118TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 118–302
Part 1

FISA REFORM AND REAUTHORIZATION ACT OF 2023

DECEMBER 8, 2023.—Ordered to be printed

Mr. TURNER, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 6611]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 6611) to amend the Foreign Intelligence Surveillance Act of 1978 to make certain reforms to the authorities under such Act, to reauthorize title VII of such Act, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass

SECTION-BY-SECTION

SECTION-BY-SECTION SUMMARY OF FISA REFORM AND REAUTHORIZATION ACT OF 2023

TITLE I—RESTRICTIONS ON FEDERAL BUREAU OF INVESTIGATION QUERIES

Section 101. Revoking Federal Bureau of Investigation authority to conduct queries unrelated to national security.

Section 101 prohibits the FBI from conducting any query of Section 702 information that is designed solely to retrieve evidence of a crime, with narrow exceptions for when the FBI has a reasonable belief that the query could assist in mitigating or eliminating a threat to life or serious bodily harm, or when the query is necessary to comply with criminal court-related litigation or discovery obligations.

Section 102. Strictly limiting Federal Bureau of Investigation personnel authorizing United States person queries.

Section 102 requires an FBI supervisor or FBI attorney to provide prior approval of every U.S. person query conducted by the FBI, unless the FBI employee seeking to conduct the U.S. person query has a reasonable belief that the query could assist in mitigating or eliminating a threat to life or serious bodily harm. Compared to the status quo, Section 102 will reduce FBI personnel authorized to approve U.S. person queries by over 90 percent.

Section 103. Notification for certain queries conducted by Federal Bureau of Investigation.

Section 103 requires the FBI Director, in the event the FBI conducts a query of the name or other personally identifying information of a Member of Congress, to notify both that Member of Congress and congressional leadership. Section 103 allows a temporary exception if such notification would impede an ongoing national security or law enforcement investigation.

Section 104. Requirement for congressional consent prior to certain Federal Bureau of Investigation queries for purpose of defensive briefings.

Section 104 requires the FBI to obtain a Member of Congress's consent before conducting a query for the purpose of supplementing a defensive briefing for that Member on a counterintelligence threat to the Member, unless the Deputy Director of the FBI determines that exigent circumstances exist to justify the query. Section 104 further requires the FBI Director to notify congressional leadership when such consent was sought or when such exigent circumstances existed.

Section 105. Restrictions relating to conduct of certain queries by Federal Bureau of Investigation.

Section 105 codifies additional requirements on the FBI, including requiring specialized training, higher-level approval for sensitive queries (such as those involving public officials, members of the media, or religious leaders) and those involving batch job technology, case-specific recorded query justifications, and standardized FBI systems to protect against inadvertent over-broad querying, with the ability for the Foreign Intelligence Surveillance Court (FISC) to waive certain requirements.

Section 106. Prohibition on involvement of political appointees in process to approve Federal Bureau of Investigation queries.

Section 106 prohibits any political appointee at the FBI from being able to approve any FBI query, including any U.S. person query, of Section 702 information.

Section 107. Requirement for adoption of certain minimum accountability standards.

Section 107 requires the FBI Director to issue minimum accountability standards to ensure appropriate consequences for FBI employees who conduct noncompliant U.S. person queries of Section 702 information, including zero tolerance for willful misconduct, escalating consequences for unintentional noncompliance, and con-

sequences for FBI supervisors who oversee individuals who conduct noncompliant U.S. person queries. Section 107 further requires the FBI Director to submit these standards to the congressional intelligence and judiciary committees within 90 days of enactment, and to submit an annual report for three years on each adverse personnel action taken pursuant to these accountability standards.

Section 108. Restriction on certain information available to Federal Bureau of Investigation.

Section 108 codifies a prohibition on the FBI storing unminimized Section 702 information in its databases unless the information pertains to a foreign target who is relevant to an existing, open, predicated, full national security investigation by the FBI, with narrow exceptions if the FBI agreed to assist another federal agency or if the Director of the National Security Agency determines that exigent circumstances exist and subsequently notifies Congress.

Section 109. Mandatory audits of United States person queries conducted by Federal Bureau of Investigation.

Section 109 requires the National Security Division of the Department of Justice to independently audit every U.S. person query conducted by the FBI no later than 180 days after each query was conducted.

Section 110. Prohibited purposes for queries using United States person query terms.

Section 110 prohibits any U.S. person query of Section 702 information if the purpose is either (1) to suppress or burden criticism, dissent, or the free expression of ideas or political opinions by that U.S. person, or (2) to disadvantage or harm that U.S. person based on their ethnicity, race, gender, sexual orientation, or religion. Section 110 is intended to provide further assurance that U.S. government employees conduct U.S. person queries of Section 702 information in order to retrieve foreign intelligence information, and not for any other purpose.

TITLE II—FISA APPLICATIONS AND ORDERS

Section 201. Requirement for sworn statements for factual assertions.

Section 201 requires the U.S. government, when applying for a probable cause order under FISA, to include a sworn statement of the facts by the U.S. government applicant.

Section 202. Prohibition on use of politically derived information in applications for certain orders by the Foreign Intelligence Surveillance Court.

Section 202 requires the U.S. government to certify under oath, when applying for a probable cause order to conduct electronic surveillance or physical search, that none of the information in the application is opposition research from a political organization, unless the information is independently corroborated and the government's application clearly identifies the political organization

source and the investigative techniques used to corroborate the information.

Section 203. Prohibition on use of press reports in applications for certain orders by the Foreign Intelligence Surveillance Court.

Section 203 requires the U.S. government to certify under oath, when applying for a probable cause order to conduct electronic surveillance or physical search, that none of the information in the application is solely attributable to or derived from media source content, unless the application clearly identifies each author and publisher, as applicable.

Section 204. Description of techniques carried out before application.

Section 204 requires the U.S. government, when applying for a probable cause order to conduct electronic surveillance of a U.S. person, to include a statement summarizing the investigative techniques carried out before making the application.

Section 205. Requirement for certain justification prior to extension of orders.

Section 205 requires the U.S. government, when applying for an extension of a probable cause order to conduct electronic surveillance or physical search of a U.S. person, to include a summary of the foreign intelligence information obtained pursuant to prior FISC orders relating to that U.S. person or a reasonable explanation of the failure to obtain such information.

Section 206. Requirement for certifications regarding accuracy of applications.

Section 206 requires the U.S. government, in all applications to the FISC, to certify that the Attorney General or designated attorney for the government has notice of all information that might call into question the accuracy of that application or otherwise raise doubts about probable cause. Section 206 also requires the Attorney General, in consultation with the FBI Director, to issue procedures governing case file reviews to ensure that applications to the FISC regarding U.S. persons are accurate and complete.

Section 207. Requirement for justification of underlying criminal offense in certain applications.

Section 207 requires the U.S. government, when applying for a probable cause order to conduct electronic surveillance or physical search of a U.S. person alleged to be acting as an agent of a foreign power, to justify its belief that the respective U.S. person is in violation of or about to violate U.S. criminal law.

Section 208. Modification to duration of approved period under certain orders for non-United States persons.

Section 208 modifies to one year the period of time that the U.S. government can, under a probable cause order from the FISC, conduct electronic surveillance or physical search of a non-U.S. person.

TITLE III—FOREIGN INTELLIGENCE SURVEILLANCE COURT AND FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

Section 301. Designation of counsel to scrutinize applications for United States persons.

Section 301 requires a FISC judge to designate an attorney to scrutinize a U.S. government application to conduct electronic surveillance of a U.S. person, and to provide a written analysis to the judge regarding (1) the sufficiency of the government's evidence that the judge will use to make the determination whether there is probable cause to believe the U.S. person is a foreign power or agent of a foreign power; (2) any material weaknesses, flaws, or other concerns in the application; and (3) a recommendation as to whether the judge should approve, deny, or require the government to supplement or otherwise modify the application.

Section 302. Requirement for transcripts of proceedings.

Section 302 requires that all hearings before the FISC or the Foreign Intelligence Surveillance Court of Review (FISC–R) be transcribed and stored.

Section 303. Requirement for notification to Congress of certain transcripts.

Section 303 requires notification to the congressional intelligence and judiciary committees when a transcript is produced from any proceeding before the FISC or FISC–R. Section 303 also provides that if either committee requests to review an existing transcript, the Attorney General shall facilitate that request within three business days.

Section 304. Judicial consistency for extensions.

Section 304 requires that, to the extent practicable and absent exigent circumstances, the FISC judge who originally issued a probable cause order authorizing electronic surveillance regarding a U.S. person shall be the same judge who decides whether to grant or deny an application to extend that order.

Section 305. Mandatory appointment of amicus curiae in judicial review of annual section 702 certifications and procedures.

Section 305 requires the FISC to appoint amicus curiae to assist in considering any Section 702 certification or related procedures submitted for court review, unless the FISC issues a finding that such appointment is not appropriate or is likely to result in undue delay. Section 305 also requires that the FISC, when appointing amicus under this requirement, shall to the maximum extent practicable appoint an individual who possesses expertise in both privacy and civil liberties and intelligence collection. Section 305 further requires the FISC to issue an order approving or not approving the government's continued use of Section 702 within 60 days and authorizes the FISC to extend that 60-day deadline only if the FISC issues an order finding that extraordinary circumstances necessitate additional time for review and that such an extension is consistent with national security.

TITLE IV—FISA PENALTIES

Section 401. Removal or suspension of federal officers for misconduct before Foreign Intelligence Surveillance Court.

Section 401 mandates disciplinary action, including removal or suspension without pay, for any employee or officer of the U.S. government who engages in intentional misconduct with respect to proceedings before the FISC or FISC–R.

Section 402. Penalties for unauthorized disclosure of application for electronic surveillance.

Section 402 adds a new criminal offense under FISA for the knowing and willful disclosure or use of a FISA electronic surveillance application, in whole or in part, in any way that prejudices the safety or interest of the United States or benefits any foreign government to the United States' detriment.

Section 403. Increased criminal penalties for offense under FISA.

Section 403 amends the criminal penalties in FISA to provide that a person who is found guilty of a criminal offense under FISA is punishable by imprisonment of not more than 10 years and/or a fine under Title 18 of the United States Code, which can be up to $250,000.

Section 404. Criminal penalties for unauthorized disclosure of certain incidentally collected United States person information.

Section 404 adds a new criminal offense for the knowing and willful disclosure or use of the classified contents of a communication acquired under Section 702 to which a known United States person is a party, in any manner that prejudices the safety or interest of the United States or benefits any foreign government to the United States' detriment. Section 404 further provides that a person who is found guilty of this offense is punishable by imprisonment of not more than 8 years and/or a fine under Title 18 of the United States Code, which can be up to $250,000.

Section 405. Contempts constituting crimes.

Section 405 amends the criminal code to include the FISC and FISC–R for purposes of crimes constituting contempt of court.

Section 406. Sentencing enhancement for false declarations before FISC.

Section 406 amends the criminal code to include a sentencing enhancement with imprisonment of up to 10 years for knowingly making a false material declaration before the FISC or FISC–R.

Section 407. Annual reporting on disciplinary actions by Federal Bureau of Investigation.

Section 407 requires the FBI Director to annually submit a report to the congressional intelligence and judiciary committees that describes the accountability actions taken by the FBI in the preceding 12-month period for noncompliant querying of Section 702 information, including ongoing personnel investigations and any related adverse personnel actions taken.

