congress passed FISA in 1978, the law was drafted so that foreign persons located outside the U.S. were also outside the scope of FISA.[7] This was primarily due to the law's definition of "electronic surveillance" being constrained by the technological capabilities of the 1970's.[8] However, by 2008, both the nature of the threats and the technology used by bad actors had evolved considerably; in particular, "many terrorists and other foreign intelligence targets abroad were using communications services based in this country, especially those provided by U.S.-based Internet service providers."[9] Congress recognized that, as the threats and technology changed, so too must the law.[10]

In 2008, Congress amended FISA by adding Title VII, which includes Section 702, with significant bipartisan support.[11] Title VII was created to extend FISA's legal framework "to apply FISA's protections to overseas targets dependent based on the target's nationality, and not the location where the acquisition occurs."[12] Section 702 provides for the ability to collect foreign intelligence information when the electronic communications of non-U.S. persons reasonably believed to be located outside the United States travel through electronic service providers located within the United States.[13] Under Section 702, the U.S. government has the ability to compel electronic service providers to provide such information on a foreign individual within the constraints approved annually by the FISC.[14]

In the ensuing years, Section 702 has often described as "critical," "invaluable," and "important," but it is hard to find an adjective that adequately describes a tool that has done as much to safeguard American lives and liberty as it has. We are unable to calculate just how many lives it has saved. It is worth noting that there has not been another 9/11 since Section 702's inception, despite the persistent threat of terrorism.[15] However, despite Section 702 often referred

---

[4] 50 U.S.C. §§ 1801 *et seq*.
[5] FISA CT., *About the Foreign Intelligence Surveillance Court* (last visited Aug. 15, 2023).
[6] *Id*., *see also* FISA CT., *Rules of Procedures* (Nov. 1, 2010) ("Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.").
[7] OFFICE OF THE DIR. OF NAT'L INTEL., *The FISA Amendments Acts: Q&A* (Apr. 18, 2017).
[8] *Id*.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] Edward C. Liu, *Reauthorization of the FISA Amendments Act*, CONG. RESEARCH SERV. (Apr. 8, 2013).
[13] Edward C. Liu, *Foreign Intelligence Surveillance Act: An Overview*, CONG. RESEARCH SERV. (Apr. 6, 2021)
[14] *Id*.
[15] *See* Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Heritage Found. on Defending the Value of FISA Section 702 (Oct. 13, 2017) ("The fact that we have not suffered another 9/11-scale attack is not just luck. It is the product of an enormous amount of very, very hard work and diligence by thousands of professionals. Most importantly, it's a product of teamwork and information sharing and dot-connecting by those professionals in the post-9/11, post-wall world with dot-connecting made possible, especially by tools like Section 702.").

to in terms of preventing terrorism, its applications are far more diverse.[16] Including disrupting terror attacks, Section 702 also allows the U.S. government to effectively collect actionable intelligence on:

1. Proliferators of weapons of mass destruction;

2. Malicious hackers, including those who target U.S. critical infrastructure, such as hospitals and power companies, with ransomware;

3. Drug traffickers and their illicit plans to smuggle chemicals from China to create fentanyl and to traffic drugs, such as fentanyl and methamphetamine, across the Southern border;

4. Foreign spies attempting to target Americans or send operatives into the United States;

5. The murder of civilians and the forced relocation of children by the Russians in Ukraine;

6. Malign investments in U.S. companies by foreign actors seeking to undermine or steal U.S. technology; and

7. Other matters related to national and economic security risks. [17]

Four IC agencies utilize raw Section 702-acquired information on a daily basis to disrupt threats to the United States: the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the National Counterterrorism Center (NCTC).[18] Intelligence collected using Section 702 is also used to inform civilian and military officials across the government in both the executive and legislative branches.[19] In 2022, 59% of the articles in the President's Daily Brief contained information reported by the NSA using Section 702.[20]

However, this tool, which has done so much to protect the American people, has also been abused by those who swore to support and defend the American people—in particular, the FBI.[21] The FBI has neglected to treat authorities granted to it by Section 702 with the respect

[16] Edward C. Liu, *Reauthorization of the FISA Amendments Act*, CONG. RESEARCH SERV. (Apr. 8, 2013) ("Although FISA is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes. For example, it extends to the collection of information necessary for the conduct of foreign affairs.").
[17] OFFICE OF THE DIR. OF NAT'L INTEL., *FISA Section 702 Fact Sheet* (2023).
[18] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702: The Process* (2023).
[19] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702 of the Foreign Intelligence Surveillance Act* (2023) ("Once foreign intelligence is identified, the IC takes action—such as writing a report for the president, military, or other U.S. Government agencies that can prevent or disrupt a particular threat.").
[20] OFFICE OF THE DIR. OF NAT'L INTEL., *FISA Section 702 Fact Sheet* (2023).
[21] *See generally, Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, U.S. DEP'T OF JUSTICE OFFICE OF THE INSPECTOR GEN. (Dec. 2019) [hereinafter "Horowitz Report"];

those authorities deserve. Because of this, a reauthorization of Section 702 cannot occur without significant reforms. With this reauthorization, Congress not only has the opportunity to protect national security, but to enact significant and meaningful reforms designed to protect American civil rights and civil liberties too.

HPSCI's Bipartisan FISA Working Group was formed to identify all problems within FISA, including areas subject to abuses by the FBI, and to create solutions for each identified problem. Members met with experts outside the Committee, from constitutional law scholars to covert CIA officers who use Section 702 daily, to better understand what reforms were necessary. FISA Section 702 reauthorization provides Congress with a unique opportunity to enact reforms across FISA beyond Section 702 to create a better law in its entirety. The American people deserve a law that protects them from both governmental overreach and security threats. Section 702 must be reauthorized, but it also must be reformed.

If you are a Member of Congress who would like to receive more information about the contents of this report, please contact the House Permanent Select Committee on Intelligence (HPSCI) at (202) 225-4121. Classified briefings are available upon request.

Report on Matters Related to Intelligence Activities and Investigations Arising Out of the 2016 Presidential Campaigns, OFFICE OF SPECIAL COUNSEL JOHN DURHAM, U.S. DEP'T OF JUSTICE (May 12, 2023) [hereinafter "Durham Report"].

Table of Contents

History of FISA

"As I said a year and a half ago at the beginning of the process that produced this bill, 'One of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our Nation's security on the one hand, and the preservation of basic human rights on the other.' This is a difficult balance to strike, but the act I am signing today strikes it. It sacrifices neither our security nor our civil liberties. And it assures that those who serve this country in intelligence positions will have the affirmation of Congress that their activities are lawful."[22]

- *President Jimmy Carter, October 25, 1978,*
  Signing of S. 1566, the Foreign Intelligence Surveillance Act of 1978

"One of the important lessons learned after 9/11 was that America's intelligence professionals lacked some of the tools they needed to monitor the communications of terrorists abroad. It is essential that our Intelligence Community know who our enemies are talking to, what they're saying, and what they're planning."[23]

- *President George W. Bush, July 10, 2008,*
  Signing of H.R. 6304, the FISA Amendments Act of 2008

"I would have preferred a permanent reauthorization of Title VII to protect the safety and security of the Nation. By signing this Act today, however, I am ensuring that this lawful and essential intelligence program will continue to protect Americans for at least the next 6 years. We cannot let our guard down in the face of foreign threats to our safety, our freedom, and our way of life."[24]

- *President Donald J. Trump, January 19, 2018,*
  Signing of S. 139, the FISA Amendments Reauthorization Act of 2017

In January 1975, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee) was established to investigate the legality, propriety, and ethicality of intelligence activities undertaken by U.S. government intelligence agencies.[25] The inquiry was prompted by "allegations of abuse and improper activities by the intelligence agencies of the United States, and great public concern that the Congress take action to bring the intelligence agencies under the constitutional framework."[26] After holding 126 full committee meetings, 40 subcommittee hearings, interviewing approximately 800 witnesses, and reviewing 110,000 documents, the Church Committee published its final report in April 1976.[27] The Committee concluded that "intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily

[22] President Jimmy Carter, Remarks at the White House on the Foreign Intelligence Surveillance Act of 1978 (Oct. 25, 1978).
[23] President George W. Bush, Remarks at the White House on the FISA Amendments Act of 2008 (July 10, 2008).
[24] President Donald J. Trump, Remarks at the White House on the FISA Amendments Reauthorization Act of 2017 (Jan. 19, 2018).
[25] S. Res. 21, 94th Cong. (Jan. 1975).
[26] S. Select Comm. to Study Gov't Operations with Respect to Intel. Activities, S. Rep. No. 94-755 (1976), at Book I, p. III.
[27] *A History of Notable Senate Investigations: Senate Select Committee to Study Govern Operations with Respect to Intelligence Activities (The Church Committee)*, U.S. SENATE HISTORICAL OFFICE (last visited July 26, 2023).

because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."[28]

The Church Committee issued 96 recommendations, both legislative and regulatory, "to place intelligence activities within the constitutional scheme for controlling government power."[29] In response to the Church Committee's findings, FISA was carefully designed to establish safeguards on intelligence operations regarding the collection of foreign intelligence.[30] FISA was also a response to a 1972 Supreme Court case, *United States v. U.S. District Court*, in which the Court held that while warrantless electronic surveillance for purposes of domestic intelligence collection violated the Fourth Amendment, it "express[ed] no opinion as to the [the surveillance of the] activities of foreign powers or their agents."[31] When the Court declined to comment on the exact type of protections that should be afforded to foreigners, Congress stepped in to provide a constitutional legal framework.[32] On October 1978, President Jimmy Carter signed FISA into law.[33] FISA has been amended several times over the years, either expanding or limiting its scope.[34]

On September 11, 2001, the United States suffered the worst attack on U.S. soil since Pearl Harbor, when 2,977 Americans died during four coordinated terrorist attacks carried out by al-Qaeda.[35] The 9/11 Commission, established to investigate how such an attack could occur, found that:

> The September 11 attacks fell into the void between the foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets.[36]

---

[28] S. Select Comm. to Study Gov't Operations with Respect to Intel. Activities, S. Rep. No. 94-755 (1976), at Book II, p. 289.
[29] U.S. SENATE HISTORICAL OFFICE, *A History of Notable Senate Investigations: Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (The Church Committee)* (last visited July 26, 2023).
[30] Edward C. Liu, *Foreign Intelligence Surveillance Act: An Overview*, CONG. RESEARCH SERV. (Apr. 6, 2021) ("Following revelations regarding widespread privacy violations by the federal government during the Watergate era, Congress enacted FISA to establish guidelines for government collection of foreign intelligence.").
[31] *United States v. U.S. Dist. Ct. (Keith),* 407 U.S. 297, 321–24 (1972); *see also In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA CT. REV. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the United States qualifies for the "special needs" exception to the warrant requirement).
[32] *See* James Petrila, *A Brief History of Programmatic Collection Pre-Section 702*, LAWFARE (Apr. 12, 2023); Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023); James G. McAdams, III, *Foreign Intelligence Surveillance Act: An Overview*, FED. LAW ENFORCEMENT TRAINING CTRS. (2009).
[33] BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, *The Foreign Intelligence Surveillance Act of 1978* (last visited Sept. 18, 2023).
[34] *Id*.
[35] THE 9/11 MEMORIAL & MUSEUM, *9/11 FAQs* (last visited Aug. 16, 2023).
[36] The 9/11 Commission Report (2004), at 263.

Prior to 9/11, the American IC "struggled to retrieve and share pertinent information that was being communicated among terrorists using the rapidly evolving technology of the internet and cell phones."[37] Had such information been more readily available to our IC, 9/11 might have been prevented.[38]

In response to the gaps and shortcomings identified in the wake of 9/11, Congress enacted a series of important changes to national security laws over the following years designed to better protect the American people.[39] One of these was the FISA Amendments Act (FAA), which included Section 702.[40] The FAA was signed into law by President George W. Bush in July 2008, after Congress recognized the need to authorize the intelligence community "to acquire foreign intelligence information of non-U.S. persons reasonably believed to be outside the United States."[41]

Section 702 has been reauthorized by Congress twice. It was first reauthorized in 2012 by President Barack Obama and a second time in 2017 by President Donald Trump.[42] Section 702 is set to expire on December 31, 2023, if not reauthorized.

[37] THE WHITE HOUSE, *President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations for Reauthorization* (July 2023).
[38] *Id*.
[39] *Id*.
[40] *Id*.
[41] *Id*.
[42] James Petrila, *A Brief History of Programmatic Collection Pre-Section 702*, LAWFARE (Apr. 12, 2023).

Section 702 Explained

Overview

Title VII of FISA, which includes Section 702, provides a legal framework for electronic surveillance and other methods of gathering foreign intelligence information on targets outside the United States.[43] Title VII is designed to extend FISA's protections to targets outside the United States dependent primarily on the target's nationality, not the location where the information is gathered.[44] Section 702 cannot be used to target Americans or any foreign individual located inside the United States.[45]

All Courts Find Section 702 Constitutional

Section 702 has always been found to be constitutional under the Fourth Amendment.[46] Section 702 may only be used to target non-U.S. persons who are reasonably believed to be outside the United States for the purpose of obtaining foreign intelligence information.[47] As a result, Section 702 does not require the FISC to make probable-cause determinations before targeting foreign individuals for surveillance.[48] However, orders authorized under Title I do.[49] Section 702 requires the Attorney General, in consultation with the Director of National Intelligence (DNI), to adopt targeting procedures that are designed to:

> (A) ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States; and
>
> (B) prevent the intentional acquisition of 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. [50]

The three circuit courts and six district courts that have addressed the issue of Section 702 constitutionality have all unanimously held that Section 702-authorized collection is

---

[43] 50 U.S.C. §§ 1881 *et seq*.
[44] 50 U.S.C. § 1881a-c; *see also* Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONGR. RESEARCH SERV. (Mar. 17, 2023).
[45] 50 U.S.C. § 1881a.
[46] *See United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021) (affirming 187 F.Supp.3d 1240 (D. Colo. 2015)), *cert. denied*, 143 S. Ct. 246 (2022); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (affirming, in relevant part, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016)); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016) (affirming 2014 WL 2866749 (D. Or. June 24, 2014)), *cert. denied*, 138 S. Ct. 636 (2018); *United States v. Mohammad*, 339 F. Supp. 3d 724 (N.D. Ohio 2018); *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. June 28, 2018) (ECF No. 115).
[47] 50 U.S.C. § 1881a.
[48] 50 U.S.C. § 1881a(j).
[49] 50 U.S.C. § 1805.
[50] 50 U.S.C. § 1881a(d).

constitutional.[51] The U.S. Courts of Appeals for the Second, Ninth, and Tenth Circuits have all held that when "the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States, that target is not entitled to Fourth Amendment protections," even if the collection occurs inside the United States.[52] In addition, the FISC has repeatedly found Section 702 collection to be constitutional under the Fourth Amendment in its annual certification decisions.[53] Regarding incidental collection of U.S. persons' communications, the Second Circuit held in *United States v. Hasbajrami* that when surveillance is "lawful in the first place . . . the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful."[54]

Definitions

FISA has technical definitions for certain terms, including "electronic surveillance," "U.S. person," and "agent of a foreign power."