TITLE V—REPORTS AND OTHER MATTERS

Section 501. Inclusion of counternarcotics in definition of foreign intelligence.

Section 501 amends the definition of "foreign intelligence information" in FISA to include information that relates to the "international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or any controlled substance designated by the Controlled Substances Act (21 U.S.C. 801 et seq.), or precursors of the aforementioned," to authorize the U.S. government to seek, and for the FISC to approve, the creation of a certification under Section 702 focused on international drug production, distribution, and financing, to include the foreign production, distribution, and financing of fentanyl.

Section 502. Revocation of statutory reporting exemption and additional reporting requirement for Federal Bureau of Investigation.

Section 502 repeals language that exempts the FBI from having to publicly report certain information on U.S. person queries. Section 502 requires the FBI Director to annually report to the congressional intelligence and judiciary committees on the number of U.S. person queries conducted, the number of batch queries conducted, the number of queries conducted by the FBI solely to retrieve evidence of a crime, an estimate of the number of U.S. person queries conducted to protect that U.S. person, and an estimate of the number of U.S. person queries conducted where that person is currently under FBI investigation. Section 502 further requires this report be made public, subject to a declassification review.

Section 503. Notification to Congress of certain unauthorized disclosures.

Section 503 requires the Director of National Intelligence to notify the congressional intelligence committees within 7 days of becoming aware of a significant unauthorized disclosure or compromise of Section 702-acquired information.

Section 504. Definition of electronic communication service provider.

Section 504 modifies the definition of "electronic communication service provider" to account for technological changes in transmitting and storing such communications and to ensure that foreign intelligence information can continue to be collected under Section 702 in a manner consistent with congressional intent.

Section 505. Vetting of non-United States persons.

Section 505 ensures that, consistent with the framework approved by the FISC, all foreign nationals seeking to come to the United States for any purpose or period of time are vetted using Section 702 information to ensure they do not pose a terrorism or other national security threat.

Section 506. Accountability measures for executive leadership of Federal Bureau of Investigation.

Section 506 requires the FBI Director to establish measures to hold FBI executive leaders accountable for FISA noncompliance in their field office or headquarters component, to include potentially withholding a promotion or compensation from any FBI executive leader who oversees a field office or headquarters component which has underperformed with respect to FISA compliance. Section 506 also requires the FBI Director to regularly brief Congress on adverse personnel actions taken pursuant to these measures.

Section 507. Report on technology needed for near-real time monitoring of Federal Bureau of Investigation compliance.

Section 507 requires the Director of National Intelligence, in coordination with the National Security Agency and FBI, to study technological enhancements that would enable the FBI to conduct "near real-time" monitoring of compliance with the court-approved querying and other procedures under Section 702. Section 507 requires the submission of the study to the congressional intelligence and judiciary committees within one year of enactment.

Section 508. Inspector General report on Federal Bureau of Investigation querying practices.

Section 508 requires the Department of Justice Inspector General to prepare a comprehensive report on the FBI's querying compliance under Section 702, with an emphasis on U.S. person query compliance, and the FBI's implementation of the various querying-related reforms required by this Act.

Section 509. Sense of Congress on the targeted collection of United States person information.

Section 509 expresses the Sense of Congress that Section 702 has always prohibited, and continues to prohibit, the intelligence community from targeting a U.S. person for collection of foreign intelligence.

Section 510. FISA Reform Commission.

Section 510 establishes a "FISA Reform Commission" to recommend additional reforms to FISA. Commission members include the Principal Deputy Director of National Intelligence, the Deputy Attorney General, the Deputy Secretary of Defense, the Deputy Secretary of State, the Privacy and Civil Liberties Oversight Board Chair, Senate and House Members, as well as qualified, congressionally-appointed non-Members. The congressionally-appointed non-Members will be appointed by their respective leadership in consultation with the intelligence committees and the judiciary committees. The Majority and Minority sides of each chamber have equal representation.

Section 511. Extension of certain authorities; sunset.

Section 511 reauthorizes FISA Title VII, including Section 702, until December 31, 2031.

Section 512. Severability; applicability date.

Section 512 provides that if any provision of this Act is held invalid by the courts, the validity of the remainder of the Act shall not be affected. Section 512 further provides that certain amendments made to Section 702 by this Act shall apply with respect to Section 702 certifications and procedures submitted by the U.S. government after January 1, 2024.

PURPOSE AND SUMMARY OF THE BILL

The purpose of H.R. 6611 is to amend the Foreign Intelligence Surveillance Act of 1978.

BACKGROUND AND NEED FOR LEGISLATION

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.[1] 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."[2] 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.[3] The Committee concluded that "intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."[4]

The Church Committee issued 96 recommendations, both legislative and regulatory, "to place intelligence activities within the constitutional scheme for controlling government power."[5] In response to the Church Committee's findings, the Foreign Intelligence Surveillance Act (FISA) was carefully designed to establish safeguards on intelligence operations regarding the collection of foreign intelligence.[6] 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

[1] S. Res. 21, 94th Cong. (Jan. 1975).

[2] S. Select Comm. to Study Gov't Operations with Respect to Intel. Activities, S. Rep. No. 94–755 (1976), at Book I, p. III.

[3] *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).

[4] S. Select Comm. to Study Gov't Operations with Respect to Intel. Activities, S. Rep. No. 94–755 (1976), at Book II, p. 289.

[5] 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).

[6] 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.").

of foreign powers or their agents."[7] When the Court declined to comment on the exact type of protections that should be afforded to foreign powers or their agents, Congress stepped in to provide a constitutional legal framework.[8] On October 1978, President Jimmy Carter signed FISA into law.[9] FISA has been amended several times over the years, either expanding or limiting its scope.[10]

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.[11] 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.[12]

Prior to 9/11, the intelligence community "struggled to retrieve and share pertinent information that was being communicated among terrorists using the rapidly evolving technology of the internet and cell phones."[13] Had such information been more readily available to our intelligence community, 9/11 might have been prevented.[14]

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.[15] One of these was the FISA Amendments Act (FAA), which included Section 702.[16] 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."[17]

Section 702 has been reauthorized by Congress twice. It was first reauthorized in 2012 by President Barack Obama and a second time in 2018 by President Donald Trump.[18] Section 702 is set to expire on December 31, 2023, if not reauthorized.

---

[7] *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).

[8] *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).

[9] BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, *The Foreign Intelligence Surveillance Act of 1978* (last visited Sept. 18, 2023).

[10] *Id.*

[11] THE 9/11 MEMORIAL & MUSEUM, *9/11 FAQs* (last visited Aug. 16, 2023).

[12] The 9/11 Commission Report (2004), at 263.

[13] 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).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] James Petrila, *A Brief History of Programmatic Collection Pre-Section 702*, LAWFARE (Apr. 12, 2023).

Recent FBI Abuses

In the past, the Inspector General of the Department of Justice (DOJ) has noted the Federal Bureau of Investigation (FBI) "fell far short" of compliance with FISA.[19] These shortcomings have continued. In May 2023, the intelligence community made publicly available an April 2022 Foreign Intelligence Surveillance Court (FISC) Memorandum Opinion and Order (Order) detailing "significant" querying violations by the FBI.[20] Most of these violations occurred before the FBI implemented corrective reforms to its querying procedures.[21] 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."[22] However, the DOJ National Security Division (NSD), in an audit of that query, found that "only eight identifiers used in the query had sufficient ties to foreign influence activities to comply with the querying standard."[23]

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.[24] Now, FBI personnel are required to affirmatively "opt-in" before they query the Section 702 database.[25] 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.[26]

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."[27] The Court

---

[19] *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.").

[20] FISA CT. *re* Section 702 2021 Certification (Apr. 21, 2022), at 26.

[21] *Id.*

[22] *Id.* at 29.

[23] *Id.*

[24] Press Release, *FBI Releases FISA Query Guidance,* FED. BUREAU OF INVESTIGATION (Apr. 24, 2023).

[25] *Id.*

[26] U.S. DEP'T OF JUSTICE, *Recent Efforts to Strengthen FISA Compliance* (Feb. 28, 2023).

[27] FISA CT. *re* Section 702 2021 Certification (Apr. 21, 2022), at 49.

noted that preliminary indications showed "that some of these measures are having the desired effect." [28]

FBI Abuses in Title I

FISA abuses are not limited to Section 702, which is why this bipartisan legislation reforms other areas of FISA. Title I of FISA, a different legal authority than Section 702, has also been the victim of significant abuse as was apparent in the FBI counterintelligence operation, codenamed Crossfire Hurricane.

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.[29] In particular, the DOJ OIG found "so many basic and fundamental errors," including "at least 17 significant errors or omissions" in the Crossfire Hurricane FISA applications.[30]

Special Counsel John Durham similarly found "unsettling" behavior by FBI Crossfire Hurricane investigators regarding the Crossfire Hurricane FISA applications.[31] 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 ade-

---

[28] *Id.*

[29] *See generally,* Horowitz Report and Durham Report.

[30] Horowitz Report, at vii–xii.

[31] 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.").

quately 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.[32]

The Durham Report did not recommend any wholesale changes to the guidelines and policies that the Department and the FBI currently have in place.[33] 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 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."[34]

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."[35] 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."[36] Durham recommended that the Department "seriously consider" Baker's proposal.[37]

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, 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.

[32] *Id.* at 17–8.
[33] *Id.* at 18.
[34] *Id.* at 18–9.
[35] *Id.* at 306.
[36] *Id.*
[37] *Id.*

- 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.
    - 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.[38]

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.[39] 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.[40]
- 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.[41] 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 que-

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

ries—not just those that would result in 100 or more queries.[42] At the time, FBI IT professionals were working to redesign the user interface to accommodate this reform.[43]

- 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.[44]
- 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.[45]
- 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.[46]

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 Reforms," issued to its workforce.[47] This new procedure addresses

---

[42] 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).

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] U.S. DEP'T OF JUSTICE, *Recent Efforts to Strengthen FISA Compliance* (Feb. 28, 2023).

[47] 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 query incidents involving intentional misconduct, reckless behavior, and negligence.[48] 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.[49]

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.[50]

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 compensation.[51] Field office heads are required to monitor compliance by convening at least two semi-annual meetings to assess personnel performance in a number of FISA compliance areas.[52]

The Need for FISA Reform: Strengthening FISA for the Future

Reforms needed for 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. Title VII 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 Director of the FBI must issue minimum accountability standards for noncompliant querying of information 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 a U.S. person's communication if incidentally 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 que-

---

FBI Deputy Director Highlights Bureau's New FISA Query Accountability Procedures (June 13, 2023).

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

ries. 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 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 of information acquired under Section 702 conducted by the FBI within 6 months of such query. To allow for greater congressional oversight, the FBI should be required to 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 the definition of "foreign intelligence" in Section 101 of the law to expand the ability of the National Security Agency to use FISA to target international drug trafficking operations, including those distributing fentanyl and precursor chemicals, 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 foreign nationals seeking to come to the United States for terrorism and other national security threats.

The protection of civil rights and liberties is critically important. To instill confidence that U.S. person queries should only be conducted to retrieve foreign intelligence information, the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, and National Counterterrorism Center (NCTC) should be statutorily 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.