- Query: A "query" is a search of specific communications that have already been lawfully acquired to find foreign intelligence information. Performing a query is similar to using an email inbox's search feature to find a particular email. FISC-approved querying procedures provide rules governing how IC analysts can search for 702 targets' communications using queries.[55]

- Querying Procedures: Section 702 requires the Attorney General, in consultation with the DNI, to adopt "querying procedures" to govern how collected information collected under this section is searched after it has been collected. All querying procedures are required to be consistent with the Fourth Amendment. Each query must be reasonably likely to retrieve foreign intelligence information[56] or evidence of a crime.[57]

---

[51] *United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021) (affirming 187 F.Supp.3d 1240 (D. Colo. 2015)), *cert. denied*, 143 S. Ct. 246 (2022); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (affirming, in relevant part, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016)); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016) (affirming 2014 WL 2866749 (D. Or. June 24, 2014)), *cert. denied*, 138 S. Ct. 636 (2018); *United States v. Mohammad*, 339 F. Supp. 3d 724 (N.D. Ohio 2018); *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. June 28, 2018) (ECF No. 115).

[52] *Id.*; *see, specifically, United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021) (affirming 187 F.Supp.3d 1240 (D. Colo. 2015)), *cert. denied*, 143 S. Ct. 246 (2022) ("We agree with *Mohamud* and *Hasbajrami*. When the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States, that target is not entitled to Fourth Amendment protections. Even if the instrumentalities of surveillance were located in the United States, the foreign target does not have Fourth Amendment protection because 'what matters here is the location of the *target*, and not where the government literally obtained the electronic data.' *Mohamud*, 843 F.3d at 439 (quotations omitted) (emphasis in original)").

[53] *See, e.g.*, [Redacted], Mem. Op. (F.I.S.C. Nov. 18, 2020); [Redacted], Mem. Op. (F.I.S.C. Dec. 6, 2019).

[54] *United States v. Hasbajrami*, 945 F.3d 666 (2d Cir. 2019) (affirming, in relevant part, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016)).

[55] 50 U.S.C. § 1881a(f)(3)(B).

[56] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *CIA's Section 702 Querying Procedures* (Mar. 13, 2023); William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *NSA's Section 702 Querying Procedures* (Mar. 13, 2023); William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *NCTC's Section 702 Querying Procedures* (Mar. 13, 2023).

[57] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *FBI's Section 702 Querying Procedures* (Mar. 13, 2023); *see also* 50 U.S.C. § 1881a(f)(1).

- Targeting Procedures: Section 702 requires the Attorney General, in consultation with the DNI, to develop "targeting procedures" that intelligence officials will use to identify targets for surveillance under Section 702. These targeting procedures must be reasonably designed to: "(A) ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States; and (B) prevent the intentional acquisition of 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." The FISC then reviews these targeting procedures to ensure they are reasonably designed to limit targets to persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of communications in which all parties are known to be in the United States. Additionally, the government may not intentionally target any persons in the United States or U.S. persons who are abroad. It is illegal for the government to engage in "reverse targeting," in which an overseas non-U.S. person is targeted with the purpose of collecting on a particular person reasonably believed to be within the United States.[58]

- Incidental Collection: Any communication, such as emails or calls, collected between a Section 702 target and a non-target is referred to as "incidental collection." U.S. persons are never the target of Section 702. Any U.S. person whose communications are incidentally collected when they are communicating with a foreign target of Section 702 surveillance can never become the target of Section 702 collection themselves. The civil rights and civil liberties of U.S. persons whose communications are incidentally collected are safeguarded through FISC-approved minimization and querying procedures.[59] According to the ODNI, incidental collection involves three categories of individuals:

    1. Witting Participant: For example, a U.S. person contacts a member of ISIS looking for ways to support ISIS. Under Section 702, the government may learn of this contact through incidental collection if the ISIS member is a non-U.S. person, is located overseas, and is currently targeted under Section 702. The U.S. person cannot be targeted under Section 702. If the government wanted to conduct electronic surveillance of the U.S. person, it would have to apply for and obtain a probable cause-based order under FISA. The government could use the Section 702 incidental collection from the targeting of the non-U.S. person ISIS member in such a FISA application.

    2. Unwitting Participant: For example, an American consultant is hired to "advise" on a project by a non-U.S. person targeted under Section 702. The consultant is

[58] 50 U.S.C. § 1881a; Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).

[59] See *United States v. Hasbajrami*, 945 F.3d 666 (2d Cir. 2019) (affirming, in relevant part, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016), *United States v. Hasbajrami*, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016) ("While Section 702 does not allow intentional targeting of U.S. persons or non-U.S. persons located in the United States, 50 U.S.C. §1881a(b)(1)-(4), it is inevitable that the government will incidentally intercept communications of persons who are not the intended targets—including, as here, U.S. persons in the United States—during the ordinary course of lawful surveillance. Minimization and targeting procedures help protect the privacy interests of U.S. persons whose communications are incidentally intercepted."); OFFICE OF THE DIR. OF NAT'L INTEL., *Incidental Collection in a Targeted Intelligence Program* (2023).

unaware that the project involves the export of components related to weapons of mass destruction (WMDs). The non-U.S. person target's communications with the American consultant would contain incidentally collected U.S. person information. This information would allow the FBI to reach out to the consultant and warn him or her that their client is actually engaged in the proliferation of WMDs.

3. Potential Victim: For example, a non-U.S. person targeted under Section 702 initiates a cyber-intrusion of a U.S. company. The identity of the victimized U.S. company and its contact information would be incidental collection. The IC would use this information to warn or protect the U.S. company from attack.[60]

- Minimization Procedures: "Minimization procedures" are adopted by the Attorney General to minimize the acquisition and retention and prohibit the dissemination of nonpublic information of nonconsenting U.S. persons, consistent with the need to obtain, produce, and disseminate foreign intelligence information. FISA requires minimization procedures to prohibit the dissemination of nonpublic information that would identify a U.S. person, unless such person's identity is necessary to understand foreign intelligence information or assess its importance. FISA, however, provides minimization procedures allowing for the retention of information that is evidence of a crime and to disseminate such information for law enforcement purposes. The contents of a U.S. person's communications that are obtained under Section 102 (regarding communication methods and premises used exclusively by foreign governments) may not be retained for longer than 72 hours, unless a court order authorizing such surveillance is obtained, or if the information indicates a threat of death or serious bodily harm.[61]

- U.S. Person: A "U.S person" is 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.[62]

- Foreign Intelligence Information:

    1. Information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
        - Actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
        - Sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

[60] OFFICE OF THE DIR. OF NAT'L INTEL., *Incidental Collection in a Targeted Intelligence Program* (2023).
[61] 50 U.S.C. § 1801(h); Edward C. Liu, *Section-by-Section Summary of the Foreign Intelligence Surveillance Act of 1978*, CONG. RESEARCH SERV. (June 8, 2022).
[62] 50 U.S.C. § 1801(i).

- 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—
    - The national defense or the security of the United States; or
    - The conduct of the foreign affairs of the United States.[63]

- Foreign Power:

1. A foreign government or any component thereof, whether or not recognized by the United States;
2. A faction of a foreign nation or nations, not substantially composed of U.S. persons;
3. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
4. A group engaged in international terrorism or activities in preparation thereof;
5. A foreign-based political organization, not substantially composed of U.S. persons;
6. An entity directed and controlled by a foreign government or governments; or
7. An entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction.[64]

- Agent of a Foreign Power: FISA's definition of "agent of a foreign power" has different elements depending on whether the agent is a U.S. person or a non-U.S. person.

1. A non-U.S. person may be an agent of a foreign power if:
    - The person acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism, irrespective of whether the person is inside the United States;
    - The person acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the United States contrary to U.S. interests, when the circumstances show that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
    - The person engages in the international proliferation of weapons of mass destruction or activities in preparation thereof.

2. Any person (including a U.S. person) may be an agent of a foreign power if:
    - The person knowingly engages in unlawful clandestine intelligence-gathering activities for or on behalf of a foreign power;

[63] 50 U.S.C. § 1801(e).
[64] 50 U.S.C. § 1801(a).

- The person, under the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
- The person knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power;
- The person knowingly aids or abets any person in, or conspires with any person to engage in, the conduct of activities described in the above; or
- The person knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power.[65]

- Electronic Surveillance: FISA's definition of "electronic surveillance" includes four categories in which communications are acquired. Each category of electronic surveillance varies based on the target of the acquisition, the type of communication being acquired, and the location where the communication is being acquired. The four categories are:

    1. Acquisitions of wire or radio communications by targeting a specific U.S. person who is presently in the United States.
    2. Acquisition of the contents of a wire communication to or from a person in the United States, if such acquisition occurs in the United States.
    3. Acquisition of the contents of any radio communication where both the sender and all intended recipients are located within the United States.
    4. Installation or use of an electronic, mechanical, or other surveillance device in the United States to acquire information, other than from a wire or radio communication.[66]

[65] 50 U.S.C. § 1801(b); Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).
[66] 50 U.S.C. § 1801(f); Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).

The Foreign Intelligence Surveillance Courts

FISA established two specialized courts to consider applications for the use of FISA's investigative authorities and to issue or deny orders authorizing the use of said authorities: the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR).[67] The FISC hears the government's primarily *ex parte* applications to use FISA's investigative authorities.[68] The FISCR hears the government's appeals from the FISC.[69] In general, the FISC operates like every other federal court in the country, with rules of procedure, written filings, hearings, orders, and opinions.[70]

When the FISC was originally established in 1978, its primary purpose was to review applications for electronic surveillance inside the United States for foreign intelligence purposes.[71] Over time, Congress expanded the jurisdiction of the FISC to keep up with evolving threats and technology.[72] Today, "the FISC reviews and decides whether to approve requests related to a number of other investigatory activities for foreign intelligence purposes, including searches of property in the United States, applications to conduct pen register and trap and trace surveillance, requests to obtain business records, applications to conduct certain surveillance activities overseas that target U.S. persons who are officers, employees, or agents of a foreign power, and certifications under Section 702 of FISA."[73]

The FISC is located in Washington, D.C.[74] It is composed of eleven Senate-confirmed federal district court judges who are appointed to serve by the Chief Justice of the Supreme Court.[75] Therefore, all judges who preside over the FISC are Article III judges.[76] By statute, each judge serves a maximum term of seven years and all terms are staggered so that there is continuity on the Court.[77] FISC judges must be selected from at least seven of the United States judicial circuits, and three of the judges must live within 20 miles of Washington, D.C.[78] Typically, judges preside over the Court for one week at a time, on a rotating basis.[79] Each judge that sits on the FISC does so in addition to their regular caseload in their home federal district.[80]

---

[67] Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).
[68] *Id*.
[69] *Id*.
[70] OFFICE OF THE DIR. OF NAT'L INTEL., *The Foreign Intelligence Surveillance Court* (2023).
[71] *Id.*
[72] *Id*.
[73] *Id*.
[74] FISA CT., *About the Foreign Intelligence Surveillance Court* (last visited Aug. 28, 2023).
[75] *Id*.
[76] FISA CT., *Rules of Procedures* (Nov. 1, 2010) ("Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.").
[77] FISA CT., *About the Foreign Intelligence Surveillance Court* (last visited Aug. 28, 2023).
[78] *Id*.
[79] *Id*.
[80] OFFICE OF THE DIR. OF NAT'L INTEL., *The Foreign Intelligence Surveillance Court* (2023).

FISA Myths vs. FISA Realities

MYTH	REALITY
1. FISA will cease to exist if Section 702 expires.	1. Only Title VII, which includes Section 702, will expire on December 31, 2023.[81] Other titles of FISA will remain active.
2. If Section 702 expires, a different FISA provision or an alternative foreign intelligence authority, like Executive Order 12333, could replace Section 702.	2. Section 702 is the only legal authority within FISA that authorizes the U.S. government to collect foreign intelligence information on non-U.S. persons in this manner. Executive Order 12333 would not permit the type of surveillance conducted under Section 702.[82] There is no other authority currently available that could replicate Section 702's efficiency and effectiveness.[83]
3. Section 702 is unconstitutional.	3. Every federal court to review Section 702 has held that it is constitutional. Foreigners located abroad with no substantial connections to the United States are not entitled to Fourth Amendment protections.[84]

[81] Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).
[82] Adam Klein, *FISA 702 (2008-2023)*, LAWFARE (Dec. 27, 2022) ("There is no comparable substitute. 'Traditional' FISA, which requires lengthy applications to the secret FISA court, was used in fewer than 500 cases last year. Section 702, which doesn't require individual court orders, can cover orders of magnitude more targets: more than 230,000 in 2021. Even a small fraction of that volume would overwhelm the FISA court. Nor can overseas collection under Executive Order 12333 make up the difference. To be sure, Executive Order 12333 collection on these targets would be lawful; all of Section 702's targets are non-Americans overseas. The intelligence community's heavy use of the more constrained Section 702 suggests, however, that collecting data on home turf offers considerable advantages over collection abroad.").
[83] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702 of the Foreign Intelligence Surveillance Act* (2023).
[84] *See United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021) (affirming 187 F.Supp.3d 1240 (D. Colo. 2015)), *cert. denied*, 143 S. Ct. 246 (2022); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (affirming, in relevant part, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016)); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016)

4. Judges who preside over the FISC are "secret judges."	4. Judges who preside over the FISC are Article III judges who are Senate confirmed. They sit on the FISC in addition to having their regular caseloads in their home federal districts.[85]
5. Section 702 collects on all foreigners. Any foreigner you communicate with is subject to Section 702 collection.	5. Section 702 is a highly targeted collection program that only collects on foreigners who possess or communicate specific types of foreign intelligence information.[86] It is individualized and extremely limited.[87]
6. If a U.S. person communicates with a target of Section 702 collection, all of the U.S. person's emails are subject to collection and review by the IC.	6. If a U.S. person communicates with a target of Section 702 collection, only the specific correspondence in which the foreign target is a party is collected—this is referred to as "incidental collection."[88] The government can never target U.S. persons whose communications are incidentally collected under Section 702.[89]

(affirming 2014 WL 2866749 (D. Or. June 24, 2014)), *cert. denied*, 138 S. Ct. 636 (2018); *United States v. Mohammad*, 339 F. Supp. 3d 724 (N.D. Ohio 2018); *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. June 28, 2018) (ECF No. 115).

[85] 50 U.S.C. § 1803 ("The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance . . .").

[86] OFFICE OF THE DIR. OF NAT'L INTEL., *Targeting Under FISA Section 702* (2023).

[87] *Id*.

[88] OFFICE OF THE DIR. OF NAT'L INTEL., *Incidental Collection in a Targeted Intelligence Program* (2023) ("Incidental collection may involve innocuous contact with family or friends, or it may, for example, constitute foreign intelligence that must be shared to prevent harm. In the latter case, the incidental collection might be with a witting participant, an unwitting participant, or a potential victim.").

[89] *Id*.

7. Letting Section 702 expire would eliminate the tool under which Carter Page was surveilled.	7. Carter Page was surveilled under different authorities within FISA Title I and not under Section 702.[90]
8. Section 702 is used to target Americans.	8. Section 702 cannot be used to target Americans anywhere in the world or any person inside the United States regardless of nationality.[91] There are no exceptions to this.[92]
9. Section 702 permits "warrantless backdoor searches."	9. "Warrantless backdoor searches" are not permitted under Section 702. If a U.S. person's information is incidentally collected, it does not authorize the U.S. government to target that U.S. person under Section 702.[93]
10. A search using a U.S. person query term—such as an email address or a phone number associated with a U.S. person—acquires new information that the government did not previously have it its possession.	10. U.S. person queries are searches of information that has already been lawfully acquired.[94] It is similar to a police officer searching the license plate number of a driver pulled over for speeding.

[90] *See generally, Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, U.S. DEP'T OF JUSTICE OFFICE OF THE INSPECTOR GEN. (Dec. 2019).
[91] Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023) ("Section 702 may only be used to target non-U.S. persons who are reasonably believed to be outside the United States, for the purpose of obtaining foreign intelligence information").
[92] *Id*. ("Additionally, the government may not intentionally target any persons in the United States or U.S. persons who are abroad.").
[93] *Id*.
[94] OFFICE OF THE DIR. OF NAT'L INTEL., *FISA Section 702 Fact Sheet* (2023).

11. Section 702 is a mass surveillance program.	11. Section 702 is a targeted foreign intelligence program in which the targets are only "non-U.S. persons reasonably believed to be located outside the United States and expected to possess, communicate, or receive foreign intelligence information."[95]
12. The IC could just get a warrant before conducting a query using a U.S. person query term.	12. A warrant requirement would jeopardize the IC's ability to respond swiftly to urgent threats or to collect valuable foreign intelligence information.[96]

[95] OFFICE OF THE DIR. OF NAT'L INTEL., *Incidental Collection in a Targeted Intelligence Program* (2023).
[96] Stewart Baker & Michael Ellis, *The Left's FISA Reform Trap*, REAL CLEAR POLITICS (Sept. 20, 2023) ("The difference is that we haven't supported a warrant requirement, for several reasons: 1) Warrants wouldn't address the partisan abuses we've seen in recent years; 2) A warrant requirement defies decades of law and practice, and 3) Imposing one would cripple national security in a way reminiscent of our failures before 9/11.").

How the Intelligence Community Uses Section 702

Overview

Once an approved target for Section 702 collection has been identified, collection is initiated by the NSA.[97] The NSA accomplishes this by "provid[ing] specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification."[98] Once approved, those identifiers are used to determine which communications to collect.[99] Electronic service providers are then compelled to assist the NSA in acquiring the communications associated with those identifiers.[100]

Section 702's "targeting procedures" only permits targeting of non-U.S. persons located outside the United States, who are in possession of foreign intelligence information.[101] The NSA disseminates the Section 702 collection to the agency with jurisdiction for querying—either the CIA, FBI, NCTC, or itself.[102] This information is disseminated in the form of raw data (*i.e.*, emails, telephone calls, etc.), which is referred to as "unminimized" collection.[103]

Every single query is required to follow the "query standard."[104] The query standard for each agency is:

- CIA – Reasonably likely to retrieve foreign intelligence information[105]
- NSA – Reasonably likely to retrieve foreign intelligence information[106]
- NCTC – Reasonably likely to retrieve foreign intelligence information[107]
- FBI only — Reasonably likely to retrieve foreign intelligence information and/or evidence of a crime[108]

The query standard has three requirements: "(1) every query must have an authorized purpose, (2) every query must be reasonably designed in light of that purpose (*e.g.*, the query terms may not be overbroad, but instead must be tailored to that authorized purpose), and (3) IC personnel must have a specific factual basis to believe that the query is reasonably likely to

[97] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702 Overview* (2023).
[98] NAT'L SEC. AGENCY, *Signals Intelligence: Foreign Intelligence Surveillance Act of 1978* (last visited Sept. 11, 2023).
[99] *Id*.
[100] *Id*.
[101] 50 U.S.C. § 1881a; *see also* Matthew Olsen, Assistant Att'y Gen. for Nat'l Sec., U.S. DEP'T OF JUSTICE, *NSA's Section 702 Targeting Procedures* (Mar. 13, 2023); Matthew Olsen, Assistant Att'y Gen. for Nat'l Sec., U.S. DEP'T OF JUSTICE, *FBI's Section 702 Targeting Procedures* (Mar. 13, 2023).
[102] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702 Overview* (2023).
[103] OFFICE OF THE DIR. OF NAT'L INTEL., *Finding the Foreign Intelligence Information* (2023).
[104] *Id*.
[105] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *CIA's Section 702 Querying Procedures* (Mar. 13, 2023).
[106] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *NSA's Section 702 Querying Procedures* (Mar. 13, 2023).
[107] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *NCTC's Section 702 Querying Procedures* (Mar. 13, 2023).
[108] William Barr, Att'y Gen., U.S. DEP'T OF JUSTICE, *FBI's Section 702 Querying Procedures* (Mar. 13, 2023).

retrieve foreign intelligence information or (again, only in the case of FBI) evidence of a crime."[109]

Procedures to Protect U.S. Persons

Section 702 only targets non-U.S. persons who are reasonably believed to be outside of the United States.[110] However, these non-U.S. persons may be in contact with U.S. citizens, and any communications between the U.S. person and the non-U.S. person may be "incidentally" collected.[111] Only the individual communication between said U.S. person and said non-U.S. person is collected under Section 702. For example, only an email sent from a U.S. citizen to a foreign target in Syria is collected, not the entirety of the U.S. person's email account.

Section 702 is a targeted collection program.[112] As such, not all foreigners are targets of Section 702 information.[113] Only a small number of Americans are in contact with specific foreigners in possession of or communicating the type of foreign intelligence information that warrants targeting under Section 702.[114] According to the ODNI:

> To put the likelihood of obtaining U.S. person communications in perspective, the world's population is approximately 7.5 billion and there are over 3 billion internet users worldwide. In 2016, the IC had approximately 106,469 targets authorized for collection under Section 702, which is approximately .004% of the world's internet users and .001% of the world's population. Targeting under Section 702 is individualized and focused only on specific foreigners who are assessed to have foreign intelligence information. It is very unlikely that the average U.S. person would be in contact with a foreigner who falls within the limited and select group of individuals targeted under Section 702.[115]

Under Section 702, the IC is required to apply minimization procedures to limit the retention and reporting of information related to U.S. persons.[116] As a result, most U.S. person

---

[109] *Id*.
[110] 50 U.S.C. 1881a ("An acquisition authorized under subsection (a)—(1) may not intentionally target any person known at the time of acquisition to be located in the United States; (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; (3) may not intentionally target a United States person reasonably believed to be located outside the United States; (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; (5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and (6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.").
[111] OFFICE OF THE DIR. OF NAT'L INTEL., *Incidental Collection in a Targeted Intelligence Program* (2023).
[112] OFFICE OF THE DIR. OF NAT'L INTEL., *Section 702 Overview* (2023).
[113] *Id*.
[114] *Id*.
[115] OFFICE OF THE DIR. OF NAT'L INTEL, *When Is It Permissible to Identity an American in an Intelligence Report?* (2023).
[116] *Id*.

information acquired under Section 702 is excluded from intelligence reporting.[117] After a certain period of time, the IC is required to delete any unminimized Section 702 information, regardless of the nationality of the individuals from which it was collected.[118]

In general, "for non-public information concerning an unconsenting U.S. person, agencies may only include the identity of the U.S. person if it itself constitutes foreign intelligence, is necessary for the recipient to understand the foreign intelligence being transmitted, or is evidence of a crime."[119] When it is deemed necessary to refer to a U.S. person in an intelligence report, an agency's minimization procedures generally require it protect that individual's privacy by "masking" their identity.[120] Masking occurs when the identity of a U.S. person is replaced with a generic phrase such as "U.S. person 1" or "named U.S. person #1."[121]

FISA's targeting, querying, and minimization procedures are built-in safeguards designed to protect the constitutional rights of U.S. persons. A robust compliance and oversight framework involving all three branches of government—the legislative, the executive, and the judiciary (via the FISC)—ensures that each agency with access to FISA adheres to such statutorily required procedures.[122]

---

[117] *Id*.
[118] OFFICE OF THE DIR. OF NAT'L INTEL, *Section 702 Overview* (2023).
[119] OFFICE OF CIVIL LIBERTIES, PRIVACY, & TRANSPARENCY, OFFICE OF THE DIR. OF NAT'L INTEL, *Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act* (Nov. 2017).
[120] OFFICE OF THE DIR. OF NAT'L INTEL., *When Is It Permissible to Identity an American in an Intelligence Report?* (2023).
[121] *Id*.
[122] OFFICE OF CIVIL LIBERTIES, PRIVACY, AND TRANSPARENCY, OFFICE OF THE DIR. OF NAT'L INTEL., *Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act* (Nov. 2017) ("The IC's use of FISA is subject to robust oversight regime that begins with each agencies' internal oversight offices (*e.g*., compliance, legal, civil liberties and privacy, and inspector generals), continues with oversight by the DOJ, and extends to outside the executive branch with oversight by the FISC and Congress. Significantly, both the FISC and Congress are notified of every identified compliance incident. For example, as required by FISA, Congress is kept fully informed of IC's implementation of FISA Titles I and III and Section 702 authorities through semiannual reports and through copies of FISC opinions that relate to significant interpretations of law. Additionally, certain formal entities, like the Privacy and Civil Liberties Oversight Board (PCLOB), may choose to further examine and make recommendations regarding FISA (regardless of the FISA provision) as it pertains to counterterrorism matters. The following describes the compliance and oversight of Section 702 collection.").

Recent FBI Abuses

In the past, the DOJ OIG has noted the FBI "fell far short" of compliance with FISA.[123] These shortcomings have continued. In May 2023, the IC made publicly available an April 2022 FISC Memorandum Opinion and Order (Order) detailing "significant" querying violations by the FBI.[124] Most of these violations occurred before the FBI implemented corrective reforms to its querying procedures.[125] In one incident, an FBI analyst conducted a batch query of over 19,000 donors to a congressional campaign, after the analyst believed "the campaign was a target of foreign influence."[126] However, the DOJ National Security Division (NSD), who conducted an audit, found that "only eight identifiers used in the query had sufficient ties to foreign influence activities to comply with the querying standard."[127]

Prior to 2022, most of the FBI's compliance failures appear to have been caused by a culture at the FBI where searches of FISA databases were done with impunity by poorly trained agents and analysts with easy access to a database that was in dire need of better safeguarding. For example, prior to reforms made in 2021, FBI systems for storing raw Section 702 information did not require personnel to affirmatively "opt-in" to query that information, leading to many inadvertent, noncompliant queries of Section 702 data.[128] Now, FBI personnel are required to affirmatively "opt-in" before they query the Section 702 database.[129] It also seems that FBI management failed to take query compliance incidents seriously and were slow to implement reforms that would have addressed many of the problems. However, the FBI has realized the depth and breadth of its issues, thanks in part to stringent oversight by Congress and the FISC. The FBI has implemented a series of recent revisions to its querying procedures, to include systems modifications and heightened oversight.[130]

In its April 2022 Order, the FISC was "encouraged" by "the amendments to the FBI's querying procedures and the substantial efforts to improve FBI querying practices, including heightened documentation requirements, several systems changes, and enhanced guidance, training, and oversight measures."[131] The Court noted that preliminary indications showed "that

---

[123] *Hearing Before the H. Comm. on the Judiciary: Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them*, 118th Cong. (2023) (statement of Michael Horowitz, Inspector Gen., U.S. Dep't of Justice, "Our review of the Department's applications to authorize FISA surveillance of Carter Page found that FBI personnel fell far short of the requirement in FBI policy that they ensure that all factual statements in a FISA application are 'scrupulously accurate.' We identified multiple instances in which factual assertions relied upon by the FISC in the FISA applications were inaccurate, incomplete, or unsupported by appropriate documentation, based upon information the FBI had in its possession at the time the applications were filed.").
[124] FISA CT. *re* Section 702 2021 Certification (Apr. 21, 2022), at 26.
[125] *Id*.
[126] *Id*. at 29.
[127] *Id*.
[128] Press Release, *FBI Releases FISA Query Guidance*, FED. BUREAU OF INVESTIGATION (Apr. 24, 2023).
[129] *Id*.
[130] U.S. DEP'T OF JUSTICE, *Recent Efforts to Strengthen FISA Compliance* (Feb. 28, 2023).
[131] FISA CT. *re* Section 702 2021 Certification (Apr. 21, 2022), at 49.

some of these measures are having the desired effect."[132] The Court issued a warning and offered a potential reform solution—one that Congress is currently considering—when it wrote:

> Nonetheless, compliance problems with the FBI's querying of Section 702 information have proven to be persistent and widespread. If they are not substantially mitigated by these recent measures, it may become necessary to consider other responses, such as substantially limiting the number of FBI personnel with access to unminimized Section 702 information.[133]

Crossfire Hurricane and Carter Page

FISA abuses are not limited to Section 702, which is why this reauthorization presents Congress with the special opportunity to reform other areas of FISA. Title I of FISA, a different legal authority than Section 702, has also been the victim of significant abuse. In July 2016, the FBI launched Crossfire Hurricane, a codename for a counterintelligence operation aimed at investigating purported links between Donald Trump's presidential campaign and Russian government officials.[134] Soon after opening Crossfire Hurricane, the FBI opened full investigations on four individuals affiliated with the Trump Campaign: George Papadopoulos, Carter Page, Paul Manafort, and Michael Flynn.[135]

In addition to opening full investigations on Trump campaign members, the FBI sought FISA applications on Page and Papadopoulos.[136] The FBI was unsuccessful in its attempt to use FISA authorities against Papadopoulos, and initially was similarly unsuccessful in its attempt to do the same against Page.[137] However, once Crossfire Hurricane investigators obtained the Steele Dossier, a collective of unverified reports paid for by Hillary Clinton's campaign and the Democratic National Committee and produced by Christopher Steele, the efforts to seek a FISA application against Page were successful.[138]

Two independent investigations by the Department of Justice (DOJ) Office of Inspector (OIG) General Michael Horowitz and Special Counsel John Durham found abuses by the FBI in the opening and subsequent investigation of Crossfire Hurricane.[139] In particular, the DOJ OIG found "so many basic and fundamental errors," including "at least 17 significant errors or omissions" in the Carter Page FISA applications.[140]

---

[132] *Id*.
[133] *Id*.
[134] Durham Report, at 10.
[135] *Id*. at 17.
[136] *Id*.
[137] *Id*. at 11.
[138] *Id*.
[139] *See generally,* Horowitz Report and Durham Report.
[140] Horowitz Report, at vii-xii.