Reforms needed for other FISA authorities, including 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 anyone who engages in intentional misconduct before the FISC.

The electronic surveillance application process itself needs reform. For example, the government should be prohibited from utilizing uncorroborated political opposition research to obtain a FISA surveillance application. In addition, there should be a statutory requirement that FISA applications be accompanied by a sworn statement of the facts, to allow criminal accountability for any government applicant who lies to the FISC. Leaks to the media are also problematic and have the ability to cause particular harm. Due to this, the leaking of any FISA surveillance application, including by the FBI or DOJ, is deserved to be punished with enhanced criminal penalties.

Reforms needed for 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 statutory 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, 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.

COMMITTEE ACTION

H.R. 6611 was introduced on December 6, 2023, by Representative Michael Turner (R–OH)and Representative Jim Himes (D–CT). The bill was referred to the House—Intelligence (Permanent Select); Judiciary. On December 7, 2023, the Select Committee on Intelligence met to consider the bill. The bill was adopted and ordered favorably reported to the House of Representatives by voice vote.

Hearings

For the purposes of clause 3(c)(6) of House rule XIII, the following hearings and events was used to develop or consider this measure: On March 9, 2023 The Committee held an open hearing Titled "Worldwide Threats," which in great part was a kickoff discussion regarding the need to reform and reauthorize FISA. Subsequently the Committee held over 30 open and closed events and discussions directly related to the need to reform and reauthorize FISA. All of these led to the introduction of H.R. 6611.

Committee Oversight Findings and Recommendations

Regarding clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the oversight findings and recommendations are reflected in the descriptive portion of the report.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

As required by clause 3(c)(4) of rule XIII, the general performance goals and objectives of H.R. 6611 are to amend the Foreign Intelligence Surveillance Act of 1978 so that the nation's national security is made more efficient and effective. The Act and the oversight findings and recommendations in the descriptive portion of the report reflect in detail the Committee's specific performance goals and objectives.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

DUPLICATION OF EXISTING PROGRAMS

This bill does not establish or reauthorize a program of the federal government known to be duplicative of another program.

FEDERAL ADVISORY COMMITTEE ACT STATEMENT

The Act does not establish or authorize the establishment of an advisory committee within the definition of section 5(b) of the appendix to title 5, United States Code.

EARMARK STATEMENT

This bill does not contain any Congressional earmarks, limited tax benefits, or limited tariff benefits as defined under clause 9(e), 9(f), and 9(g) of rule XXI of the Rules of the House of Representatives.

UNFUNDED MANDATES REFORM ACT STATEMENT

H,R. 6611 does not contain any unfunded mandates pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION OF STATE, LOCAL, OR TRIBAL LAW

Any preemptive effect of this bill over state, local, or tribal law is intended to be consistent with the bill's purposes and text and the Supremacy Clause of Article VI of the U.S. Constitution.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Cost of Legislation and the Congressional Budget Act. With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) and clause 3(d) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, on December 7, 2023, the Committee transmitted H.R. 6611 to the Congressional Budget Office and requested an estimate of the costs incurred in carrying out the bill, including any federal mandates. Pursuant to clause 3(d)(1) of House rule XIII, the Committee adopts as its own the cost estimate prepared

by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

* * * * * * *

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 101. As used in this title:

(a) "Foreign power" means—

(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 United States 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 therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) "Agent of a foreign power" means—

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United

States, when the circumstances indicate 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;

(C) engages in international terrorism or activities in preparation therefore;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to 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;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) 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; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that—

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they

are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power**[**; or**]***;*

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(D) international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or any controlled substance designated by the Controlled Substances Act (21 U.S.C. 801 et seq.), or precursors of any aforementioned; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if

both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

(h) "Minimization procedures", with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), 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, as defined in subsection (a) (1), (2), or (3).

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communications while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communications or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(p) "Weapon of mass destruction" means—

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

* * * * * * *

DESIGNATION OF JUDGES

SEC. 103. (a)(1) 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 anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any

judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 702(i), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall provide for the record a written statement of each reason 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.

(c) Proceedings under this Act shall be conducted as expeditiously as possible*, and hearings shall be transcribed*. The record of proceedings under this Act, including applications made*, transcriptions of hearings,* 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. *Transcriptions and any related records, including testimony and affidavits, shall be stored in a file associated with the relevant application or order.*

(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

(e)(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have juris-

diction to review petitions filed pursuant to section 501(f)(1) or 702(h)(4).

(2) Not later than 60 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 501(f)(1) or 702(h)(4) by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.

(g)(1) The courts established pursuant to subsections (a) and (b) may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this Act.

(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:

(A) All of the judges on the court established pursuant to subsection (a).

(B) All of the judges on the court of review established pursuant to subsection (b).

(C) The Chief Justice of the United States.

(D) The Committee on the Judiciary of the Senate.

(E) The Select Committee on Intelligence of the Senate.

(F) The Committee on the Judiciary of the House of Representatives.

(G) The Permanent Select Committee on Intelligence of the House of Representatives.

(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(h) Nothing in this Act shall be construed to reduce or contravene the inherent authority of a court established under this section to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.

(i) AMICUS CURIAE.—

(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after the enactment of this subsection, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges

may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

(2) AUTHORIZATION.—[A court established]

(A) IN GENERAL.—A court established under subsection (a) or (b), consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

[(A)] *(i)* shall [appoint an individual who has] *appoint one or more individuals who have* been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate[; and]*;*

[(B)] *(ii)* may [appoint an individual or organization] *appoint one or more individuals or organizations* to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organization leave to file an amicus curiae brief[.]*; and*

(iii) shall appoint one or more individuals who have been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any certification or procedures submitted for review pursuant to section 702, including any amendments to such certifications or procedures, if the court established under subsection (a) has not appointed an individual under clause (i) or (ii), unless the court issues a finding that such appointment is not appropriate or is likely to result in undue delay.

(B) EXPERTISE.—In appointing one or more individuals under subparagraph (A)(iii), the court shall, to the maximum extent practicable, appoint an individual who possesses expertise in both privacy and civil liberties and intelligence collection.

(C) TIMING.—In the event that the court appoints one or more individuals or organizations pursuant to this paragraph to assist such court in a proceeding under section 702, notwithstanding subsection (j)(1)(B) of such section, the court shall issue an order pursuant to subsection (j)(3) of such section as expeditiously as possible consistent with subsection (k)(1) of such section, but in no event later than 60 days after the date on which such certification, procedures, or amendments are submitted for the court's review, or later than 60 days after the court has issued an order appointing one or more individuals pursuant to this paragraph, whichever is earlier, unless a judge of that court issues an order finding that extraordinary circumstances necessitate additional time for review and that such extension of time is consistent with the national security.

(3) QUALIFICATIONS OF AMICUS CURIAE.—

(A) EXPERTISE.—Individuals designated under paragraph (1) shall be persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to a court established under subsection (a) or (b).

(B) SECURITY CLEARANCE.—Individuals designated pursuant to paragraph (1) shall be persons who are determined to be eligible for access to classified information necessary to participate in matters before the courts. Amicus curiae appointed by the court pursuant to paragraph (2) shall be persons who are determined to be eligible for access to classified information, if such access is necessary to participate in the matters in which they may be appointed.

(4) DUTIES.—If a court established under subsection (a) or (b) appoints an amicus curiae under **[**paragraph (2)(A)**]** *paragraph (2)*, the amicus curiae shall **[**provide to the court, as appropriate**]**—

(A) be limited to addressing the specific issues identified by the court; and

(B) provide to the court, as appropriate—

[(A)**]** *(i)* legal arguments that advance the protection of individual privacy and civil liberties *of United States persons*;

[(B)**]** *(ii)* information related to intelligence collection or communications technology; or

[(C)**]** *(iii)* legal arguments or information regarding any other area relevant to the issue presented to the court.

(5) ASSISTANCE.—An amicus curiae appointed under paragraph (2)(A) may request that the court designate or appoint additional amici curiae pursuant to paragraph (1) or paragraph (2), to be available to assist the amicus curiae.

(6) ACCESS TO INFORMATION.—

(A) IN GENERAL.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

(i) shall have access to any legal precedent, application, certification, petition, motion, or such other materials that the court determines are relevant to the duties of the amicus curiae; and

(ii) may, if the court determines that it is relevant to the duties of the amicus curiae, consult with any other individuals designated pursuant to paragraph (1) regarding information relevant to any assigned proceeding.

(B) BRIEFINGS.—The Attorney General may periodically brief or provide relevant materials to individuals designated pursuant to paragraph (1) regarding constructions and interpretations of this Act and legal, technological, and other issues related to actions authorized by this Act.

(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or pro-

ceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States.

(D) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Government to provide information to an amicus curiae appointed by the court that is privileged from disclosure.

(7) NOTIFICATION.—A presiding judge of a court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (2).

(8) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a nonreimbursable basis) the assistance of the executive branch in the implementation of this subsection.

(9) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support for an individual designated to serve as amicus curiae under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

(10) RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

(11) COMPENSATION.—Notwithstanding any other provision of law, a court established under subsection (a) or (b) may compensate an amicus curiae appointed under paragraph (2) for assistance provided under such paragraph as the court considers appropriate and at such rate as the court considers appropriate.

(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(1), or any other person, to provide briefing or other assistance.

(l) DESIGNATION OF COUNSEL FOR CERTAIN APPLICATIONS.—To assist the court in the consideration of any application for an order pursuant to section 104 that targets a United States person, the presiding judge designated under subsection (b) shall appoint one or more attorneys to review such applications, and provide a written analysis to the judge considering the application, of—

(1) the sufficiency of the evidence used to make the probable cause determination under section 105(a)(2);

(2) any material weaknesses, flaws, or other concerns in the application; and

(3) a recommendation as to the following, which the judge shall consider during a proceeding on the application, as appropriate—

(A) that the application should be approved, denied, or modified;

(B) that the Government should supply additional information in connection with such application; or

(C) that any requirements or conditions should be imposed on the Government for the approval of such application.

(m) REMOVAL OR SUSPENSION OF FEDERAL OFFICERS FOR MISCONDUCT BEFORE COURTS.—An officer or employee of the United States Government who engages in intentional misconduct with respect to proceedings before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review shall be subject to appropriate adverse actions, including, as appropriate, suspension without pay or removal.

APPLICATION FOR AN ORDER

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) **[**a statement of**]** *a sworn statement of* the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power*, and, in the case of a target that is a United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or will occur*; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e)**[**; and**]***;*

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques**[**;**]***; and*

(F) that none of the information included in the statement described in paragraph (3) was solely produced by, derived from information produced by, or obtained using the funds of, a political organization (as such term is defined in section 527 of the Internal Revenue Code of 1986) on the opponent of a candidate in an election for Federal, State, or local office, unless—

(i) the political organization is clearly identified in the body of the statement described in paragraph (3);

(ii) the information has been corroborated; and

(iii) the investigative techniques used to corroborate the information are clearly identified in the body of the statement described in paragraph (3); and

(G) that none of the information included in the statement described in paragraph (3) is solely attributable to or derived from the content of a media source unless the statement includes a clear identification of each author of that content, and, where applicable, the publisher of that content;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application**[**; and**]***;*

(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of

the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter**[**.**]***; and*

(10) with respect to a target who is a United States person, a statement summarizing the investigative techniques carried out before making the application;

(11) in the case of an application for an extension of an order under this title for a surveillance targeted against a United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information; and

(12) a certification by the applicant or declarant that, to the best knowledge of the applicant or declarant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) 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

(B) otherwise raise doubts with respect to the findings required under section 105(a).