Special Counsel John Durham similarly found "unsettling" behavior by FBI Crossfire Hurricane investigators regarding the Page FISA applications.[141] Durham concluded:

> Based on the review of Crossfire Hurricane and related intelligence activities, we conclude that the Department and the FBI failed to uphold their important mission of strict fidelity to the law in connection with certain events and activities described in this report. As noted, former FBI attorney Kevin Clinesmith committed a criminal offense by fabricating language in an email that was material to the FBI obtaining a FISA surveillance order. In other instances, FBI personnel working on that same FISA application displayed, at best, a cavalier attitude towards accuracy and completeness. FBI personnel also repeatedly disregarded important requirements when they continued to seek renewals of that FISA surveillance while acknowledging - both then and in hindsight - that they did not genuinely believe there was probable cause to believe that the target was knowingly engaged in clandestine intelligence activities on behalf of a foreign power, or knowingly helping another person in such activities. And certain personnel disregarded significant exculpatory information that should have prompted investigative restraint and re-examination.
>
> Our investigation also revealed that senior FBI personnel displayed a serious lack of analytical rigor towards the information that they received, especially information received from politically affiliated persons and entities. This information in part triggered and sustained Crossfire Hurricane and contributed to the subsequent need for Special Counsel Mueller's investigation. In particular, there was significant reliance on investigative leads provided or funded (directly or indirectly) by Trump's political opponents. The Department did not adequately examine or question these materials and the motivations of those providing them, even when at about the same time the Director of the FBI and others learned of significant and potentially contrary intelligence.[142]

The Durham Report did not recommend any wholesale changes to the guidelines and policies that the Department and the FBI currently have in place.[143] Rather, Durham highlighted that it is incumbent on the FBI to properly follow existing guidelines, policies, and laws. Durham wrote:

> [T]he answer is not the creation of new rules but a renewed fidelity to the old. The promulgation of additional rules and regulations to be learned in yet more training sessions would likely prove to be a fruitless exercise if the FBI's guiding principles of "Fidelity, Bravery and Integrity" are not engrained in the hearts and

[141] Durham Report, at 219 ("Later that day, however, in the second meeting between CHS-I and Papadopoulos, there was an explicit discussion about the allegation which predicated the opening of the Crossfire Hurricane investigation. The Crossfire Hurricane investigative team's interpretation of that conversation, as included in the initial and subsequent Page FISA applications, is unsettling.").
[142] *Id*. at 17-8.
[143] *Id*. at 18.

minds of those sworn to meet the FBI' s mission of "Protect[ing] the American People and Uphold[ing] the Constitution of the United States."[144]

There was only one specific FBI reform that Durham recommended. Durham suggested that "one possible way to provide additional scrutiny of politically sensitive investigations would be to identify, in advance, an official who is responsible for challenging the steps taken in the investigation."[145] He noted that former NSA General Counsel Stewart Baker has proposed having a "career position for a nonpartisan FBI agent or lawyer to challenge the FISA application and every other stage of the investigation" in investigations that "pose partisan risk."[146] Durham recommended that the Department "seriously consider" Baker's proposal.[147]

Recent FBI Reforms

Over the last few years, the FBI has implemented a series of reforms to address FISA abuses. In response to the 17 "significant errors and omissions" identified by OIG Horowitz in the Title I applications against Carter Page, the FBI issued the following corrective actions:

- New FISA Request and Verification Requirements – In February 2020, it became mandatory for FBI personnel seeking to collect information under FISA to use updated versions of two important forms—the FISA Request Form, which FBI personnel use to initiate the process of developing a FISA application in coordination with DOJ attorneys, and the FISA Verification Form (or "Woods Form"), which serves to ensure documentation for FISA applications is complete and accurate.
    - Changes in these forms ensure agents identify any information that might undermine probable cause, and provide all material information about the reliability of sources, assets, or contacts in the FISA application—even sources operated by other U.S. or foreign government agencies.
- Accuracy Guidance – In July 2021, the FBI and DOJ revised their joint accuracy policy, incorporating OIG recommendations to ensure adequate procedures are in place for DOJ to obtain all relevant and accurate information during the drafting of any FISA application.
- Field Agents as Affiants – The accuracy and completeness of FISA applications are now attested to by a field agent and field supervisor knowledgeable of the investigation, rather than the previous process, which required a FBI Headquarters (HQ) program manager to do so.

[144] *Id*. at 18-9.
[145] *Id*. at 306.
[146] *Id*.
[147] *Id*.

- FBI attorneys are required to confirm that the application satisfies the necessary requirements of the FISA statute to obtain the requested authority.

- Senior FBI executives also have to confirm that they have read the application and reach the same conclusion.

- Supervisory Review – An FBI field supervisor must review each factual assertion and its corresponding documentation in the Woods File, and then attest that all information that might reasonably call into question the accuracy of such information has been provided to the DOJ attorneys working on the FISA application.

- Standardized Recordkeeping – All supporting documentation for FISA applications, commonly referred to as "Woods Files," must now be maintained in FBI's electronic case file system, unless otherwise prohibited (*e.g.*, documents are at a higher classification level). Separate files are now required for each initiation, amendment, or renewal application.

- Additional DOJ Oversight – Existing internal legal review requirements were expanded and strengthened, with new "completeness" reviews by DOJ attorneys to supplement the existing "accuracy" reviews they conducted of FISA application files.

- New Internal Oversight Mechanism – In 2020, at the Direction of then-Attorney General Bill Barr, FBI created a new Office of Internal Auditing, which focuses on auditing the FBI's use of its FISA authorities and recommending reforms on an ongoing basis.

- New Limitations on HQ-Run Investigations – Except in extraordinary circumstances, FBI policy now requires that investigations must be run out of field offices, not FBI HQ.

- Confidential Human Source (CHS) Program Improvements – Updated AG Guidelines on assessing and validating CHSs allow the FBI to promptly identify high-risk sources and address concerns earlier than ever.

- Improved CHS Verifications – FBI personnel seeking to collect information under FISA must provide DOJ attorneys with relevant information about CHS bias, motivation, reliability, and reporting for every application.

    - All CHS information must be re-confirmed at the time the FISA Verification Form is completed.

- Training – Recurring mandatory trainings were added for all personnel who work FISA or CHS matters, to include trainings focused specifically on FISA Rigor and

lessons learned from the OIG and other reviews, as well as training tailored specifically to personnel who work on FISA applications.

- Defensive Briefings – The FBI instituted procedures concerning defensive briefings for individuals – such as legislative and executive branch officials who may be targets of foreign powers – and established the Foreign Influence Defensive Briefing Board to standardize the process for determining when and how to deliver defensive briefings.

- Sensitive Investigations – In February 2020, then-Attorney General Barr announced new requirements for opening certain sensitive investigations, and the FBI conducted a review of its existing sensitive investigative matters (SIM) policies and procedures in response to the Attorney General's direction.[148]

The FBI has also made reforms to target Section 702 abuses. The FBI's U.S. person queries of Section 702 data dropped over 93% from 2021 to 2022, after the FBI implemented some of these reforms.[149] According to the DOJ, recent efforts to improve compliance with Section 702 include:

- Requiring FBI Personnel to "Opt-In" to Query Unminimized Section 702 Information – In June 2021, the FBI changed the default settings in the systems where it stores unminimized Section 702 information so that FBI personnel with access to unminimized FISA Section 702 information need to affirmatively "opt-in" to querying such information. This system change was designed to address the large number of inadvertent queries of unminimized Section 702 information DOJ had identified in its reviews, in which FBI personnel did not realize their queries would run against such collection. Historically, users were automatically opted-in to querying unminimized Section 702 information in these databases if they had been authorized to access unminimized Section 702 information.[150]

- Ensuring Heightened Approvals on Large Batch Job FISA Queries – Also in June 2021, the FBI instituted a policy requiring FBI attorney approval prior to conducting a "batch job" that would result in 100 or more queries. The term "batch job" refers to a capability in one of the FBI's systems that allows FBI personnel to more efficiently run queries involving large numbers of query terms. Historically, there had been some compliance incidents with the use of this tool that involved a large number of queries. The FBI attorney pre-approval requirement is designed to ensure that there is additional review in situations where one incorrect decision could potentially have a greater privacy impact due to the large number of query terms.[151] In June 2023, the House and Senate Intelligence and Judiciary Committees received notice that the FBI intends to require attorney pre-approval for all batch job queries—not just those that would

[148] FED. BUREAU OF INVESTIGATION, *Fact Sheet: FBI Post-Crossfire Hurricane Reforms* (September 2023).
[149] OFFICE OF THE DIR. OF NAT'L INTEL., *FISA Section 702 Fact Sheet* (2023).
[150] U.S. DEP'T OF JUSTICE, *Recent Efforts to Strengthen FISA Compliance* (Feb. 28, 2023).
[151] *Id*.

result in 100 or more queries.[152] At the time, FBI IT professionals were working to redesign the user interface to accommodate this reform.[153]

- Supplemental Guidance and Mandatory Training on Query Requirements – In November 2021, DOJ, ODNI, and the FBI issued new comprehensive guidance to all FBI FISA users on the proper application of the query rules, and in December 2021, the FBI instituted new mandatory training on that guidance, which personnel were required to complete by the end of January 2022. The FBI expanded and updated this training at the end of 2022. On an annual basis, all FBI personnel with access to unminimized FISA information are required to complete the expanded and updated query training or lose access to FISA systems. The guidance and mandatory training directly address misunderstandings about the rules applicable to queries of unminimized FISA information and instruct personnel on how to properly apply the query rules. In addition, the text of FBI's Section 702 querying procedures was revised to more clearly spell out the query standard to FBI personnel.[154]

- Requirement for Case-Specific Justifications for U.S. Person Query Terms in FBI Systems – In the fall of 2021, at the direction of the FISC, the FBI modified its systems containing unminimized Section 702 information to require a case-specific justification for every query using a U.S. person query term before accessing any content retrieved by such a query from unminimized Section 702 information. Previously, personnel were permitted to use a pre-populated common justification, when applicable, for the query. These case-specific justifications are subject to review and audit by DOJ as part of its regular oversight reviews.[155]

- New Restrictions and Oversight of Sensitive Queries – In March 2022, the FBI instituted a new policy requiring enhanced pre-approval requirements for certain "sensitive" queries, such as those involving elected officials, members of the media, members of academia, or religious figures. Under the new policy, an FBI attorney must review these queries before they are conducted. The FBI's Deputy Director must also personally approve certain queries before they can be conducted. This measure was designed to ensure that there is additional review at a leadership level of queries that reflect particular investigative sensitivities.[156]

In June 2023, the FBI notified Committees of jurisdiction—the House and Senate Intelligence and Judiciary Committees—of new internal procedures titled, "FBI FISA Query Accountability Procedures, Field Office Health Measure, and Other Upcoming FBI FISA

[152] Congressional Notice, *(U) FBI FISA Query Accountability Procedures, Field Office Health Measure, and other upcoming FBI FISA reforms*, FED. BUREAU OF INVESTIGATION (June 12, 2023) (on file with Committee staff).
[153] *Id*.
[154] *Id*.
[155] *Id*.
[156] U.S. DEP'T OF JUSTICE, *Recent Efforts to Strengthen FISA Compliance* (Feb. 28, 2023).

Reforms," issued to its workforce.[157] This new procedure addresses FBI query incidents involving intentional misconduct, reckless behavior, and negligence.[158] Regarding intentional misconduct and reckless behavior, it clarified the existing requirements for referring such incidents to the FBI's Inspection Division for investigation and disciplinary action by the FBI's Office of Professional Responsibility.[159]

Regarding incidents involving negligence, it establishes a new policy with escalating consequences, as well as a centralized ability to track an individual employee's history of performance incidents:

> An initial incident would trigger immediate suspension of FISA access while employee: (1) retakes all mandatory FISA training, (2) executes a signed certification that will be placed in the employee's personnel files, and (3) receives mandatory one-on-one counseling with their field office attorney. Subsequent incidents within a 24-month period would require further measures, up to and including indefinite loss of FISA access, reassignment to a new role, and/or referral to FBI's Inspection Division to review potentially reckless conduct.[160]

The revised internal procedures also include a new FISA Compliance "Field Office Health Measure," which will require Field Office Executive Leadership (*i.e.*, Special Agents in Charge and Assistant Directors in Charge) to be evaluated on a series of health measures for their field offices—including FISA compliance—that will affect eligibility for promotion and annual bonuses.[161] Field office heads are required to monitor compliance by convening at least two semiannual meetings to assess personnel performance in a number of FISA compliance areas.[162]

---

[157] Congressional Notice, *(U) FBI FISA Query Accountability Procedures, Field Office Health Measure, and other upcoming FBI FISA reforms*, FED. BUREAU OF INVESTIGATION (June 12, 2023) (on file with Committee staff); *see also* Press Release, FED. BUREAU OF INVESTIGATION, *FBI Deputy Director Highlights Bureau's New FISA Query Accountability Procedures* (June 13, 2023).
[158] *Id*.
[159] *Id*.
[160] *Id*.
[161] *Id*.
[162] *Id*.

Examples of Section 702 Successes

Overview

Missions involving Section 702 use are generally highly classified given their sensitive nature. The Office of the Director of National Intelligence has declassified the following examples of Section 702-acquired information aiding national security interests:

- Section 702 has identified threats to U.S. troops and disrupted planned terrorist attacks at home and abroad, and contributed to the successful operation against Ayman al-Zawahiri in 2022.

- Section 702-acquired information [has] informed the U.S. Government's understanding of the Chinese origins of a chemical used to synthesize fentanyl; foreign actors' illicit plans to smuggle methamphetamine across the U.S. border; the quantities and potency of drugs, including fentanyl, destined for illegal transfer to the United States, as well as specific smuggling techniques used to avoid detection; and a foreign narcotics trafficker's purchase of a vast quantity of pills for transfer to the United States.

- Section 702 has helped uncover gruesome atrocities committed by Russia in Ukraine—including the murder of noncombatants and the forced relocation of children from Russian-occupied Ukraine to the Russian Federation—and the detention of refugees fleeing violence by Russian personnel.

- Section 702-acquired information has been used to identify multiple foreign ransomware attacks on U.S. critical infrastructure. This intelligence positioned the U.S. Government to respond to and mitigate these events, and in some instances prevent significant attacks on U.S. networks.

- Section 702-acquired information related to sanctioned foreign adversaries was used in U.S. Government efforts to stop weapons of mass destruction components from reaching foreign actors.

- Section 702 has resulted in the identification and disruption of hostile foreign actors' attempts to recruit spies in the United States or send their operatives to the United States.

- Section 702 has identified key economic security risks, including strategic malign investment by foreign actors in certain U.S. companies.[163]

[163] OFFICE OF THE DIR. OF NAT'L INTEL., *FISA Section 702 Fact Sheet* (2023).

FISA in the Fight Against Fentanyl

"Fentanyl is the single deadliest drug threat our nation has ever encountered," warned Drug Enforcement Administration (DEA) Administrator Anne Milgram in 2022.[164] Its threat is pervasive, found everywhere from small towns to major cities, and killing everyone from babies to the elderly.[165] The CDC estimates that in 2022 nearly 110,000 deaths in the United States were attributable to drug overdose, two-thirds of which involved synthetic opioids like fentanyl.[166] Over 150 people die from overdoses from drugs like fentanyl every day in the United States.[167] In 2022, the DEA seized more than 379 million deadly doses of fentanyl—enough to kill every single American.[168]

Section 702 is a vital tool in combating the flow of fentanyl across southern border and other ports of entry into United States.[169] The majority of the chemicals used to create fentanyl come from China.[170] Information acquired under Section 702 has revealed critical intelligence connecting at least one foreign government official to the trade.[171] Section 702 also provides actionable intelligence that authorities can use to swiftly disrupt specific transfer attempts of fentanyl chemical precursors and pills into the United States.[172] For example, Section 702 has allowed U.S. intelligence agencies to warn commercial shipping companies that smugglers are using their freight to conceal illicit chemical loads.[173] Section 702 has also proven critical in the recruitment of foreigners abroad to collect intelligence for the United States by infiltrating smuggling organizations, allowing U.S. intelligence and law enforcement officials greater insight into the plans and tactics of drug smugglers.[174]

What makes Section 702 uniquely effective in combating the drug trade is that it allows foreign communications to be monitored in real-time, giving intelligence and law enforcement officials the information they need to keep pace with the fast moving, complex nature of

---

[164] Press Release, DRUG ENFORCEMENT ADMIN., *DEA Recognizes National Fentanyl Prevention Awareness Day* (Aug. 19, 2022).
[165] *Id*.; Aliza Chasan, *Baby Boy Dies in Florida After Teen Mother Puts Fentanyl in Baby Bottle, Sheriff Says*, CBS NEWS (July 12, 2023).
[166] CTRS. FOR DISEASE CONTROL & PREVENTION, *Provisional Drug Overdose Death Counts* (2023).
[167] CTRS. FOR DISEASE CONTROL & PREVENTION, *Fentanyl Facts* (2023).
[168] Press Release, DRUG ENFORCEMENT ADMIN., *Drug Enforcement Administration Announces the Seizure of Over 379 Million Deadly Doses of Fentanyl in 2022* (Dec. 20, 2022).
[169] Michael Wilner, *Spy Agencies Battling the Fentanyl Crisis Fear Their Most Powerful Weapon Is at Risk*, HAWAII TRIB. HERALD (Sept. 12, 2023).
[170] DRUG ENFORCEMENT ADMIN., *DEA Intelligence Report: Fentanyl Flow to the United States* (January 2020) ("Currently, China remains the primary source of fentanyl and fentanyl-related substances trafficked through international mail and express consignment operations environment, as well as the main source for all fentanyl-related substances trafficked into the United States.").
[171] Michael Wilner, *Spy Agencies Battling the Fentanyl Crisis Fear Their Most Powerful Weapon Is at Risk*, HAWAII TRIB. HERALD (Sept. 12, 2023).
[172] *Id*.; THE WHITE HOUSE, *President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations for Reauthorization* (July 2023) ("Examples of Section 702 successes abound: [. . .] enabling the seizure of numerous fentanyl pills, powder, precursor chemicals, and production equipment.").
[173] *Id*.
[174] *Id*.

international drug trafficking and quickly interdict drug shipments into the United States.[175] As one intelligence official stated, "702 is really the only source of information that allows us to stay dynamic in thwarting the threat. If we were to lose it, it would make us blind."[176]

FISA Preventing al-Qaeda and ISIS Attacks

Section 702 has been a powerful weapon against terror attacks, particularly those perpetuated by al-Qaeda and the Islamic State of Iraq and Syria (ISIS). Some of Section 702's success in fighting the war on terror include:

1. Ayman al-Zawahiri – Zawahiri was the mastermind behind many of the most atrocious terror attacks against Americans to date, including: the attacks that killed nearly 3,000 Americans on 9/11, the attack on the USS Cole in Yemen that killed 17 sailors in 2000, and attacks on U.S. embassies in Tanzania and Kenya that killed 224 people in 1998.[177] Following Osama bin Laden's death in May 2011, Zawahiri became the leader of al-Qaeda.[178] In this position, he coordinated al-Qaeda activities around the world, including setting priorities and providing operational guidance.[179] In July 2022, Section 702 played a critical role in the strike that killed Zawahiri.[180] Information acquired under Section 702 led IC officials to discover that Zawahiri was living in a safehouse in downtown Kabul.[181] Using this information, Zawahiri was killed by a targeted Hellfire missile strike in said safehouse in July 2022.[182]

2. Najibullah Zazi – Zazi and a group of accomplices had imminent plans to detonate explosives in coordinated attacks on New York City subway lines during rush hour in September 2009.[183] He had previously received weapons and explosives training at an al-Qaeda training camp in Pakistan.[184] Section 702 collection against an email address used by a member of al-Qaeda in Pakistan uncovered an email sent from Zazi requesting urgent advice on how to make explosives.[185] Intelligence officials investigated further and discovered the full scale and scope of the attack.[186] Because of information acquired under Section 702, the attack was prevented and Zazi and his co-conspirators were

---

[175] *Id*.
[176] *Id*.
[177] Press Release, U.S. DEP'T OF DEFENSE, *U.S. Drone Strike Kills al-Qaida Leader in Kabul* (Aug. 2, 2022).
[178] *Id*.
[179] *Id*.
[180] *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary* 118th Cong. (2023) (joint statement of David Cohen, Deputy Dir., Cent. Intel. Agency, George Barnes, Deputy Dir., Nat'l Sec. Agency, Chris Fonzone, Gen. Counsel, Office of the Dir. of Nat'l Intel., Paul Abbate, Deputy Dir., Fed. Bureau of Investigation, and Matt Olsen, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Justice).
[181] *Id*.
[182] Press Release, U.S. DEP'T OF DEFENSE, *U.S. Drone Strike Kills al-Qaida Leader in Kabul* (Aug. 2, 2022).
[183] OFFICE OF THE DIR. OF NAT'L INTEL., *Guide to Section 702 Value Examples* (Oct. 2017).
[184] William K. Rashbaum & Karen Zraick, *Government Says Al Qaeda Ordered N.Y. Plot*, N.Y. TIMES (Apr. 23, 2010).
[185] OFFICE OF THE DIR. OF NAT'L INTEL., *Guide to Section 702 Value Examples* (Oct. 2017).
[186] *Id*.

arrested for their roles in the planned attack.[187] Later, U.S. government officials would determine that Saleh al-Somali, al-Qaeda's head of external operations, and Rashid Rauf, an al-Qaeda operative, ordered the attack.[188] Both were later killed in U.S. drone attacks.[189]

3. Hajji Iman – By 2015, Iman became the second in command of the ISIS, a role in which he coordinated operations with ISIS fighters across Syria and Iraq.[190] The ODNI reported that, "During Hajji Iman's tenure as a senior ISIS leader, ISIS issued multiple public calls for attacks against U.S. and Western interests around the world. ISIS members and sympathizers responded by planning or conducting numerous attacks."[191] Using Section 702, the NSA collected foreign intelligence information about the activities of Iman and his associates, including their location.[192] With this information, U.S. Special Forces launched a raid to apprehend Iman in Syria in 2016.[193] When shots were fired as U.S. forces, they returned fire, killing Iman and several other associates.[194]

4. Shawn Parson – In October 2013, the FBI began investigating Shawn Parson, a foreign person from Trinidad and Tobago, after he posted a series of comments online expressing his desire to commit terror attacks against Western interests.[195] In November 2014, Parson traveled from Trinidad and Tobago to Syria, where he continued to spread terrorist propaganda.[196] Using Section 702, the FBI discovered Parson was a prominent figure of an especially prolific ISIS network.[197] In particular, this ISIS network was known for identifying American military members and posting their names and addresses online, instructing their followers to "kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking they are safe.[198]" Parson, a native English speaker, appeared in an ISIS recruiting video and personally encouraged his followers to attack U.S. military bases in Colorado and Ohio, as well as "soft targets" in New York City, Chicago, and Los Angeles.[199] Section 702 not only revealed Parson's own terrorist propaganda, but also the identities and rhetoric of his fellow ISIS associates and supporters.[200] This information was shared with international partners, possibly preventing attacks in their countries.[201] Parson was killed in Syria in September 2015.[202]

---

[187] *Id*.
[188] William K. Rashbaum & Karen Zraick, *Government Says Al Qaeda Ordered N.Y. Plot*, N.Y. TIMES (Apr. 23, 2010).
[189] *Id*.
[190] OFFICE OF THE DIR. OF NAT'L INTEL., *To Catch a Terrorist* (2023).
[191] *Id*.
[192] OFFICE OF THE DIR. OF NAT'L INTEL., *Guide to Section 702 Value Examples* (Oct. 2017).
[193] *Id*.
[194] *Id*.
[195] *Id*.
[196] *Id*.
[197] *Id*.
[198] *Id*.
[199] *Id*.
[200] *Id*.
[201] *Id*.
[202] *Id*.

Section 702 has been "tremendously effective" in the fight against terror.[203] It gives IC and law enforcement officials the ability to monitor the purveyors of propaganda in real-time and intercept terror plots before they can become terror attacks.[204] Section 702 is the difference between preventing an attack and investigating it after the fact.

[203] *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities: Hearing Before the S. Comm. on the Judiciary* 118th Cong. (2023) (joint statement of David Cohen, Deputy Dir., Cent. Intel. Agency, George Barnes, Deputy Dir., Nat'l Sec. Agency, Chris Fonzone, Gen. Counsel, Office of the Dir. of Nat'l Intel., Paul Abbate, Deputy Dir., Fed. Bureau of Investigation, and Matt Olsen, Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Justice).
[204] *See generally*, OFFICE OF THE DIR. OF NAT'L INTEL., *Guide to Section 702 Value Examples* (Oct. 2017).

House Intelligence and House Judiciary Joint Majority FISA Working Group

HPSCI and the House Judiciary Committee (HJC) share jurisdiction of FISA. At the direction of House Speaker Kevin McCarthy (CA-20), HPSCI and HJC formed a FISA Joint Working Group to consider reform proposals. HPSCI Chairman Michael Turner (OH-10) and HJC Chairman Jim Jordan (OH-4) assigned members of their respective committees to form the Joint Working Group.

HPSCI's representatives are Darin LaHood (IL-16), Brian Fitzpatrick (PA-1), and Chris Stewart (UT-2).[205] HJC's representatives are Andy Biggs (AZ-5), Tom McClintock (CA-5), and Laurel Lee (FL-15). Congressman LaHood served as Chair of the Joint Working Group. The Joint Working Group met formally on the following dates: July 13; July 20; August 14; September 13; and November 3, in addition to a series of informal calls and meetings between Members.

The Joint Working Group's goal was to reach a consensus on the varied issues with FISA and necessary reforms. Committee representatives agreed that FISA 702 reauthorization presented an opportunity to enact broader FISA reforms outside the scope of Section 702, to encompass reforms within Title I. There was also unanimous agreement that reforms were necessary due to ineffective oversight by the FBI. Each Member participated fully in the effort to improve the existing FISA law.

The Joint Working Group's initial task was to identify the universe of problems with FISA. Each Member identified problems with FISA that were of particular concern to them. Members were typically in full agreement concerning FISA abuses and the problems with FISA. Members spent several sessions analyzing the scale and scope of these problems. For issues where there was a majority determination that a problem existed, the Group endeavored to find solutions. If multiple solutions to a problem were available, Members engaged in broad debate on which solution would be best for Congress to pursue as a legislative reform. The problems and solutions discussed in *The Need for FISA Reform: Strengthening FISA for the Future* and the *House Intelligence Committee Efforts on FISA Reauthorization sections* of this report are a product of the Joint Working Group.

Of particular concern to the Joint Working Group was the FBI's lack of institutional integrity in their use of Section 702. Members discussed at length what additional safeguards could be implemented to continue FBI's participation in Section 702 in a manner that protected constitutional rights. The Joint Working Group agreed that the FBI's querying process had to be the subject of significant reform. In particular, the Group agreed that the number of FBI employees with access and ability to query FISA information would need to be significantly reduced.

Another issue of special interest was the need for greater transparency of the FISC. One of the proposed solutions with consensus was to require the FISC to provide transcripts of

[205] Congressman Chris Stewart resigned from Congress on September 15, 2023. He was not replaced on the Working Group.

proceedings to the House and Senate Intelligence and Judiciary Committees. Allowing Congress to have greater oversight of the FISC would enhance the checks-and-balances originally envisioned by the Founding Fathers. Dozens of other proposed reforms were discussed, all with the intent to make FISA a better law.

The Need for FISA Reform: Strengthening FISA for the Future

Problems with Section 702

Section 702 has a number of problems requiring significant reform—from the need for increased penalties, compliance, and oversight, to the querying abuses by the FBI. Section 702 currently has no delineated penalties for those who purposefully abuse Section 702-acquired information or for those who are negligent and make mistakes while using Section 702-acquired information. The DNI and the Attorney General must issue a common set of minimum accountability standards for noncompliant querying of U.S. person contents acquired under Section 702, including zero tolerance for willful misconduct, escalating consequences for unintentional noncompliance, and consequences for the supervisors overseeing noncompliant users. In addition, there must be criminal penalties for those who intentionally leak information acquired under Section 702.

The FBI has a history of abuse regarding the querying of Section 702 information. This is partly due to the number of FBI personnel with access to the Section 702 database. Our reforms would cut over 90% of the FBI out of the ability to authorize U.S. person queries. Having fewer, more highly trained individuals with the ability to approve a query of Section 702-acquired information is an important step toward reforming the FBI's treatment of Section 702 information.

There is insufficient oversight and supervision of Section 702 use, particularly by the FBI. For example, there is no universal external review when the FBI queries sensitive U.S. persons. To address that, the DOJ must be required to audit every U.S. person query with information acquired under Section 702 conducted by the FBI within 6 months of such query. To allow for greater congressional oversight, the FBI should notify the House and Senate leaders, and the chairs and ranking members of the House and Senate Intelligence Committees, when the FBI queries a term that would identify a member of Congress.

Under scrutinization by Congress and the FISC, the FBI has recently implemented a series of important reforms to its internal procedures to address these abuses. Congress must codify these internal procedures to give them the weight of law, as well as make stronger reforms to ensure that FBI abuses are a problem of the past. As such, the FBI Director should be directed to ensure there are measures in place to hold FBI executive leaders accountable for the performance of their field office or headquarters component in terms of FISA compliance. The FBI should regularly brief Congress on these accountability measures and to describe any adverse personnel actions taken against FBI executive leaders whose field office or component has underperformed with respect to FISA compliance.

Section 702 can be strengthened by the addition of new provisions that make our nation more secure. For example, amending Section 101 to expand the ability of the NSA to target international drug trafficking operations, including those distributing fentanyl and precursor chemicals, by including "counternarcotics" in the definition of "foreign intelligence," would codify FISA's ability to be used to combat the flow of illegal drugs across our borders. In

addition, Section 702 needs to be amended to allow the NSA to query non-U.S. person terms for the purpose of screening and vetting immigration and non-immigrant visa applicants.

The protection of civil rights and liberties is critically important. The FBI, CIA, NSA, and NCTC should be prohibited from conducting any U.S. person query whose purpose is either (1) to suppress or burden criticism, dissent, or the free expression of ideas or political opinions by such U.S. person, or (2) to disadvantage such U.S. person based on their ethnicity, race, gender, sexual orientation, or religion.

Problems with Title I

Section 702 reauthorization gives Congress the opportunity to fix problems in other areas of FISA, including those uncovered during the multiple investigations of Crossfire Hurricane with the Title I electronic surveillance application process. Compulsory reprimand must be required, including suspension without pay or removal, for anything who engages in intentional misconduct before the FISC. Criminal penalties must be added and enhanced, including adding the FISC as a court system under which a person can be prosecuted for contempt. Civil remedies are necessary, too. One reform proposal is to create a new cause of action for an aggrieved U.S. person to be able to sue the employing government agency whose employee engaged in unlawful government surveillance for actual damages, punitive damages, and reasonable attorney's fees.