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

(d)(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2).

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sen-

tence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

ISSUANCE OF AN ORDER

SEC. 105. (a) Upon an application made pursuant to section 104, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States 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; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(4) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

(b) In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c)(1) SPECIFICATIONS.—An order approving an electronic surveillance under this section shall specify—

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3);

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) SPECIAL DIRECTIONS FOR CERTAIN ORDERS.—An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d)(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted [against a foreign power, as defined in section 101(a), (1), (2), or (3),] *against a foreign power* for the period specified in the application or for one year, whichever is less, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for [120 days] *one year*, whichever is less.

[(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this Act for a surveillance targeted against a foreign power, a defined in paragraph (5), (6), or (7) of section 101(a), or against a foreign power as defined in section 101(a)(4) that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.]

[(3)] *(2)* At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

[(4)] *(3)* A denial of the application made under section 104 may be reviewed as provided in section 103.

(5) An extension of an order issued under this title for surveillance targeted against a United States person, to the extent practicable and absent exigent circumstances, shall be granted or denied by the same judge who issued the original order.

(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—

(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted.

(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e).

(B) An issuance of a court order under this title or title III of this Act.

(C) The Attorney General provides direction that the acquisition be terminated.

(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), or a court order is not obtained under this title or title III of this Act, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.

(g) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine to capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and

(D) *Provided,* That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 705 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(h) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the certification or application.

(i) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

(j) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).

* * * * * * *

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he **[**intentionally**]**—

(1) *intentionally* engages in electronic surveillance under color of law except as authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112**[**; or**]***;*

(2) **[**disclose**]** *intentionally discloses* or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112**[**.**]***; or*

(3) knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit or any foreign government to the detriment of the United States an applica-

tion, in whole or in part, for an order for electronic surveillance under this Act.

(b) DEFENSE.—It is a defense to a prosecution [under subsection (a)] *under paragraph (1) or (2) of subsection (a)* that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) PENALTY.—[An offense in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.] *A person guilty of an offense in this section shall be fined under title 18, imprisoned for not more than 10 years, or both.*

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

* * * * * * *

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

APPLICATION FOR AN ORDER

SEC. 303. (a) Each application for an order approving a physical search under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this title. Each application shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the target of the search, and a description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;

(3) [a statement of] *a sworn statement of* the facts and circumstances relied upon by the applicant to justify the applicant's belief that—

(A) the target of the physical search is a foreign power or an agent of a foreign power*, and, in the case of a target that is a United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or will occur*;

(B) the premises or property to be searched contains foreign intelligence information; and

(C) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e)**[**; and**]***;*

(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D)**[**;**]***; and*

(F) that none of the information included in the statement described in paragraph (3) was solely produced by, derived from information produced by, or obtained using the funds of, a political organization (as such term is defined in section 527 of the Internal Revenue Code of 1986) on the opponent of a candidate in an election for Federal, State, or local office, unless—

(i) the political organization is clearly identified in the body of the statement described in paragraph (3);

(ii) the information has been corroborated; and

(iii) the investigative techniques used to corroborate the information are clearly identified in the body of the statement described in paragraph (3); and

(G) that none of the information included in the statement described in paragraph (3) is solely attributable to or derived from the content of a media source unless the statement includes a clear identification of each author of that content, and, where applicable, the publisher of that content;

(7) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information**[**; and**]***;*

(8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, premises, or property specified in the application, and the action taken on each previous application**[**.**]***;*

(9) in the case of an application for an extension of an order under this title in which the target of the physical search is a

United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information; and

(10) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) 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

(B) otherwise raise doubts with respect to the findings required under section 304(a).

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 304.

(d)(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2).

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications

under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

ISSUANCE OF AN ORDER

SEC. 304. (a) Upon an application made pursuant to section 303, the judge shall enter an ex parte order as requested or as modified approving the physical search if the judge finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

(3) the proposed minimization procedures meet the definition of minimization contained in this title; and

(4) the application which has been filed contains all statements and certifications required by section 303, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 303(a)(6)(E) and any other information furnished under section 303(c).

(b) In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) An order approving a physical search under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the physical search;

(B) the nature and location of each of the premises or property to be searched;

(C) the type of information, material, or property to be seized, altered, or reproduced;

(D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization proce-

dures shall apply to the information acquired by each search; and

(E) the period of time during which physical searches are approved; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search;

(C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the search or the aid furnished that such person wishes to retain;

(D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and

(E) that the Federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.

(d)(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted **[**against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a),**]** *against a foreign power* for the period specified in the application or for one year, whichever is less, and (B) an order under this section for a physical search targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for **[**120 days**]** *one year*, whichever is less.

[(2) Extensions of an order issued under this title may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 101(a), or against a foreign power, as defined in section 101(a)(4), that is not a United States person, or against an agent of a foreign power who is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.**]**

[(3)**]** *(2)* At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—

(A) reasonably determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;

(B) reasonably determines that the factual basis for issuance of an order under this title to approve such physical search exists;

(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization that the decision has been made to employ an emergency physical search; and

(D) makes an application in accordance with this title to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.

(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

(5) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Applications made and orders granted under this title shall be retained for a period of at least 10 years from the date of the application.

* * * * * * *

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

SEC. 402. (a)(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under title I of this Act to conduct the electronic surveillance referred to in that paragraph.

(b) Each application under this section shall be in writing under oath or affirmation to—

(1) a judge of the court established by section 103(a) of this Act; or

(2) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include—

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application;

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution**[**; and**]***;*

(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device**[**.**]***; and*

(4) a certification by the applicant seeking to use the pen register or trap and trace device covered by the application that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) 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

(B) otherwise raise doubts with respect to the findings required under subsection (d).

(d)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section.

(2) An order issued under this section—

(A) shall specify—

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that—

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person—

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 105(b)(2)(C) of this Act, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order—

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)—

(I) the name of the customer or subscriber;

(II) the address of the customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned net-

work address or associated routing or transmission information;

(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;

(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order—

(I) the name of such customer or subscriber;

(II) the address of such customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(3) A denial of the application made under this subsection may be reviewed as provided in section 103.

(e)(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d). The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms of an order issued under this section.

(g) Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) PRIVACY PROCEDURES.—

(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States

persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.

* * * * * * *

TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

SEC. 502. (a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a) of this Act; or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and

(2) shall specify that—

(A) the records concerned are sought for an investigation described in subsection (a); and

(B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.

(E) a statement by the applicant that, to the best knowledge of the applicant, the application fairly reflects all information that might reasonably—

(i) 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

(ii) otherwise raise doubts with respect to the findings required under subsection (c).

(c)(1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfies the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in sub-section (a).

(d)(1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).

(2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section.

TITLE VI—OVERSIGHT

SEC. 601. SEMIANNUAL REPORT OF THE ATTORNEY GENERAL.

(a) REPORT.—On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security, a report setting forth with respect to the preceding 6-month period—

(1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for—

(A) electronic surveillance under section 105;

(B) physical searches under section 304;

(C) pen registers under section 402;

(D) access to records under section 501;

(E) acquisitions under section 703; and

(F) acquisitions under section 704;

(2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C);

(3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;

(4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice; and

(5) copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act.

(b) FREQUENCY.—The first report under this section shall be submitted not later than 6 months after the date of enactment of this section. Subsequent reports under this section shall be submitted semi-annually thereafter.

(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion**[**; and**]***;*

(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a)**[**.**]***; and*

(3) for any hearing, oral argument, or other proceeding before the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review for which a court reporter produces a transcript, not later than 45 days after the government receives the final transcript or the date on which the matter of the hearing, oral argument, or other proceeding is resolved, whichever is later, a notice of the existence of such transcript. Not later than three business days after a committee referred to in subsection (a) requests to review an existing transcript, the Attorney General shall facilitate such request.

(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.

(e) DEFINITIONS.—In this section:

(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term "Foreign Intelligence Surveillance Court" means the court established under section 103(a).

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term "Foreign Intelligence Surveillance Court of Review" means the court established under section 103(b).

* * * * * * *

SEC. 603. ANNUAL REPORTS.

(a) REPORT BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—

(1) REPORT REQUIRED.—The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes—

(A) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

(B) the number of such orders granted under each of those sections;

(C) the number of orders modified under each of those sections;

(D) the number of applications or certifications denied under each of those sections;

(E) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae; and

(F) the number of findings issued under section 103(i) that such appointment is not appropriate and the text of any such findings.

(2) PUBLICATION.—The Director shall make the report required under paragraph (1) publicly available on an Internet Web site, except that the Director shall not make publicly available on an Internet Web site the findings described in subparagraph (F) of paragraph (1).

(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

(1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of—

(A) the number of targets of such orders;

(B) the number of targets of such orders who are known to not be United States persons; and

(C) the number of targets of such orders who are known to be United States persons;

(2) the total number of orders issued pursuant to section 702, including pursuant to subsection (f)(2) of such section, and a good faith estimate of—

(A) the number of targets of such orders;

(B) the number of search terms concerning a known United States person used to retrieve the unminimized contents *(or combined unminimized contents and noncontents information)* of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person;

(C) the number of queries concerning a known United States person of unminimized noncontents information relating to electronic communications or wire communica-

tions obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person;

(D) the number of instances in which the Federal Bureau of Investigation opened, under the Criminal Investigative Division or any successor division, an investigation of a United States person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under such section;

(3) the total number of orders issued pursuant to title IV and a good faith estimate of—

(A) the number of targets of such orders, including—

(i) the number of targets of such orders who are known to not be United States persons; and

(ii) the number of targets of such orders who are known to be United States persons; and

(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

(4) the number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to subsection (c) or (d) of section 106 (including with respect to information acquired from an acquisition conducted under section 702) or subsection (d) or (e) of section 305 of the intent of the government to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or an acquisition conducted pursuant to this Act;

(5) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

(A) the number of targets of such orders; and

(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

(6) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

(A) the number of targets of such orders;

(B) the number of unique identifiers used to communicate information collected pursuant to such orders; and

(C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and

(7) the total number of national security letters issued and the number of requests for information contained within such national security letters.

(c) TIMING.—The annual reports required by subsections (a) and (b) shall be made publicly available during April of each year and include information relating to the previous calendar year.

(d) EXCEPTIONS.—

(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), (5), or (6) of subsection (b) is fewer than 500,

it shall be expressed as a numerical range of "fewer than 500" and shall not be expressed as an individual number.

[(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

[(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs (2)(B), (2)(C), and (6)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation, except with respect to information required under paragraph (2) relating to orders issued under section 702(f)(2).

[(B) ELECTRONIC MAIL ADDRESS AND TELEPHONE NUMBERS.—Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.]

(2) NONAPPLICABILITY TO ELECTRONIC MAIL ADDRESS AND TELEPHONE NUMBERS.—Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.

(3) CERTIFICATION.—

(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subsection (b)(2)(C) cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

(i) certify that conclusion in writing to the Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives;

(ii) report the good faith estimate for those relevant elements able to provide such good faith estimate;

(iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and

(iv) make such certification publicly available on an Internet Web site.