The electronic surveillance application process itself needs reform. For example, not all material information is required to be included in the written application but is instead orally provided to the FISC. In addition, there is no sworn statement required in the application process. Leaks to the media are also problematic. Information related to the applications leaks from the FBI and DOJ to the media with no accountability. We have reforms that will remedy these problems.

Problems with the FISC

The FISC and its proceedings are in need of reform, primarily to allow for greater transparency and oversight. For example, there is currently no requirement that FISC proceedings be transcribed and stored, in addition to testimony and affidavits, in the relevant court file. That must be changed. To allow for greater congressional oversight, transcripts need to be available by request for review by the congressional committees of jurisdiction. In addition, the Chairs and Ranking Members of the House and Senate Intelligence Committees, or their designated staff, must be permitted to attend FISC proceedings.

In addition, applications for renewal are not currently required to be reviewed by the same judge who granted or denied the original application. This prevents an application from having continuity in review and impairs a judge's ability to detect material differences between an original application and its renewal. This also must be changed.

Miscellaneous Problems

There are several other fixes that need to be made to FISA to make it a stronger law. For example, reauthorizing the roving wiretap authority under Title I, which provided for roving surveillance of a target who takes active measures to thwart FISA surveillance, such as cycling through burner phones, would help law enforcement and intelligence officials more easily track bad actors. In addition, reauthorizing the "lone wolf" authority under Title I, under which a non-U.S. person who "engages in international terrorism or activities in preparation thereof" was included in the definition of "agent of a foreign power," would make it easier to identify and prevent acts of terror.

House Intelligence Committee Efforts on FISA Reauthorization

Reforms to Section 702

Heightened Penalties

1. Insert a new subsection in Section 702 to create a pathway for the Committees, upon a joint request by either the Chairs and/or Ranking Members of the Judiciary and Intelligence Committees of either chamber, to trigger a mandatory, independent investigation by the Inspector General (IG) into alleged compliance violations or abuse. The IG would be responsible for investigating the allegations and any accountability actions taken by the FBI in response, and to report to the Committees.

2. Require the DNI and the Attorney General to issue a common set of minimum accountability standards for noncompliant querying of U.S. person contents acquired under Section 702, including zero tolerance for willful misconduct, escalating consequences for unintentional noncompliance, and consequences for the supervisors overseeing noncompliant users. This includes a requirement that these standards are submitted to Congress and subsequent annual reporting on specific disciplinary actions.

3. Amend Title XII to insert a new Section 709, Penalties. This would establish that a person is guilty of a criminal offense under this section if they intentionally leak information acquired under Section 702 that identifies a U.S. person to any person not entitled to receive classified information. The penalty for this offense would be a fine or imprisonment of up to eight years, or both.

Greater Transparency and Reporting

4. Amend Section 603 to require the FBI to report its U.S. person query metrics in the annual public FISA transparency report.

5. Amend Section 702 to require the FBI to notify the House and Senate leaders, and the Chairs and Ranking Members of the Intelligence Committees, when the FBI queries a term reasonably believed to identify a member of Congress.

6. Require the DOJ OIG to prepare a comprehensive report regarding the FBI's querying compliance under Section 702, with an emphasis on compliance with the rules governing U.S. person queries, and regarding the FBI's implementation of the various querying-related reforms required by Congress, by the FISC, and by the DOJ.

7. Amend Section 603 to require the FBI to report to Congress on an annual basis a comprehensive account of ongoing disciplinary investigations, adjudication of concluded investigations, and subsequent disciplinary actions resulting from noncompliant querying of information acquired under Section 702.

8. Amend Title VI to require the DNI to promptly notify Congress of any known or suspected disclosure of information acquired under Section 702, regardless of knowledge of identity of alleged leaker, to any person not entitled to receive classified information.

9. Amend Section 701 to define Electronic Communication Service Provider to include equipment.

10. Require that, once the FBI has determined that a member of Congress should receive a defensive briefing, they only conduct a query of information acquired under Section 702 to supplement such briefing if the member consents to the query. This also requires the FBI Director to notify Congress accordingly.

More Measures to Ensure Compliance

11. Require the FBI Director to ensure there are measures in place to hold FBI executive leaders accountable for the performance of their field office or headquarters component in terms of FISA compliance. This also requires the FBI to regularly brief Congress on these accountability measures and to describe any adverse personnel actions taken against FBI executive leaders whose field office or component has underperformed with respect to FISA compliance.

12. Require the DOJ to audit every U.S. person query within information acquired under Section 702 conducted by the FBI within 6 months of such query. This requirement would sunset after four years, or earlier if the Attorney General certifies to Congress that an internal auditing process of similar rigor has been instituted at the FBI.

13. Require the ODNI, in coordination with the NSA, to conduct a study on technological enhancements that would enable near-real time monitoring of 702 database compliance at the FBI.

Tighter Querying Restrictions

14. Amend Section 702 to require that the querying procedures for the FBI specifically include provisions:
    a. Requiring FBI personnel successfully complete training prior to conducting queries of information acquired under Section 702;
    b. Requiring approval from an FBI attorney prior to conducting any single query containing more than one search term;
    c. Requiring prior approval for queries related to sensitive investigative matters, including FBI Deputy Director approval for query terms related to political or press affiliated persons and FBI attorney approval for query terms related to religious persons;
    d. Requiring FBI personnel to provide written and recorded justifications for individual queries prior to conducting them; and
    e. Mandating that FBI systems maintain a function which requires the user to affirmatively record their intention to query information acquired under Section 702.

15. Amend Section 702 to limit the authority for FBI personnel able to authorize a query of U.S. person terms to a limited group of supervisors and attorneys.

16. Require the FBI to obtain a probable cause warrant prior to conducting any query of a U.S. person term for the purpose of Evidence of a Crime only.

17. Amend Section 702 to prohibit the FBI from receiving information acquired under Section 702 which is not directly related to an existing, open, predicated national security investigation.

18. Amend Section 101 to expand the ability for the NSA to target international drug trafficking operations, including those distributing fentanyl and precursor chemicals, by including counternarcotics in the definition of Foreign Intelligence.

19. Prohibit the FBI, CIA, NSA, and NCTC from conducting any U.S. person query whose purpose is either (1) to suppress or burden criticism, dissent, or the free expression of ideas or political opinions by such U.S. person, or (2) to disadvantage such U.S. person based on their ethnicity, race, gender, sexual orientation, or religion.

20. Amend Section 702 to prohibit any political appointee (defined as a position designated as a Presidential Appointment with Senate Confirmation, Presidential Appointment (without Senate Confirmation), Noncareer Senior Executive Service Appointment, or Schedule C Excepted Appointment) from inclusion in the FBI's prior approval process for queries.

21. Amend Section 702 to allow for the NSA to query non-U.S. person terms for the purpose of screening and vetting immigration and non-immigrant visa applicants.

22. Statement that any U.S. person targeted for collection, based upon incidental 702-obtained information, can only be targeted under court order.

Reforms to Title I

Heightened Penalties

23. Amend Section 103 to require appropriate adverse actions, including suspension without pay or removal, for anyone who engages in intentional misconduct with respect to proceedings before the FISC or the FISCR.

24. Amend Section 110 (Civil Liability) to create enhanced penalties where the aggrieved person is a U.S. person, and increase the punitive damages amount for U.S. persons to not less than 100 times the amount of actual damages.

25. Amend Section 110 (Civil Liability) to create a new cause of action for an aggrieved person who is a U.S. person to be able to also sue the employing government agency

whose employee engaged in unlawful government surveillance for actual damages, punitive damages, and reasonable attorney's fees.

26. Amend Title 18 to add an enhanced penalty of imprisonment for not more than eight years for knowingly making any false material declaration to the FISC or the FISCR.

27. Amend Section 109 to increase the maximum penalty from five to eight years for a person who unlawfully intentionally engages in or discloses information obtained through electronic surveillance not authorized by law.

28. Amend Section 109 to add criminal penalties for intentionally disclosing a FISA application, in whole or in part, to an unauthorized person.

29. Amend Title 18 to add the FISC or the FISCR as a court system under which a person shall be prosecuted for contempt.

Improved Application Quality and Process

30. Amend Sections 104 and 303 to prohibit the use of information derived from political organizations, such as opposition research, within any application for an order approving electronic surveillance unless that information is corroborated by other investigative techniques and both the information and investigative techniques are clearly identified within the application.

31. Amend Sections 104 and 303 to prohibit the use of information derived from a press report within any application for an order approving electronic surveillance unless that information is clearly identified within the application, corroborated by other investigative techniques, and the identity of the reporter and the press outlet are included.

32. Amend Sections 104 and 303 to require a statement describing the investigative techniques carried out before making the application.

33. Amend Sections 105 and 304 to require any application for an extension of an order for surveillance include a statement setting forth the results thus far obtained from the surveillance, or a reasonable explanation of the failure to obtain such results.

34. Amend Sections 104, 303, 703, and 704 to require the submission of material facts and circumstances in an application for an order approving electronic surveillance be made through certification under oath.

35. Amend Sections 104 and 303 to require an application for U.S. person surveillance under which the U.S. person is alleged to be acting as an agent of a foreign power, as defined specifically in Section 101(b)(2)(B), to include a full and complete statement of the facts and circumstances justifying the details as to the underlying criminal offense.

36. Amend Sections 104, 303, 402, 501, 703, and 704 to require certification to the FISC that the FISA application has been reviewed for accuracy and completeness and that the attorney for the government and the DOJ has been apprised of all material information that might reasonably call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made or otherwise raise doubts with respect to probable cause. This also requires that the Attorney General, in consultation with the FBI Director, shall issue procedures governing the review of case files, as appropriate, to ensure that U.S. person surveillance applications are accurate and complete.

37. Amend Sections 104 and 304 to shift resources to more strictly scrutinize the surveillance of U.S. persons over the surveillance of foreign persons by extending the time period by which a foreign person can be surveilled to one year prior to requiring application for an extension, allowing DOJ attorneys to prioritize matters such as accuracy and completeness assessments of U.S. persons applications over extensions of foreign person applications.

38. Amend Section 103 to designate a counsel to serve in cases involving a U.S. person target with the purpose of scrutinizing and providing the FISC with a written analysis of whether the government's proposed application contains any material weaknesses, flaws, or otherwise raises concerns to the judge assigned to consider the application.

Reforms to the FISC

Greater Congressional Oversight of Improved FISC

39. Amend Section 103 to require FISC and FISCR proceedings be transcribed and stored, in addition to testimony and affidavits, in the relevant court file.

40. Amend Section 601 to require copies of FISC and FISCR transcripts to be available by request for review by the House and Senate Intelligence and Judiciary Committees within 45 days of the date on which the matter concerning such hearing or oral argument is resolved.

41. Amend Section 105 to require the extension of a FISC order, to the extent practicable, to be granted or denied by the same judge who issued the original order.

42. Amend Section 702 to require the FISC to appoint amicus curiae in the annual Section 702 reauthorization application process, in order to ensure that Americans' privacy and civil liberties are protected.

43. Amend Section 103 to permit, for congressional oversight purposes, Chairs and Ranking Members of the House and Senate Intelligence Committees, or their designated staff, to attend FISC and FISCR proceedings.

Miscellaneous Reforms

Other Improvements to FISA

44. Reauthorize the roving wiretap authority under Title I, which provided for roving surveillance of a target who takes active measures to thwart FISA surveillance (such as cycling through burner phones).

45. Reauthorize the "lone wolf" authority under Title I, under which a non-U.S. person who "engages in international terrorism or activities in preparation thereof" was included in the definition of "agent of a foreign power."

FISA Title I vs. FISA Section 702

FISA is a comprehensive piece of legislation that includes more than just Section 702, although the provisions are often conflated. For example, the FBI's surveillance of Carter Page, a former foreign policy advisor to then-candidate Donald Trump, was conducted under Title I of FISA, not Section 702.[206] Only Title VII of FISA, which includes Section 702, is set to expire on December 31, 2023.[207] The rest of FISA will remain intact, regardless of whether Congress reauthorizes Section 702. However, Congress has the opportunity to make significant reforms to all of FISA.

Title I or "Traditional FISA" targets foreign powers or agents of foreign powers, *i.e.*, spies, who are located inside the United States, regardless of whether they are a U.S. person.[208] Section 702 only targets non-U.S. persons who are reasonably believed to be outside of the United States.[209] Below is a comparison of Title I against Section 702 that will highlight more of these differences.

Comparison of Application Procedures for Traditional FISA (Title I) and Section 702[210]		
	Traditional FISA (Title I)	*Section 702*
Authorizing Officials for Applications	Applications for electronic surveillance must be approved by the AG. 50 U.S.C. § 1804(a), (d).	Before authorizing any foreign intelligence acquisitions under Section 702, the AG and the DNI shall provide to the FISC a written certification and any supporting affidavit attesting that the statutory requirements under Section 702 have been met. 50 U.S.C. § 1881a(h). FBI applications to access the contents of Section 702-acquired

[206] *See generally,* Horowitz Report.
[207] Edward C. Liu, *Reauthorization of Title VII of the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV. (Mar. 17, 2023).
[208] 50 U.S.C. 1801.
[209] 50 U.S.C. 1881a ("An acquisition authorized under subsection (a)—(1) may not intentionally target any person known at the time of acquisition to be located in the United States; (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; (3) may not intentionally target a United States person reasonably believed to be located outside the United States; (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; (5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and (6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.").
[210] Edward C. Liu, *Comparison of FISA Title I and Section 702 Application Procedures*, CONG. RESEARCH SERV. (Oct. 3, 2023).

		communications, in connection with a non-national security related criminal investigation, where such contents have been retrieved using a U.S. person query term that was not designed to find and extract foreign intelligence information (hereinafter "FBI 702(f)(2) applications"), require the approval of the AG. 50 U.S.C. § 1881a(f)(2)(C).
Court of Jurisdiction	Applications are made to the FISC. 50 U.S.C. § 1804(a).	The FISC shall have jurisdiction to review the certification and the targeting, minimization, and querying procedures submitted by the AG and the DNI. 50 U.S.C. § 1881a(j)(1)(A). The FISC shall also have jurisdiction to review FBI 702(f)(2) applications. 50 U.S.C. § 1881a(f)(2)(B).
Internal DOJ Review	Under the FBI's Woods Procedures, FBI agents are required to complete a FISA Verification Form prior to submission of the application. Agents must also review the FISA application for factual accuracy and collect all relevant documentation. FBI agents are also required to create and maintain a "Woods File" that contains (1) supporting documentation for every factual assertion contained in the application and (2) the results of required database searches and confidential human source (CHS) file searches. FBI agents must also verify statements in the application regarding the reliability of the source. When submitting renewal applications, each factual assertion must be re-verified and supporting documentation must be provided for any new factual assertions. Dep't of Justice, *Audit of the*	As of July 6, 2021, the Woods Procedures are applicable to applications for traditional electronic surveillance, physical searches, installation of pen register and trap and trace devices, and orders to produce business records under FISA, but it is not clear whether they are applicable to the submission of certifications and proposed procedures under Section 702 or FBI 702(f)(2) applications. *See* Dep't of Justice, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures For Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* n.4 (Sept. 2021), https://oig.justice.gov/sites/default/files/reports/21-129.pdf.

	Federal Bureau of Investigation's Execution of Its Woods Procedures For Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons 3-4 (Sept. 2021), https://oig.justice.gov/sites/default/files/reports/21-129.pdf.	
Ex Parte Court Proceedings	Orders for electronic surveillance shall be issued *ex parte*. 50 U.S.C. § 1805(a). Non-adversarial hearings must be *ex parte* and conducted within the FISC's secure facility. FISC R. 17(b).	In any proceedings under this section, the Court shall, upon request of the Government, review *ex parte* and in camera any Government submission, or portions of a submission, which may include classified information. 50 U.S.C. § 1881a(l)(2). Non-adversarial hearings must be *ex parte* and conducted within the FISC's secure facility. FISC R. 17(b).
Appointment of Amici Curiae	If, in the opinion of the FISC, an application presents a novel or significant interpretation of law, the court shall appoint an amicus curiae to (1) make legal arguments that advance the protection of individual privacy and civil liberties; (2) provide information related to intelligence collection or communications technology; or (3) provide other assistance specified by the court, unless the court finds that such an appointment would not be appropriate. 50 U.S.C. § 1803(i)(2).	Same as under Traditional FISA.
Application Contents: Applicant	Application must include the identity of the federal officer making the application. 50 U.S.C. § 1804(a)(1)-(2).	Certification by AG and DNI must be submitted under oath and be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is appointed by the President, by and with the advice and consent of the Senate, or the head of an element of the intelligence community. 50 U.S.C. § 1881a(a), (h)(2)(C).

		FBI 702(f)(2) applications must include the identity of the federal officer making the application. 50 U.S.C. § 1881a(f)(2)(C)(i).
Application Contents: Target	Application must include the identity, if known, or a description, if the identity is not known, of the specific target of the electronic surveillance; a statement of the facts and circumstances justifying the belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power; and the facilities or places to be surveilled are being used, or are about to be used, by a foreign power or an agent of a foreign power. 50 U.S.C. § 1804(a)(3).	Certification by AG and DNI does not include information about specific targets, but must include targeting procedures that are reasonably designed to ensure that any acquisition authorized under the subsection is limited to targeting persons reasonably believed to be located outside the United States; and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be in the United States. 50 U.S.C. § 1881a(d)(1). Certification must also include guidelines to ensure that acquisitions do not intentionally target persons known to be in the United States; do not "reverse target"[211] U.S. persons; do not intentionally target U.S. persons abroad; do not intentionally acquire purely domestic communication; comply with limitations on "about collection";[212] and are conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States. 50 U.S.C. § 1881a(b), (g). FBI 702(f)(2) applications must include an affidavit or other statement of the facts and circumstances relied upon by the applicant to justify the belief that the query would provide

[211] "Reverse targeting" refers to the intentional targeting of an overseas non-U.S. person with the purpose of targeting a specific person within the United States. 50 U.S.C. § 1881a(b)(2).
[212] "About collection" refers to the acquisition of communications that are neither to nor from the target, but which mention the target. 50 U.S.C. § 1881a(b)(5). [*Note*: The NSA stopped "about collection" in 2017.]

		evidence of criminal activity; contraband, fruits of a crime, or other items illegally possessed by a third party; or property designed for use, intended for use, or used in committing a crime. 50 U.S.C. § 1881a(f)(2)(C)(ii).
Application Contents: Alternative Measures	Application must include certifications, including supporting statements, by certain executive branch officials that the information sought is foreign intelligence information; that a significant purpose of the surveillance is to obtain foreign intelligence information; and that such information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a)(6).	None required.
Application Contents: Scope of Surveillance	Application must include proposed minimization procedures; a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; a summary statement of the means by which the surveillance will be carried out, including whether physical entry is required; and a statement of the duration for which the electronic surveillance is required to be maintained. 50 U.S.C. § 1804(a)(7), (9).	Certification must include proposed targeting, minimization, and querying procedures and additional guidelines to ensure compliance. 50 U.S.C. § 1881a(h)(2)(B).
Application Contents: Application History	Application must include information about previous FISA applications involving any of the same persons, facilities, or places, and the action taken on each previous application. 50 U.S.C. § 1804(a)(8).	None required.
FISC Probable Cause Determinations	FISC judge may issue order if there is probable cause to believe that the target of the electronic surveillance is a foreign power or	None required for review of certification.

	an agent of a foreign power and each of the facilities or places to be surveilled are being used, or are about to be used, by a foreign power or an agent of a foreign power, based on the facts submitted. No U.S. person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States. 50 U.S.C. § 1805(a)(2).	FISC may issue an order granting FBI 702(f)(2) application if the court finds probable cause to believe the query would provide evidence described in the application. 50 U.S.C. § 1881a(f)(2)(D).
Record of Proceedings	The record of proceedings, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the AG and the DNI. 50 U.S.C. § 1803(c). Testimony received by the FISC may be recorded electronically or as the judge may otherwise direct, consistent with the court's security measures. FISC R. 17(d). Upon motion of United States after denial of an application or appeal, the record shall be transmitted to the FISCR or the Supreme Court, respectively, under seal. 50 U.S.C. § 1803(a)(1), (b). Certifications, applications made, and orders granted shall be retained for a period of at least 10 years. 50 U.S.C. § 1805(h).	The FISC shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the AG and the DNI. 50 U.S.C. § 1881a(l)(1). Testimony received by the FISC may be recorded electronically or as the judge may otherwise direct, consistent with the court's security measures. FISC R. 17(d).
Initial Duration of Order	Initial orders may last up to 90 days by default. Duration of order may be up to 120 days if target is a non-U.S. person who is an agent of a foreign power. Duration may be up to one year if target is a	Foreign intelligence acquisitions under Section 702 may be authorized for up to one year. 50 U.S.C. § 1881a(a).

	foreign government or any component thereof; a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. 50 U.S.C. § 1805(d)(1).	
Appeals	If the FISC denies an application for traditional electronic surveillance, it shall immediately provide a written statement on the record of the reasons for the decision. If the government appeals the denial, the record shall be transmitted, under seal, to the FISCR. If the FISCR determines that the application was properly denied, the court shall provide a written statement on the record providing the reasons for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision. 50 U.S.C. § 1803(a)(1), (b).	The government may appeal any order by the FISC regarding a certification to the FISCR, which shall have jurisdiction to consider such appeal. The FISCR shall provide a written statement for any decision. Upon the filing of a petition for a writ of certiorari the record for review in the FISCR shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision. 50 U.S.C. § 1881a(j)(4).
Renewals	Order may be renewed for same initial duration using same application process. If the target is a foreign-based political organization, not substantially composed of U.S. persons; an entity that is directed and controlled by a foreign government or governments; an entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction; or a group engaged in international	If the AG and the DNI seek to reauthorize collection under Section 702, the certification, procedures, and other material shall be submitted to the FISC at least 30 days prior to the expiration of the current authorization, to the extent practicable. The current authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, until the Court issues an order with respect to the reauthorization. 50 U.S.C. § 1881a(j)(5).

	terrorism or activities in preparation therefor that is not a U.S. person, the order may be renewed for up to one year if the judge also finds that no communication of any individual U.S. person will be acquired. If the target is an agent of a foreign power that is not a U.S. person, the order may also be renewed for up to one year. 50 U.S.C. § 1805(d)(2).	
Emergencies	The AG may authorize the emergency use of electronic surveillance for up to 7 days. A standard application for an electronic surveillance order must be submitted within seven days of the beginning of the emergency surveillance. If the FISC subsequently denies such an emergency application, no information obtained during the emergency period may be used as evidence or otherwise disclosed in any trial, hearing, or other proceeding. No information concerning any U.S. person acquired from such surveillance shall subsequently be used or disclosed in any other manner unless the AG determines that the information indicates a threat of death or serious bodily harm to any person. 50 U.S.C. § 1805(e). If a non-U.S. person target is subject to surveillance under Section 702 while outside the United States and subsequently enters the United States, the surveillance may continue for up to 72 hours if the head of an element of the intelligence community determines that a lapse would pose a threat of death or	The AG and DNI may authorize collection under Section 702 without a court order upon a determination that exigent circumstances exist, intelligence important to U.S. national security may be lost or not timely acquired, and there is insufficient time to obtain an order. The AG and the DNI shall submit a certification for such collection to the FISC as soon as practicable but no later than 7 days after such determination is made. 50 U.S.C. § 1881a(c)(2), (h)(1)(B). The FBI may conduct a query of information collected under Section 702 without prior approval from the FISC if the FBI determines there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm. 50 U.S.C. § 1881a(f)(2)(E).

	serious bodily harm to any person. 50 U.S.C. § 1805(f).	
Notice to Targets of Surveillance	If the government intends to use information obtained or derived through electronic surveillance in any trial, hearing, or other proceeding against an aggrieved person, the government must notify that person of the intent to use such information. 50 U.S.C. § 1806(c). If emergency electronic surveillance is conducted and a subsequent order approving the surveillance is not obtained, the FISC shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the FISC may determine in his discretion it is in the interest of justice to serve, notice of the fact of the application; the period of the surveillance; and the fact that during the period information was or was not obtained. On an *ex parte* showing of good cause to the FISC, this notice may be postponed or suspended for up to ninety days. On a further *ex parte* showing of good cause, the FISC shall forego ordering notice. 50 U.S.C. § 1806(j).	Same notice requirements apply, except that requirement to notify targets of emergency surveillance is not required. 50 U.S.C. § 1881e(a)(1).
Suppression of Evidence	If information derived from electronic surveillance is sought to be used as evidence against a person in any proceeding, the person may move to suppress such information if it was unlawfully acquired or otherwise not in compliance with the order authorizing electronic surveillance. If the AG files an affidavit that disclosure would	Same suppression procedures apply to Section 702 information. 50 U.S.C. § 1881e(a)(1). Additionally, evidence acquired under Section 702 may not be used against a U.S. person in any criminal proceeding unless an FBI 702(f)(2) application was granted with respect to the information, or the AG determines that the criminal

	harm the national security of the United States, such a motion shall be considered by the court in camera and *ex parte* to determine the lawfulness of such electronic surveillance. The court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance. 50 U.S.C. § 1806(e), (f).	proceeding is related to the national security of the United States; or involves death, kidnapping, serious bodily injury, certain offenses against a minor, incapacitation or destruction of critical infrastructure, cybersecurity, transnational crime, or human trafficking. The AG's determination is not subject to judicial review. 50 U.S.C. § 1881e(a)(2).
Civil Liability	An aggrieved person, other than a foreign power or an agent of a foreign power, may bring a civil suit against a person that, acting under color of law, has intentionally subjected the aggrieved person to electronic surveillance that is not authorized under FISA, the Electronic Communications Privacy Act, Stored Communications Act, or another express statutory authorization. An aggrieved person may also sue any person who intentionally discloses or uses information knowing, or having reason to know, that such information was obtained through unauthorized electronic surveillance. Successful plaintiffs may recover actual damages (or liquidated damages), punitive damages, and reasonable attorney's fees. 50 U.S.C. § 1810.	Acquisitions of communications that are not authorized under Section 702 may give rise to civil liability under the civil-suit provision in Title I depending on whether the elements of that cause of action are met. However, FISA does not include a civil liability provision for violations that are specific to Section 702, such as violations of the requirements surrounding FBI 702(f)(2) applications.

FISA Title I vs. ECPA ("Wiretap Act")

FISA Title I is also not to be confused with the Electronic Communications Privacy Act (ECPA) ("Wiretap Act"). FISA Title I provides a statutory framework for government agencies to obtain authorization to conduct electronic surveillance to gather foreign intelligence, while ECPA establishes a judicially supervised procedure to authorize similar surveillance for law enforcement purposes. Below is a comparison of the two statutes.

Comparison of Procedures for FISA Title I Electronic Surveillance and ECPA Interception Orders[213]		
Authorizing Officials for Applications	Applications for electronic surveillance must be approved by: • Attorney General or acting Attorney General • Deputy Attorney General • Designated Assistant Attorney General for National Security. 50 U.S.C. §§ 1801(g), 1804(a), (d).	Applications for oral, wire, or electronic interception must be authorized by: • Attorney General • Deputy Attorney General • Associate Attorney General • Any Assistant Attorney General, or acting Assistant Attorney General • Designated Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division. 18 U.S.C. § 2516(1).
Court of Jurisdiction	Applications are made in writing upon oath or affirmation to judges designated to sit on the Foreign Intelligence Surveillance Court (FISC), one of two specialized foreign intelligence courts created to approve the use of FISA investigative authorities. 50 U.S.C. § 1803(a). The FISC has original jurisdiction over FISA applications, while the Foreign Intelligence Surveillance Court of Review (FISCR) may hear appeals from the FISC.	Applications are made in writing upon oath or affirmation to U.S. district court judge, or U.S. court of appeals judge. 18 U.S.C. § 2510(9).

[213] Edward C. Liu, *Comparison of FISA Electronic Surveillance and ECPA Wiretapping Application Procedures*, CONG. RESEARCH SERV. (July 18, 2023).

	50 U.S.C. § 1803(a), (b).	
Internal DOJ Review	Under the FBI's Woods Procedures, FBI agents are required to complete a FISA Verification Form prior to submission of the application. Agents must also review the FISA application for factual accuracy and collect all relevant documentation. FBI agents are also required to create and maintain a "Woods File" that contains (1) supporting documentation for every factual assertion contained in the application and (2) the results of required database searches and confidential human source (CHS) file searches. FBI agents must also verify statements in the application regarding the reliability of the source. When submitting renewal applications, each factual assertion must be re-verified and supporting documentation must be provided for any new factual assertions. U.S. Dep't of Justice, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures For Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* 3-4 (Sept. 2021).	The Electronic Surveillance Unit (ESU) of the DOJ Criminal Division's Office of Enforcement Operations reviews proposed applications for electronic surveillance, including: • Affidavits setting forth the facts of the investigation that establish probable cause and other statements required to be included in the application; • The application by U.S. Attorneys or Assistants that provides the basis for the court's jurisdiction; • The proposed order to be signed by the court; and • A completed cover sheet that includes the signature of a supervising attorney who reviewed and approved the application. All submissions must be approved by a supervising attorney other than the attorney submitting the application. That supervisory attorney's signature on the cover sheet demonstrates that he or she has reviewed the affidavit, application, and draft order included in the submission packet, and that he or she supports the request and approves of it. U.S. Dep't of Justice, Justice Manual § 9-7.110 (Jan. 2020).
Ex Parte Court Proceedings	Orders for electronic surveillance shall be issued *ex parte*. 50 U.S.C. § 1805(a). If, in the opinion of the FISC, an application presents a novel or significant interpretation of law, the	Orders authorizing interception of oral, wire, or electronic communications shall be issued *ex parte*. 18 U.S.C. § 2518(3).