(B) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

(C) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

(e) MANDATORY REPORTING BY DIRECTOR OF FEDERAL BUREAU OF INVESTIGATION.—The Director of the Federal Bureau of Investigation shall annually submit to the Permanent Select Committee on Intelligence and the Committee on Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, a report describing the accountability actions taken by the Federal Bureau of Investigation in the preceding 12-month period for noncompliant querying of information acquired under section 702, to include the number of ongo-

ing personnel investigations, the outcome of any completed personnel investigations and any related adverse personnel actions taken.

(f) MANDATORY REPORTING ON SECTION 702 BY DIRECTOR OF FEDERAL BUREAU OF INVESTIGATION.—

(1) ANNUAL REPORT.—The Director of the Federal Bureau of Investigation shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate a report that includes—

(A) the number of United States person queries by the Federal Bureau of Investigation of unminimized contents or noncontents acquired pursuant to section 702(a);

(B) the number of approved queries using the Federal Bureau of Investigation's batch job technology, or successor tool;

(C) the number of queries using the Federal Bureau of Investigation's batch job technology, or successor tool, conducted by the Federal Bureau of Investigation against information acquired pursuant to section 702(a) for which pre-approval was not obtained due to emergency circumstances;

(D) the number of United States person queries conducted by the Federal Bureau of Investigation of unminimized contents or noncontents acquired pursuant to section 702(a) solely to retrieve evidence of a crime;

(E) a good faith estimate of the number of United States person query terms used by the Federal Bureau of Investigation to conduct queries of unminimized contents or noncontents acquired pursuant to section 702(a) primarily to protect the United States person who is the subject of the query; and

(F) a good faith estimate of the number of United States person query terms used by the Federal Bureau of Investigation to conduct queries of unminimized contents or noncontents acquired pursuant to section 702(a) where the United States person who is the subject of the query is a target or subject of an investigation by the Federal Bureau of Investigation.

(2) PUBLIC AVAILABILITY.—Subject to declassification review by the Attorney General and the Director of National Intelligence, each annual report submitted pursuant to paragraph (1) shall be available to the public during the first April following the calendar year covered by the report.

[(e)**]** *(g)* DEFINITIONS.—In this section:

(1) CONTENTS.—The term "contents" has the meaning given that term under section 2510 of title 18, United States Code.

(2) ELECTRONIC COMMUNICATION.—The term "electronic communication" has the meaning given that term under section 2510 of title 18, United States Code.

(3) NATIONAL SECURITY LETTER.—The term "national security letter" means a request for a report, records, or other information under—

(A) section 2709 of title 18, United States Code;

(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A));

(C) subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)); or

(D) section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

(4) UNITED STATES PERSON.—The term "United States person" means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

(5) WIRE COMMUNICATION.—The term "wire communication" has the meaning given that term under section 2510 of title 18, United States Code.

* * * * * * *

TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

SEC. 701. DEFINITIONS.

(a) IN GENERAL.—In this title, the terms"agent of a foreign power", "Attorney General", "contents", "electronic surveillance", "foreign intelligence information", "foreign power", "person", "United States", and "United States person" have the meanings given such terms in section 101, except as specifically provided in this title.

(b) ADDITIONAL DEFINITIONS.—In this title:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms "Foreign Intelligence Surveillance Court" and "Court" mean the court established under section 103(a).

(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms "Foreign Intelligence Surveillance Court of Review" and "Court of Review" mean the court established under section 103(b).

(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term "electronic communication service provider" means—

(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

(D) any [other communication] service provider who has access to wire or electronic communications either as such

communications are transmitted or as such communications are stored*, or equipment that is being or may be used to transmit or store such communications*; or

(E) an officer, employee, *custodian,* or agent of an entity described in subparagraph (A), (B), (C), or (D).

(5) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (j)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) LIMITATIONS.—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.

(c) CONDUCT OF ACQUISITION.—

(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (h), such certification.

(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (j)(3) prior to the implementation of such authorization.

(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

(A) before the submission of a certification in accordance with subsection (h); or

(B) by amending a certification pursuant to subsection (j)(1)(C) at any time during which judicial review under subsection (j) of such certification is pending.

(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) TARGETING PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

(A) ensure that any acquisition authorized under subsection (a) 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.

(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(e) MINIMIZATION PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(3) PUBLICATION.—The Director of National Intelligence, in consultation with the Attorney General, shall—

(A) conduct a declassification review of any minimization procedures adopted or amended in accordance with paragraph (1); and

(B) consistent with such review, and not later than 180 days after conducting such review, make such minimization procedures publicly available to the greatest extent practicable, which may be in redacted form.

(f) QUERIES.—

(1) PROCEDURES REQUIRED.—

(A) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt querying procedures consistent with the requirements of the fourth amendment to the Constitution of the United States for information collected pursuant to an authorization under subsection (a).

(B) RECORD OF UNITED STATES PERSON QUERY TERMS.—The Attorney General, in consultation with the Director of

National Intelligence, shall ensure that the procedures adopted under subparagraph (A) include a technical procedure whereby a record is kept of each United States person query term used for a query.

(C) JUDICIAL REVIEW.—The procedures adopted in accordance with subparagraph (A) shall be subject to judicial review pursuant to subsection (j).

[(2) ACCESS TO RESULTS OF CERTAIN QUERIES CONDUCTED BY FBI.—

[(A) COURT ORDER REQUIRED FOR FBI REVIEW OF CERTAIN QUERY RESULTS IN CRIMINAL INVESTIGATIONS UNRELATED TO NATIONAL SECURITY.—Except as provided by subparagraph (E), in connection with a predicated criminal investigation opened by the Federal Bureau of Investigation that does not relate to the national security of the United States, the Federal Bureau of Investigation may not access the contents of communications acquired under subsection (a) that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information unless—

[(i) the Federal Bureau of Investigation applies for an order of the Court under subparagraph (C); and

[(ii) the Court enters an order under subparagraph (D) approving such application.

[(B) JURISDICTION.—The Court shall have jurisdiction to review an application and to enter an order approving the access described in subparagraph (A).

[(C) APPLICATION.—Each application for an order under this paragraph shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subparagraph (B). Each application shall require the approval of the Attorney General based upon the finding of the Attorney General that the application satisfies the criteria and requirements of such application, as set forth in this paragraph, and shall include—

[(i) the identity of the Federal officer making the application; and

[(ii) an affidavit or other information containing a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant that the contents of communications described in subparagraph (A) covered by the application would provide evidence of—

[(I) criminal activity;

[(II) contraband, fruits of a crime, or other items illegally possessed by a third party; or

[(III) property designed for use, intended for use, or used in committing a crime.

[(D) ORDER.—Upon an application made pursuant to subparagraph (C), the Court shall enter an order approving the accessing of the contents of communications described in subparagraph (A) covered by the application if the Court finds probable cause to believe that such contents would provide any of the evidence described in subparagraph (C)(ii).

[(E) EXCEPTION.—The requirement for an order of the Court under subparagraph (A) to access the contents of communications described in such subparagraph shall not apply with respect to a query if the Federal Bureau of Investigation determines there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm.

[(F) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed as—

[(i) limiting the authority of the Federal Bureau of Investigation to conduct lawful queries of information acquired under subsection (a);

[(ii) limiting the authority of the Federal Bureau of Investigation to review, without a court order, the results of any query of information acquired under subsection (a) that was reasonably designed to find and extract foreign intelligence information, regardless of whether such foreign intelligence information could also be considered evidence of a crime; or

[(iii) prohibiting or otherwise limiting the ability of the Federal Bureau of Investigation to access the results of queries conducted when evaluating whether to open an assessment or predicated investigation relating to the national security of the United States.]

(2) PROHIBITION ON CONDUCT OF QUERIES THAT ARE SOLELY DESIGNED TO FIND AND EXTRACT EVIDENCE OF A CRIME.—

(A) LIMITS ON AUTHORIZATIONS OF UNITED STATES PERSON QUERIES.—The querying procedures adopted pursuant to paragraph (1) for the Federal Bureau of Investigation shall prohibit queries of information acquired under subsection (a) that are solely designed to find and extract evidence of criminal activity.

(B) EXCEPTIONS.—The restriction under subparagraph (A) shall not apply with respect to a query if—"(i) there is a reasonable belief that such query may retrieve information that could assist in mitigating or eliminating a threat to life or serious bodily harm"; or "(ii) such query is necessary to identify information that must be produced or preserved in connection with a litigation matter or to fulfill discovery obligations in criminal matters under the laws of the United States or any State thereof."

(3) RESTRICTIONS IMPOSED ON FEDERAL BUREAU OF INVESTIGATION.—

(A) LIMITS ON AUTHORIZATIONS OF UNITED STATES PERSON QUERIES.—

(i) IN GENERAL.—Federal Bureau of Investigation personnel must obtain prior approval from a Federal Bureau of Investigation supervisor (or employee of equivalent or greater rank) or attorney who is authorized to access unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) for any query of such unminimized contents or noncontents made using a United States person query term.

(ii) EXCEPTION.—A United States person query to be conducted by the Federal Bureau of Investigation of unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) using a United States person query term may be conducted without obtaining prior approval as specified in clause (i) only if the person conducting the United States person query has a reasonable belief that conducting the query could assist in mitigating or eliminating a threat to life or serious bodily harm.

(B) NOTIFICATION REQUIREMENT FOR CERTAIN FBI QUERIES

(i) REQUIREMENT The Director of the Federal Bureau of Investigation shall promptly notify appropriate congressional leadership of any query conducted by the Federal Bureau of Investigation using a query term that is reasonably believed to be the name or other personally identifying information of a Member of Congress, and shall also notify the member who is the subject of such query.

(ii) APPROPRIATE CONGRESSIONAL LEADERSHIP DEFINED In this subparagraph, the term "appropriate congressional leadership" means the following:

(I) The chairs and ranking minority members of the congressional intelligence committees.

(II) The Speaker and minority leader of the House of Representatives.

(III) The majority and minority leaders of the Senate.

(iii) NATIONAL SECURITY CONSIDERATIONS In submitting a notification under clause (i), the Director shall give due regard to the protection of classified information, sources and methods, and national security.

(iv) WAIVER

(I) IN GENERAL The Director may waive a notification required under clause (i) if the Director determines such notification would impede an ongoing national security or law enforcement investigation.

(II) TERMINATION A waiver under subclause (I) shall terminate on the date the Director determines the relevant notification would not impede the relevant national security or law enforcement investigation or on the date that such investigation ends, whichever is earlier

(C) CONSENT REQUIRED FOR FBI TO CONDUCT CERTAIN QUERIES FOR PURPOSE OF DEFENSIVE BRIEFING

(i) CONSENT REQUIRED The Federal Bureau of Investigation may not, for the exclusive purpose of supplementing the contents of a briefing on the defense against a counterintelligence threat to a Member of Congress, conduct a query using a query term that is the name or restricted personal information (as such term is defined in section 119 of title 18, United States Code) of that member unless—

(I) the member provides consent to the use of the query term; or

(II) the Deputy Director of the Federal Bureau of Investigation determines that exigent circumstances exist sufficient to justify the conduct of such query.