	court shall appoint an amicus curiae to (1) make legal arguments that advance the protection of individual privacy and civil liberties; (2) provide information related to intelligence collection or communications technology; or (3) provide other assistance specified by the court, unless the court finds that such an appointment would not be appropriate. 50 U.S.C. § 1803(i)(2). Non-adversarial hearings must be *ex parte* and conducted within the FISC's secure facility. FISC R. 17(b).	
Application Contents: Applicant	Application must include the identity of the federal officer making the application. 50 U.S.C. § 1804(a)(1)-(2).	Application must include the identity of the investigative or law enforcement officer making the application and the officer authorizing the application. 18 U.S.C. § 2518(1)(a).
Application Contents: Target	Application must include the identity, if known, or a description, if the identity is not known, of the specific target of the electronic surveillance; a statement of the facts and circumstances justifying the belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power; and the facilities or places to be surveilled are being used, or are about to be used, by a foreign power or an agent of a foreign power. 50 U.S.C. § 1804(a)(3).	Application must include the identity of the person, if known, allegedly committing the offense whose communications are to be intercepted; and a full and complete statement of the facts and circumstances justifying the belief that an order should be issued, including details as to the underlying offense. 18 U.S.C. § 2518(1)(b)(i), (iv).
Application Contents: Alternative Measures	Application must include certifications, including supporting statements, by certain executive branch officials that the information sought is foreign intelligence information; that a significant purpose of the surveillance is to obtain foreign intelligence information; and that such information cannot reasonably be	Application must include a full and complete statement as to whether other investigative procedures have been tried and failed or, if not, why they reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C. § 2518(1)I.

	obtained by normal investigative techniques. 50 U.S.C. § 1804(a)(6).	
Application Contents: Scope of Surveillance	Application must include proposed minimization procedures; a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; a summary statement of the means by which the surveillance will be carried out, including whether physical entry is required; and a statement of the duration for which the electronic surveillance is required to be maintained. 50 U.S.C. § 1804(a)(7), (9).	Application must include a particular description of the nature and location of the facilities or place where the communication is to be intercepted, a particular description of the type of communications sought to be intercepted, and a statement of the duration for which the interception is required to be maintained. 18 U.S.C. § 2518(1)(b)(ii)-(iii), (d). If identifying the facilities or place where a communication is to be intercepted is not practical or is being thwarted by the target, the application must include a full and complete statement to that effect. 18 U.S.C. § 2518(11).
Application Contents: Application History	Application must include information about previous FISA applications involving any of the same persons, facilities, or places, and the action taken on each previous application. 50 U.S.C. § 1804(a)(8).	Application must include information concerning all previous applications known to the individual authorizing and making the application that were made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application. Where the application is for the extension of an order, the application must also include a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. 18 U.S.C. § 2518(1)I, (f).
Probable Cause Determinations	FISC judge may issue order if there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power and each of the	Judge may issue order if, based on the facts submitted, there is probable cause to believe that an individual is committing, has committed, or is about to commit a predicate offense;

	facilities or places to be surveilled are being used, or are about to be used, by a foreign power or an agent of a foreign power, based on the facts submitted. No U.S. person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States. 50 U.S.C. § 1805(a)(2).	that particular communications concerning that offense will be obtained through such interception; that the facilities from which, or the place where, the communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. 18 U.S.C. § 2518(3).
Record of Proceedings	The record of proceedings, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence. 50 U.S.C. § 1803I. Testimony received by the FISC may be recorded electronically or as the judge may otherwise direct, consistent with the court's security measures. FISC R. 17(d). Upon motion of United States after denial of an application or appeal, the record shall be transmitted to the FISCR or the Supreme Court, respectively, under seal. 50 U.S.C. § 1803(a)(1), (b). Certifications, applications made, and orders granted shall be retained for a period of at least 10 years. 50 U.S.C. § 1805(h).	Testimony taken in the presence of a judge in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit. F.R. Crim. P. 41(d)(2)I.
Initial Duration of Order	Initial orders may last up to 90 days by default. Duration of order may be up to 120 days if target is a non-U.S. person who is an agent of a foreign power. Duration may be up to one year if target is a foreign government or any component thereof; a faction of a foreign nation or nations, not substantially composed of U.S.	Initial orders may last up to 30 days. 18 U.S.C. § 2518(5).

	persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. 50 U.S.C. § 1805(d)(1).	
Renewals	Order may be renewed for same initial duration using same application process. If the target is a foreign-based political organization, not substantially composed of U.S. persons; an entity that is directed and controlled by a foreign government or governments; an entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction; or a group engaged in international terrorism or activities in preparation therefor that is not a U.S. person, the order may be renewed for up to one year if the judge also finds that no communication of any individual U.S. person will be acquired. If the target is an agent of a foreign power that is not a U.S. person, the order may also be renewed for up to one year. 50 U.S.C. § 1805(d)(2).	Order may be renewed for additional 30-day periods using same application process. 18 U.S.C. § 2518(5).
Emergencies	The Attorney General, Acting Attorney General, Deputy Attorney General, or (if designated) the Assistant Attorney General for National Security may authorize the emergency use of electronic surveillance for up to 7 days. A standard application for an electronic surveillance order must be submitted within seven days of the beginning of the emergency surveillance. If the FISC subsequently denies such an emergency application, no information obtained during the emergency period may be used as evidence or otherwise disclosed in any trial, hearing, or other	Any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, or the Associate Attorney General, may intercept wire, oral, or electronic communications after reasonably determining that an emergency exists involving immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. The officer must also find that there are grounds upon which an order could be issued to authorize such

	proceeding. No information concerning any U.S. person acquired from such surveillance shall subsequently be used or disclosed in any other manner unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person. 50 U.S.C. § 1805I. If a non-U.S. person target is subject to surveillance under Section 702b while outside the United States and subsequently enters the United States, the surveillance may continue for up to 72 hours if the head of an element of the intelligence community determines that a lapse would pose a threat of death or serious bodily harm to any person. 50 U.S.C. § 1805(f).	interception and must apply for such an order within 48 hours.
Notice to Targets of Surveillance	If the government intends to use information obtained or derived through electronic surveillance in any trial, hearing, or other proceeding against an aggrieved person, the government must notify that person of the intent to use such information. 50 U.S.C. § 1806I.	Targets of surveillance shall be notified within a reasonable time, but not later than 90 days, after an application is denied or after an order has expired of (1) the existence of the application or order; (2) the dates covered; and (3) whether their communications were intercepted. Other parties to intercepted communications may also be notified if the judge determines is in the interest of justice. Such notified persons, or their counsel, may request to inspect such portions of the intercepted communications that the judge determines to be in the interest of justice. On an *ex parte* showing of good cause by the government, this required notice may be postponed. 18 U.S.C. § 2518(8)(d).
Suppression of Evidence	If information derived from electronic surveillance is sought to be used as evidence against a person in any proceeding, the person may move to suppress such information if	Any aggrieved person may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds

	it was unlawfully acquired or otherwise not in compliance with the order authorizing electronic surveillance. If the Attorney General files an affidavit that disclosure would harm the national security of the United States, such a motion shall be considered by the court in camera and *ex parte* to determine the lawfulness of such electronic surveillance. The court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance. 50 U.S.C. § 1806I, (f).	that the communication was unlawfully intercepted; the order under which it was intercepted is insufficient on its face; or the interception was not made in conformity with the order. The judge, upon the filing of such motion by the aggrieved person, may in their discretion make available to the aggrieved person or their counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice. 18 U.S.C. § 2518(10).
Civil Liability	An aggrieved person, other than a foreign power or an agent of a foreign power, may bring a civil suit for unlawful surveillance under FISA. Successful plaintiffs may recover actual damages (or liquidated damages), punitive damages, and reasonable attorney's fees. 50 U.S.C. § 1810.	Persons subject to surveillance in violation of ECPA may sue to obtain injunctive relief, damages (equal to the greater of actual damages (or liquidated damages), punitive damages, reasonable attorney's fees and reasonable litigation costs. 18 U.S.C. §§ 2520, 2521, 2712.

Oversight of FISA

FISA currently has a series of mandated reporting requirements. These reporting provisions give the Executive Branch, Legislative Branch, and even the general public the ability to monitor FISA's efficacy and oversee its usage. Statutorily mandated reporting requirements are particularly valuable to Congress for conducting oversight of agency non-compliance and, as has been the case with the FBI, hold agency officials accountable when they fail to follow the law. All of the reports, including some made public, are transmitted to either or both of the U.S. House and Senate Intelligence and Judiciary Committees. Among the reforms currently being considered by Congress are enhanced reporting provisions to afford for greater oversight of the intelligence agencies that use FISA. Below are the current mandatory reporting provisions.

FISA Mandatory Reporting Provisions[214]			
Citation and Contents	*Reporting Entity and Frequency*	*Recipients*	*Unclassified Forms Required*
50 U.S.C. § 1807 • Number of electronic surveillance applications. • Number of orders granted, modified, or denied. Number of subjects targeted by electronic surveillance rounded to the nearest 500, including the number of such individuals who are United States persons, reported to the nearest band of 500.	Attorney General; Annually in April	House and Senate Intelligence and Judiciary Committees	Each report shall be submitted in unclassified form, to the extent consistent with national security. Each report, an unclassified summary of the report, or a redacted version of the report, shall be made publicly available consistent with national security.
50 U.S.C. § 1808(a) • Number of electronic surveillance applications where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown. • Each criminal case in which information acquired under FISA	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None

[214] Edward C. Liu, *Reporting Provisions in the Foreign Intelligence Surveillance Act of 1978*, CONG. RESEARCH SER. (Feb. 2, 2023).

has been authorized for use at trial. • Number of emergency uses of electronic surveillance and the total number of subsequent orders approving or denying such electronic surveillance. Number of authorizations to continue electronic surveillance of non-U.S. persons for 72 hours after they are believed to be located in the U.S. and the total number of subsequent emergency employments of electronic surveillance or emergency physical searches.			
50 U.S.C. § 1826 • Number of physical search applications. • Number of orders granted, modified, or denied. • Number of physical searches that involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where notice of the search was provided. Number of emergency physical searches and the number of subsequent orders approving or denying such physical searches.	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None
50 U.S.C. § 1846 • Number of pen register or trap and trace device (PR/TT) applications. • Number of orders either granted, modified, or denied. • Number of emergency PR/TT installations and uses and the number of subsequent orders approving or denying such installation and use. • Each department or agency for which a PR/TT application was	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	Each report shall be submitted in unclassified form, to the extent consistent with national security. Each report, an unclassified summary of the report, or a redacted version of the report, shall be made publicly available

made, with breakouts for statistics above. Good faith estimate of the total number of subjects targeted by a PR/TT rounded to the nearest 500, including the number of United States persons, reported to the nearest band of 500, and the number of United States persons whose information was reviewed or accessed.			consistent with national security.
50 U.S.C. § 1863(a) Fully inform Intelligence Committees about all requests for business records under FISA.	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None
50 U.S.C. § 1863(b) • Number of business records applications. Number of orders granted, modified, or denied.	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None
50 U.S.C. § 1871 • Aggregate number of persons targeted under FISA, including breakdowns for electronic surveillance, physical searches, PR/TT, production of tangible things,[215] and acquisitions of U.S. persons while they are outside the United States. • Number of "lone wolf" individuals covered by a FISA order.[216] • Number of times FISA information obtained under this chapter was authorized to be used in a criminal proceeding. • Summaries of significant legal interpretations of FISA by the	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None

[215] Orders for the production of tangible things, including special provisions for "call detail records," were authorized under 50 U.S.C. § 1861, as amended by Section 215 of the USA PATRIOT Act, P.L. 110-76, and the USA FREEDOM Act of 2015, P.L. 114-23. This authority lapsed on March 15, 2020.

[216] "Lone wolf" individuals were defined under 50 U.S.C. § 1801(b)(1)(C), as amended by Section 6001(b) of P.L. 108-458, as persons engaged in international terrorism regardless of whether for or on behalf of a foreign power. This definition lapsed on March 15, 2020.

Foreign Intelligence Surveillance Court (FISC) or the Foreign Intelligence Surveillance Court of Review (FISCR), including interpretations in applications or pleadings filed with such courts by the Department of Justice. Copies of all decisions, orders, or opinions of the FISC or FISCR that include significant construction or interpretation of FISA.			
50 U.S.C. § 1873(a) • Number of applications or certifications for FISA orders. • Number of such orders granted, modified, or denied under each section. • Number of appointments of amicus curiae, including the name of such individuals. Number of findings by FISC or FISCR that appointment of amicus curiae is not appropriate and the text of any such findings.	Director of the Administrative Office of the United States Courts; Annually	House and Senate Intelligence and Judiciary Committees	Subject to declassification review by Attorney General and Director of National Intelligence. Report shall be publicly available on the internet, excluding findings that appointment of amicus curiae is inappropriate.
50 U.S.C. § 1873(b) • Number of orders issued authorizing electronic surveillance, physical searches, or targeting U.S. persons outside of the United States. Good faith estimates of number of targets of such orders. • Number of orders issued under Section 702 of FISA (authorizing targeting of non-U.S. persons while they are outside the United States), or authorizing queries of information collected under Section 702. Good faith estimates of number of targets, queries, and criminal investigations based on Section 702 information.	Director of National Intelligence; Annually	Public	Report shall be made publicly available on the internet.

• Number of PR/TT orders issued and good faith estimate of the number of targets of such orders and the number of unique identifiers used to communicate information collected pursuant to such orders. • Number of criminal proceedings in which notice of the intent to use FISA information was provided. • Number of tangible things orders issued and a good faith estimate of the number of targets of such orders and the number of unique identifiers used to communicate information collected pursuant to such orders.[217] • Number of "call detail records" orders issued and a good faith estimate of the number of targets of such orders, the number of unique identifiers used to communicate information collected pursuant to such orders, and the number of U.S. person search terms used to query any database of call detail records.[218] Number of national security letters issued and the number of requests for information contained within such national security letters.			
50 U.S.C. § 1881f With respect to authorizations to target non-U.S. persons outside the United States under Section 702 of FISA: • Certifications submitted by Attorney General and Director of National Intelligence that requirements of Section 702.	Attorney General; Semi-annually	House and Senate Intelligence and Judiciary Committees	None

[217] Orders for the production of tangible things, including special provisions for "call detail records," were authorized under 50 U.S.C. § 1861, as amended by Section 215 of the USA PATRIOT Act, P.L. 110-76, and the USA FREEDOM Act of 2015, P.L. 114-23. This authority lapsed on March 15, 2020.
[218] *Id*.

• If Attorney General and Director of National Intelligence determine that acquisition before court authorization is necessary due to exigent circumstances, the reasons for exercising the authority under such section. • Any directives issued under Section 702. • A description of the judicial review during the reporting period of such certifications and targeting and minimization procedures, including copies of orders or pleadings in connection with such review that contains a significant legal interpretation of Section 702. • Actions taken to challenge or enforce a directive. • Compliance reviews conducted by the Attorney General or the Director of National Intelligence. • Descriptions of any noncompliance incidents. • Procedures implementing Section 702. With respect to orders authorizing surveillance of U.S. persons while outside the United States under Sections 703 or 704 of FISA: • Number of applications. • Number of orders granted, modified, or denied. Number of emergency acquisitions authorized by the Attorney General and the number of subsequent orders approving or denying such acquisitions.			
50 U.S.C. § 1885c • Certifications made by Attorney General to dismiss civil suit against person that provided assistance to implement FISA surveillance.	Attorney General; Every 6 months	House and Senate Intelligence and Judiciary Committees	None

Description of judicial review of such certifications, and any actions taken to preempt state investigations, disclosure requirements, suits, or sanctions against electronic communications service providers that are alleged to have provided assistance to an element of the Intelligence Community.			