(ii) NOTIFICATION

(I) NOTIFICATION OF CONSENT SOUGHT Not later than three business days after submitting a request for consent from a Member of Congress under clause (i), the Director of the Federal Bureau of Investigation shall notify the appropriate congressional leadership, regardless of whether the member provided such consent.

(II) NOTIFICATION OF EXCEPTION USED Not later than three business days after the conduct of a query under clause (i) without consent on the basis of the existence of exigent circumstances determined under subclause (II) of such clause, the Director of the Federal Bureau of Investigation shall notify the appropriate congressional leadership.

(iii) RULE OF CONSTRUCTION Nothing in this subparagraph may be construed as—

(I) applying to matters outside of the scope of the briefing on the defense against a counterintelligence threat to be provided or supplemented under clause (i); or

(II) limiting the lawful investigative activities of the Federal Bureau of Investigation other than supplementing the contents of a briefing on the defense against a counterintelligence threat to a Member of Congress.

(iv) APPROPRIATE CONGRESSIONAL LEADERSHIP DEFINED In this subparagraph, the term "appropriate congressional leadership" means the following:

(I) The chairs and ranking minority members of the congressional intelligence committees.

(II) The Speaker and minority leader of the House of Representatives.

(III) The majority and minority leaders of the Senate.

(D) QUERYING PROCEDURES APPLICABLE TO FEDERAL BUREAU OF INVESTIGATION For any procedures adopted under paragraph (1) applicable to the Federal Bureau of Investigation, the Attorney General, in consultation with the Director of National Intelligence, shall include the following requirements:

(i) TRAINING A requirement that, prior to conducting any query, personnel of the Federal Bureau of Investigation successfully complete training on the querying procedures on an annual basis.

(ii) ADDITIONAL PRIOR APPROVALS FOR SENSITIVE QUERIES A requirement that, absent exigent circumstances, prior to conducting certain queries, per-

sonnel of the Federal Bureau of Investigation receive approval, at minimum, as follows:

(I) IN GENERAL

(aa) Approval from the Deputy Director of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States elected official, an appointee of the President or a State governor, a United States political candidate, a United States political organization or a United States person prominent in such organization, or a United States media organization or a United States person who is a member of such organization.

(bb) Approval from an attorney of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization.

(cc) Approval from an attorney of the Federal Bureau of Investigation if such conduct involves batch job technology (or successor tool).

(II) PROHIBITION ON POLITICAL APPOINTEES WITHIN THE PROCESS TO APPROVE FEDERAL BUREAU OF INVESTIGATION QUERIES The procedures shall prohibit any political personnel, such as those classified by the Office of Personnel Management as Presidential Appointment with Senate Confirmation, Presidential Appointment (without Senate Confirmation), Noncareer Senior Executive Service Appointment, or Schedule C Excepted Appointment, from inclusion in the Federal Bureau of Investigation's prior approval process under subclause (I).

(iii) PRIOR WRITTEN JUSTIFICATION A requirement that, prior to conducting a query using a United States person query term, personnel of the Federal Bureau of Investigation provide a written statement of the specific factual basis to support the reasonable belief that such query meets the standards required by the procedures adopted under paragraph (1). The Federal Bureau of Investigation shall keep a record of each such written statement.

(iv) STORAGE OF CERTAIN CONTENTS AND NONCONTENTS Any system of the Federal Bureau of Investigation that stores unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) together with contents or noncontents obtained through other lawful means shall be configured in a manner that—

(I) requires personnel of the Federal Bureau of Investigation to affirmatively elect to include such unminimized contents or noncontents obtained

through acquisitions authorized under subsection (a) when running a query; or

(II) includes other controls reasonably expected to prevent inadvertent queries of such unminimized contents or noncontents.

(v) WAIVER AUTHORITY FOR FOREIGN INTELLIGENCE SURVEILLANCE COURT If the Foreign Intelligence Surveillance Court finds that the procedures adopted under paragraph (1) include measures that are reasonably expected to result in similar compliance outcomes as the measures specified in clauses (i) through (iv) of this subparagraph, the Foreign Intelligence Surveillance Court may waive one or more of the requirements specified in such clauses.

(4) MINIMUM ACCOUNTABILITY STANDARDS.—The Director of the Federal Bureau of Investigation shall issue minimum accountability standards that set forth escalating consequences for noncompliant querying of United States person terms within the contents of communications that were acquired under this section. Such standards shall include, at minimum, the following:

(A) Zero tolerance for willful misconduct.

(B) Escalating consequences for unintentional noncompliance, including the threshold for mandatory revocation of access to query information acquired under this section.

(C) Consequences for supervisors who oversee users that engage in noncompliant queries.

(5) VETTING OF NON-UNITED STATES PERSONS.—For any procedures for one or more agencies adopted under paragraph (1)(A), the Attorney General, in consultation with the Director of National Intelligence, shall ensure that the procedures enable the vetting of all non-United States persons who are being processed for travel to the United States using terms that do not qualify as United States person query terms under this Act.

[(3)**]** *(6)* DEFINITIONS.—In this subsection:

(A) The term "contents" has the meaning given that term in section 2510(8) of title 18, United States Code.

(B) The term "query" means the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under subsection (a).

(B) NOTIFICATION REQUIREMENT FOR CERTAIN FBI QUERIES.—

(i) REQUIREMENT.—The Director of the Federal Bureau of Investigation shall promptly notify appropriate congressional leadership of any query conducted by the Federal Bureau of Investigation using a query term that is reasonably believed to be the name or other personally identifying information of a Member of Congress, and shall also notify the member who is the subject of such query.

(ii) APPROPRIATE CONGRESSIONAL LEADERSHIP DEFINED.—In this subparagraph, the term "appropriate congressional leadership" means the following:

(I) The chairs and ranking minority members of the congressional intelligence committees.

(II) The Speaker and minority leader of the House of Representatives.

(III) The majority and minority leaders of the Senate.

(iii) NATIONAL SECURITY CONSIDERATIONS.—In submitting a notification under clause (i), the Director shall give due regard to the protection of classified information, sources and methods, and national security.

(iv) WAIVER.—

(I) IN GENERAL.—The Director may waive a notification required under clause (i) if the Director determines such notification would impede an ongoing national security or law enforcement investigation.

(II) TERMINATION.—A waiver under subclause (I) shall terminate on the date the Director determines the relevant notification would not impede the relevant national security or law enforcement investigation or on the date that such investigation ends, whichever is earlier

(C) CONSENT REQUIRED FOR FBI TO CONDUCT CERTAIN QUERIES FOR PURPOSE OF DEFENSIVE BRIEFING.—

(i) CONSENT REQUIRED.—The Federal Bureau of Investigation may not, for the exclusive purpose of supplementing the contents of a briefing on the defense against a counterintelligence threat to a Member of Congress, conduct a query using a query term that is the name or restricted personal information (as such term is defined in section 119 of title 18, United States Code) of that member unless—

(I) the member provides consent to the use of the query term; or

(II) the Deputy Director of the Federal Bureau of Investigation determines that exigent circumstances exist sufficient to justify the conduct of such query.

(ii) NOTIFICATION.—

(I) NOTIFICATION OF CONSENT SOUGHT.—Not later than three business days after submitting a request for consent from a Member of Congress under clause (i), the Director of the Federal Bureau of Investigation shall notify the appropriate congressional leadership, regardless of whether the member provided such consent.

(II) NOTIFICATION OF EXCEPTION USED.—Not later than three business days after the conduct of a query under clause (i) without consent on the basis of the existence of exigent circumstances determined under subclause (II) of such clause, the Director of the Federal Bureau of Investigation shall notify the appropriate congressional leadership.

(iii) RULE OF CONSTRUCTION.—Nothing in this subparagraph may be construed as—

(I) applying to matters outside of the scope of the briefing on the defense against a counterintelligence threat to be provided or supplemented under clause (i); or

(II) limiting the lawful investigative activities of the Federal Bureau of Investigation other than supplementing the contents of a briefing on the defense against a counterintelligence threat to a Member of Congress.

(iv) APPROPRIATE CONGRESSIONAL LEADERSHIP DEFINED.—In this subparagraph, the term "appropriate congressional leadership" means the following:

(I) The chairs and ranking minority members of the congressional intelligence committees.

(II) The Speaker and minority leader of the House of Representatives.

(III) The majority and minority leaders of the Senate.

(D) QUERYING PROCEDURES APPLICABLE TO FEDERAL BUREAU OF INVESTIGATION.—For any procedures adopted under paragraph (1) applicable to the Federal Bureau of Investigation, the Attorney General, in consultation with the Director of National Intelligence, shall include the following requirements:

(i) TRAINING.—A requirement that, prior to conducting any query, personnel of the Federal Bureau of Investigation successfully complete training on the querying procedures on an annual basis.

(ii) ADDITIONAL PRIOR APPROVALS FOR SENSITIVE QUERIES.—A requirement that, absent exigent circumstances, prior to conducting certain queries, personnel of the Federal Bureau of Investigation receive approval, at minimum, as follows:

(I) IN GENERAL.—

(aa) Approval from the Deputy Director of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States elected official, an appointee of the President or a State governor, a United States political candidate, a United States political organization or a United States person prominent in such organization, or a United States media organization or a United States person who is a member of such organization.

(bb) Approval from an attorney of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization.

(cc) Approval from an attorney of the Federal Bureau of Investigation if such conduct

involves batch job technology (or successor tool).

(II) PROHIBITION ON POLITICAL APPOINTEES WITHIN THE PROCESS TO APPROVE FEDERAL BUREAU OF INVESTIGATION QUERIES.—The procedures shall prohibit any political personnel, such as those classified by the Office of Personnel Management as Presidential Appointment with Senate Confirmation, Presidential Appointment (without Senate Confirmation), Noncareer Senior Executive Service Appointment, or Schedule C Excepted Appointment, from inclusion in the Federal Bureau of Investigation's prior approval process under subclause (I).

(iii) PRIOR WRITTEN JUSTIFICATION.—A requirement that, prior to conducting a query using a United States person query term, personnel of the Federal Bureau of Investigation provide a written statement of the specific factual basis to support the reasonable belief that such query meets the standards required by the procedures adopted under paragraph (1). The Federal Bureau of Investigation shall keep a record of each such written statement.

(iv) STORAGE OF CERTAIN CONTENTS AND NONCONTENTS.—Any system of the Federal Bureau of Investigation that stores unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) together with contents or noncontents obtained through other lawful means shall be configured in a manner that—

(I) requires personnel of the Federal Bureau of Investigation to affirmatively elect to include such unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) when running a query; or

(II) includes other controls reasonably expected to prevent inadvertent queries of such unminimized contents or noncontents.

(v) WAIVER AUTHORITY FOR FOREIGN INTELLIGENCE SURVEILLANCE COURT.—If the Foreign Intelligence Surveillance Court finds that the procedures adopted under paragraph (1) include measures that are reasonably expected to result in similar compliance outcomes as the measures specified in clauses (i) through (iv) of this subparagraph, the Foreign Intelligence Surveillance Court may waive one or more of the requirements specified in such clauses.

(g) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this Act.

(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(h) CERTIFICATION.—

(1) IN GENERAL.—

(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) REQUIREMENTS.—A certification made under this subsection shall—

(A) attest that—

(i) there are targeting procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(II) 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;

(ii) the minimization procedures to be used with respect to such acquisition—

(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (g) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include—

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (j)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (j).

(i) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the

acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) CHALLENGING OF DIRECTIVES.—

(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the direc-

tive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) ENFORCEMENT OF DIRECTIVES.—

(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under

seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(j) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

(1) IN GENERAL.—

(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1), and amendments to such certification or such procedures.

(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) REVIEW.—The Court shall review the following:

(A) CERTIFICATION.—A certification submitted in accordance with subsection (h) to determine whether the certification contains all the required elements.

(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) 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.

(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

(D) QUERYING PROCEDURES.—The querying procedures adopted in accordance with subsection (f)(1) to assess whether such procedures comply with the requirements of such subsection.

(3) ORDERS.—

(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (h) contains all the required elements and that the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (h) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d), (e), and (f)(1) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(D) LIMITATION ON USE OF INFORMATION.—

(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the informa-

tion indicates a threat of death or serious bodily harm to any person.

(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.

(4) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) SCHEDULE.—

(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (h) and the procedures adopted in accordance with subsections (d), (e), and (f)(1) at least 30 days prior to the expiration of such authorization.

(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order re-

lated thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(k) JUDICIAL PROCEEDINGS.—

(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(l) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

(1) STANDARDS.—The Foreign Intelligence Surveillance Court 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 Attorney General and the Director of National Intelligence.

(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. 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.

(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(m) ASSESSMENTS REVIEWS, AND REPORTING.—

(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and the guidelines adopted in accordance with subsection (g) and shall submit each assessment to—

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

(A) are authorized to review compliance with the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and the guidelines adopted in accordance with subsection (g);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) ANNUAL REVIEW.—

(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire

the communications of United States persons, and the results of any such assessment.

(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(4) REPORTING OF MATERIAL BREACH.—

(A) IN GENERAL.—The head of each element of the intelligence community involved in the acquisition of abouts communications shall fully and currently inform the Committees on the Judiciary of the House of Representatives and the Senate and the congressional intelligence committees of a material breach.

(B) DEFINITIONS.—In this paragraph:

(i) The term "abouts communication" means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized under subsection (a).

(ii) The term "material breach" means significant noncompliance with applicable law or an order of the Foreign Intelligence Surveillance Court concerning any acquisition of abouts communications.

(n) RESTRICTION ON CERTAIN INFORMATION AVAILABLE TO FEDERAL BUREAU OF INVESTIGATION.—

(1) RESTRICTION.—The Federal Bureau of Investigation may not ingest unminimized information acquired under this section into its analytic repositories unless the targeted person is relevant to an existing, open, predicated full national security investigation by the Federal Bureau of Investigation.

(2) EXCEPTION FOR EXIGENT CIRCUMSTANCES.—Paragraph (1) does not apply if the Director of the National Security Agency decides it is necessary due to exigent circumstances and provides notification within three business days to the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate.

(3) EXCEPTION FOR ASSISTANCE TO OTHER AGENCIES.—Subparagraph (A) does not apply where the Federal Bureau of Investigation has agreed to provide technical, analytical, or linguistic assistance at the request of another federal agency.

SEC. 703. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

(a) JURISDICTION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—

(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

(2) LIMITATION.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

(b) APPLICATION.—

(1) IN GENERAL.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

(A) the identity of the Federal officer making the application;

(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

(C) [a statement of] *a sworn statement of* the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;

(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;

(F) a certification made by the Attorney General or an official specified in section 104(a)(6) that—

(i) the certifying official deems the information sought to be foreign intelligence information;

(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;

(iii) such information cannot reasonably be obtained by normal investigative techniques;

(iv) designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

(v) includes a statement of the basis for the certification that—

(I) the information sought is the type of foreign intelligence information designated; and

(II) such information cannot reasonably be obtained by normal investigative techniques;

(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;

(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;

(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application[; and]*;*

(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application[.]*; and*

(K) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(i) 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

(ii) otherwise raise doubts with respect to the findings required under subsection (c).

(2) OTHER REQUIREMENTS OF THE ATTORNEY GENERAL.—The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(3) OTHER REQUIREMENTS OF THE JUDGE.—The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).

(c) ORDER.—

(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall

enter an ex parte order as requested or as modified by the Court approving the acquisition if the Court finds that—

(A) the application has been made by a Federal officer and approved by the Attorney General;

(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(C) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).

(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) REVIEW.—

(A) LIMITATION ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause under paragraph (1)(B), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the proposed minimization procedures referred to in paragraph (1)(C) do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(D) REVIEW OF CERTIFICATION.—If the judge determines that an application pursuant to subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3),

the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(4) SPECIFICATIONS.—An order approving an acquisition under this subsection shall specify—

(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition;

(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

(E) the period of time during which the acquisition is approved.

(5) DIRECTIVES.—An order approving an acquisition under this subsection shall direct—

(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by the Court, be followed;

(B) if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

(D) if applicable, that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

(6) DURATION.—An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(7) COMPLIANCE.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(d) EMERGENCY AUTHORIZATION.—

(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, if the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and

(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists,

the Attorney General may authorize such acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of a judicial order approving an acquisition under paragraph (1), such acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) USE OF INFORMATION.—If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(e) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

(f) APPEAL.—

(1) APPEAL TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for re-

view of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(g) CONSTRUCTION.—Except as provided in this section, nothing in this Act shall be construed to require an application for a court order for an acquisition that is targeted in accordance with this section at a United States person reasonably believed to be located outside the United States.

SEC. 704. OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

(a) JURISDICTION AND SCOPE.—

(1) JURISDICTION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

(2) SCOPE.—No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this Act.

(3) LIMITATIONS.—

(A) MOVING OR MISIDENTIFIED TARGETS.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

(B) APPLICABILITY.—If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 703, the acquisition may only be conducted if authorized under section 703 or in accordance with another provision of this Act other than this section.

(C) CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

(b) APPLICATION.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application as set forth in this section and shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific United States person who is the target of the acquisition;

(3) **[**a statement of**]** *a sworn statement of* the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

(A) a person reasonably believed to be located outside the United States; and

(B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(4) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;

(5) a certification made by the Attorney General, an official specified in section 104(a)(6), or the head of an element of the intelligence community that—

(A) the certifying official deems the information sought to be foreign intelligence information; and

(B) a significant purpose of the acquisition is to obtain foreign intelligence information;

(6) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application**[**; and**]***;*

(7) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application**[**.**]***; and*

(8) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) 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

(B) otherwise raise doubts with respect to the findings required under subsection (c).

(c) ORDER.—

(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court if the Court finds that—

(A) the application has been made by a Federal officer and approved by the Attorney General;

(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acqui-

sition, there is probable cause to believe that the target is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) REVIEW.—

(A) LIMITATIONS ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(D) SCOPE OF REVIEW OF CERTIFICATION.—If the judge determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such

determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(4) DURATION.—An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(5) COMPLIANCE.—At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the judge may not inquire into the circumstances relating to the conduct of the acquisition.

(d) EMERGENCY AUTHORIZATION.—

(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this section, if the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained, and

(B) the factual basis for the issuance of an order under this section exists,

the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an emergency acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) be followed.

(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of an order under subsection (c), an emergency acquisition under paragraph (1) shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) USE OF INFORMATION.—If an application submitted to the Court pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order with respect to the target of the acquisition is issued under subsection (c), no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or po-

litical subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(e) APPEAL.—

(1) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

* * * * * * *

SEC. 709. PENALTIES FOR UNAUTHORIZED DISCLOSURE.

(a) OFFENSE.—A person is guilty of an offense under this section if that person knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information that contains the contents of any communication acquired under this title to which a known United States person is a party.

(b) PENALTY.—A person guilty of an offense in this section shall be fined under title 18, imprisoned for not more than 8 years, or both.

(c) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

* * * * * * *

TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

SEC. 801. DEFINITIONS.

In this title:

(1) ASSISTANCE.—The term "assistance" means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

(2) CIVIL ACTION.—The term "civil action" includes a covered civil action.

(3) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(4) CONTENTS.—The term "contents" has the meaning given that term in section 101(n).

(5) COVERED CIVIL ACTION.—The term "covered civil action" means a civil action filed in a Federal or State court that—

(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and

(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

(6) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term "electronic communication service provider" means—

(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

(D) any [other communication] service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored*, or equipment that is being or may be used to transmit or store such communications*;

(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or

(F) an officer, employee, *custodian,* or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).

(7) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(8) PERSON.—The term "person" means—

(A) an electronic communication service provider; or

(B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—

(i) an order of the court established under section 103(a) directing such assistance;

(ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code; or

(iii) a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), or 702(h).

(9) STATE.—The term "State" means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United

States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

* * * * * * *

TITLE 18, UNITED STATES CODE

PART I—CRIMES

* * * * * * *

CHAPTER 21—CONTEMPTS

* * * * * * *

§ 402. Contempts constituting crimes

Any person, corporation or association willfully disobeying any lawful writ, process, order, rule, decree, or command of any district court of the United States*, including the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review established by section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803),* or any court of the District of Columbia, by doing any act or thing therein, or thereby forbidden, if the act or thing so done be of such character as to constitute also a criminal offense under any statute of the United States or under the laws of any State in which the act was committed, shall be prosecuted for such contempt as provided in section 3691 of this title and shall be punished by a fine under this title or imprisonment, or both.

Such fine shall be paid to the United States or to the complainant or other party injured by the act constituting the contempt, or may, where more than one is so damaged, be divided or apportioned among them as the court may direct, but in no case shall the fine to be paid to the United States exceed, in case the accused is a natural person, the sum of $1,000, nor shall such imprisonment exceed the term of six months.

This section shall not be construed to relate to contempts committed in the presence of the court, or so near thereto as to obstruct the administration of justice, nor to contempts committed in disobedience of any lawful writ, process, order, rule, decree, or command entered in any suit or action brought or prosecuted in the name of, or on behalf of, the United States, but the same, and all other cases of contempt not specifically embraced in this section may be punished in conformity to the prevailing usages at law.

For purposes of this section, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

* * * * * * *

CHAPTER 79—PERJURY

* * * * * * *

§ 1623. False declarations before grand jury or court

(a) Whoever under oath (or in any declaration, certificate, verification, or statement under penalty of perjury as permitted under section 1746 of title 28, United States Code) in any proceeding before or ancillary to any court or grand jury of the United States knowingly makes any false material declaration or makes or uses any other information, including any book, paper, document, record, recording, or other material, knowing the same to contain any false material declaration, shall be fined under this title or imprisoned not more than five years *or, if such proceedings are before or ancillary to the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review established by section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), imprisoned not more than ten years*, or both.

(b) This section is applicable whether the conduct occurred within or without the United States.

(c) An indictment or information for violation of this section alleging that, in any proceedings before or ancillary to any court or grand jury of the United States, the defendant under oath has knowingly made two or more declarations, which are inconsistent to the degree that one of them is necessarily false, need not specify which declaration is false if—

(1) each declaration was material to the point in question, and

(2) each declaration was made within the period of the statute of limitations for the offense charged under this section.

In any prosecution under this section, the falsity of a declaration set forth in the indictment or information shall be established sufficient for conviction by proof that the defendant while under oath made irreconcilably contradictory declarations material to the point in question in any proceeding before or ancillary to any court or grand jury. It shall be a defense to an indictment or information made pursuant to the first sentence of this subsection that the defendant at the time he made each declaration believed the declaration was true.

(d) Where, in the same continuous court or grand jury proceeding in which a declaration is made, the person making the declaration admits such declaration to be false, such admission shall bar prosecution under this section if, at the time the admission is made, the declaration has not substantially affected the proceeding, or it has not become manifest that such falsity has been or will be exposed.

(e) Proof beyond a reasonable doubt under this section is sufficient for conviction. It shall not be necessary that such proof be made by any particular number of witnesses or by documentary or other type of evidence.

FISA AMENDMENTS ACT OF 2008

* * * * * * *

TITLE IV—OTHER PROVISIONS

* * * * * * *

SEC. 403. REPEALS.

(a) REPEAL OF PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) AMENDMENTS TO FISA.—

(A) IN GENERAL.—Except as provided in section 404, sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(B) TECHNICAL AND CONFORMING AMENDMENTS.—

(i) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C.

(ii) CONFORMING AMENDMENTS.—Except as provided in section 404, section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(I) in paragraph (1), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)"; and

(II) in paragraph (2), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)".

(2) REPORTING REQUIREMENTS.—Except as provided in section 404, section 4 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 555) is repealed.

(3) TRANSITION PROCEDURES.—Except as provided in section 404, subsection (b) of section 6 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556) is repealed.

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective ❲December 31, 2023❳ *December 31, 2031*, title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective ❲December 31, 2023❳ *December 31, 2031*—

(A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;

(B) except as provided in section 404, section 601(a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and

(C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978".

SEC. 404. TRANSITION PROCEDURES.

(a) TRANSITION PROCEDURES FOR PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign In-

telligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

(i) the expiration of such order, authorization, or directive; or

(ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) PROTECTION FROM LIABILITY.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

(A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this

Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;

(iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and

(iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(j)(3) of such Act (as so added) at which time the provisions of that section and of section 702(j)(4) of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON [DECEMBER 31, 2023] *DECEMBER 31, 2031*.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, shall continue to apply until the later of—

(A) the expiration of such order, authorization, or directive; or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(i) of such Act, as added by section 101(a);

(B) section 702(i)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(i) of such Act (as so added);

(C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by sec-

tion 101(c)(2), and sections 702(m) and 707 of such Act, as added by section 101(a) and amended by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), or section 702(m) or 707 of such Act, as added by section 101(a) and amended by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, relating to any acquisition conducted under title VII of such Act, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017 *and the FISA Reform and Reauthorization Act of 2023*, has been included in a review, assessment, or report under such section 601, 702(l), or 707.

(5) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

* * * * * * *

ADDITIONAL VIEWS

H.R. 6611, the FISA Reform and Reauthorization Act of 2023, is the product of extensive oversight by the House Permanent Select Committee on Intelligence. The bill reflects input from Members and outside experts across the political spectrum. In a time of hyper-partisanship, it charts a bipartisan path forward on a topic of unsurpassed national significance—the safety of the American people.

Taken together, the bill's provisions would constitute the most extensive reforms ever made to the Foreign Intelligence Surveillance Act (FISA), while being carefully crafted to preserve the power and efficacy of a law used every day by the intelligence community to collect foreign intelligence, inform policymakers, and protect our country.

The bill reauthorizes FISA Title VII, including Section 702, for eight years. The importance of Section 702 to U.S. intelligence collection and U.S. national security, especially in the current threat environment, cannot be overstated. As the President's Intelligence Advisory Board wrote: "If Congress fails to reauthorize Section 702, history may judge [it] as one of the worst intelligence failures of our time."

It is not hyperbole to say that congressional failure to reauthorize Section 702 would be a catastrophic self-inflicted wound, dramatically reducing our ability to combat threats from adversary nations, terrorists, and drug trafficking organizations; to support U.S. diplomatic efforts on issues ranging from peace negotiations to climate negotiations; to protect U.S. service members and execute the national defense strategy; and to protect our homeland and our people.

At the same time, reauthorization must be accompanied by reform. Accordingly, this bill makes tough, targeted reforms to FISA—to both Section 702 and "traditional FISA"—in order to safeguard the privacy rights and civil liberties of Americans, to address well-documented and unacceptable compliance failures by the FBI, and to prevent future abuses.

For example, the bill:

- prohibits the FBI from conducting queries of Section 702-acquired information that are designed to retrieve evidence of a crime, thus making clear that Section 702 is an instrument to acquire foreign intelligence and not a tool of domestic law enforcement.
- requires an FBI supervisor or FBI attorney (about 550 individuals) to approve every U.S. person query of Section 702 information, thereby reducing the number of FBI personnel authorized to approve U.S. person queries by over 90 percent compared to the status quo.

- mandates that the FBI Deputy Director personally approve certain "sensitive" U.S. person queries, like queries of U.S. elected officials, political candidates, executive branch appointees, and members of the media.
- requires the Department of Justice to audit 100 percent of FBI's U.S. person queries, until the Attorney General certifies to the satisfaction of the Foreign Intelligence Surveillance Court that the FBI's Office of Internal Auditing is fully performing this task.
- prohibits the FBI and other U.S. government agencies from conducting a query to suppress a U.S. person's free expression of political opinions, or to disadvantage or harm that U.S. person based on their ethnicity, race, gender, sexual orientation, or religion.
- mandates that the FBI Director annually publish detailed information about the number and type of FBI U.S. person queries, including queries conducted for defensive purposes, and requires the Department of Justice's Office of the Inspector General to prepare a comprehensive report for Congress and the public regarding the FBI's querying compliance.

In addition, the bill enhances accountability for FBI and other government officials who fail to comply with the laws and rules governing FISA. For instance, the bill:

- requires the FBI Director to hold the Bureau's executive leaders accountable for FISA noncompliance in the field office or headquarters component those leaders oversee, including by withholding promotions or compensation.
- requires the FBI Director to ensure appropriate consequences for Bureau employees who conduct noncompliant U.S. person queries, including zero tolerance for willful misconduct and escalating consequences for unintentional noncompliance.
- creates new criminal and administrative penalties, and increases existing penalties, for government officials who engage in a range of intentional misconduct related to FISA, such as leaking FISA-derived information or making a false declaration before the Foreign Intelligence Surveillance Court.

Furthermore, the bill makes key reforms to strengthen the fairness, independence, and adversarial nature of proceedings held before the Foreign Intelligence Surveillance Court (FISC). For example, the bill:

- requires a FISC judge to appoint amicus curiae ("friend of the court") in the annual Section 702 reauthorization process to ensure Americans' privacy and civil liberties are protected.
- requires a FISC judge, when considering a government application to electronically surveil a U.S. person under traditional FISA, to appoint an attorney to review the application and to advise the judge on the sufficiency of the government's evidence and any deficiencies in the application.
- prohibits the government, when applying for a probable cause order from the FISC to conduct electronic surveillance or a physical search under traditional FISA, from including in its application information that is solely (1) derived from opposi-

tion research on a political candidate or (2) based on media reports.

Finally, the bill modernizes FISA to keep pace with the evolving threat landscape. For example, the bill:

- enhances the government's ability to use Section 702 to collect information on foreign nationals located abroad who are involved in the production, distribution, and financing of illicit drugs, especially fentanyl.
- ensures that, consistent with the strict legal and policy framework already approved by the FISC, foreign nationals seeking to come to the United States for any purpose or period of time are vetted using Section 702 information to ensure they do not pose a terrorism or other national security threat.

I am proud to co-lead this bill and look forward to working with my colleagues in the House and Senate, both Democrat and Republican, to reauthorize and reform this critical national security tool.

JAMES A. HIMES.

ADDITIONAL VIEWS

The reform and reauthorization of FISA 702 is one of the most important tasks that this Committee has, and this will be my second authorization process as a member of the Intelligence Committee.

I want to first thank Chairman Turner, Ranking Member Himes, and my colleagues on the Committee, and also all of the staff, both Republican and Democrat, for their efforts over the last year in investigating the uses and abuses of this authority and proposing reforms.

The process that Chairman Turner and Ranking Member Himes set up has been a thoughtful and earnest one. Over the last year, we have participated in numerous engagements with the intelligence community, the FBI, and others that have the responsibility to use these important tools authorized by law.

Through that process, including as a part of the bipartisan working group, I have come to appreciate the immense value of the FISA 702 authority in protecting Americans and countering our adversaries.

There is no question that this authority is critical for America's national security.

It has saved American lives.

It has informed our diplomats as they negotiate with our adversaries.

Everything I have seen during my time in this committee has led me to believe that FISA 702 should be reauthorized.

But, as they say, the devil is in the details.

Just as I have come to appreciate the importance of FISA 702, I have also come to understand the serious risks that the abuse of such an authority can and has led to in our country.

Under current practice and law, intelligence agencies and the FBI are able to search the 702 database for communications between foreign nationals and U.S. citizens or residents.

This, understandably, raises privacy and civil liberties risks, and while there are many legitimate cases where such searches need to be conducted, it's our responsibility to ensure that this is done in an appropriate manner.

This Committee's bill implements and codifies a number of important reforms to constrain the privacy and civil liberties risks to American citizens, but I am open to more restrictions on when the government can conduct such U.S. person queries in FISA 702, including judicial review of US person queries if structured appropriately.

In addition to what may not be in the bill, I also have serious concerns with certain provisions in the Committee's bill which prevent me from lending my support to it at this time.

The most important is the language in Section 505 which codifies a process to "vet" non-citizens who attempt to enter the United States or wish to enter the United States for immigration, tourism, business, or personal reasons, through the 702 database.

I represent San Antonio, Texas, and I have family who live in the border communities along both sides of the Rio Grande.

My constituents—and those in South Texas—have a very different relationship with the border than most Americans.

We have deep family ties with communities in Mexico that go back generations.

We depend on trade with Mexico to sustain our economies.

Thousands of people cross the border every day to visit family, commute to work, or to simply shop at the malls.

I am increasingly concerned by the rhetoric from many parts of this Congress and from leading public figures and presidential candidates who want to "shut down the border" and to stop those seeking refuge in the United States from attempting to.

Between 2017 and 2021, I spent four years fighting an ever-increasing barrage of the most ill-conceived and malicious policies to harm migrants and border communities, and I am increasingly concerned that we will re-live those experiences again.

I fear that codifying this provision—especially without meaningful safeguards—would give those who capitalize on fear and xenophobia an important tool to pursue their agenda.

I do not believe that this is the intention of the authors of the bill, but we cannot trust that those who will wield these powers that we present to them in the future will not abuse them.

Protecting the civil liberties of Americans against surveillance is personal issue to me.

My mother, a civil rights activist in the 1960s and 70s and even now, was surveilled by the FBI back then as were many of her colleagues in the Mexican-American civil rights movement and those who were in the African American civil rights movement and other political movements.

So, my family knows what it means for the government to turn these powerful tools against it.

It's clear that serious reforms of the FISA 702 authorities are needed.

There are important proposals on reforming the authority being debated in the Senate and, of course, in other Committees in the House of Representatives.

I will remain engaged with my colleagues in this Committee, the Judiciary Committee, and the Senate to come up with a way to reauthorize FISA 702 in a manner that appropriately protects civil liberties and minimizes its potential for abuse regardless of who sits in the oval office.

JOAQUIN CASTRO.

○