114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 114–109
Part 1

UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015

MAY 8, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GOODLATTE, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany H.R. 2048]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 2048) to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

Purpose and Summary

H.R. 2048, the "USA FREEDOM Act of 2015," prohibits bulk collection of records under Section 215 of the USA PATRIOT Act (Section 501 of the Foreign Intelligence Surveillance Act (FISA)), under the FISA Pen Register and Trap and Trace Device statute, and under National Security Letter (NSL) authorities. The Act creates a new program for the targeted collection of telephone metadata, provides greater privacy and civil liberties protections for Americans, expands existing congressional oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA.

Background and Need for the Legislation

In June 2013, Edward Snowden, a former defense contractor and Central Intelligence Agency (CIA) employee, released classified material on top-secret National Security Agency (NSA) data collection programs. On June 5, 2013, it was reported that on April 25, 2013, the Foreign Intelligence Surveillance Court (FISC) granted an order requested by the FBI pursuant to section 215 of the USA PATRIOT Act,[1] which was reauthorized by Congress in 2011 and expires on June 1, 2015. This secondary order compelled Verizon Communications, Inc., on an "ongoing, daily basis," to provide the NSA with "all call detail records or telephony metadata" for communications made via its systems, both within the United States and between the U.S. and other countries.[2] "Telephony metadata" includes the numbers of both parties on a call, unique identifiers, and the time and duration of all calls. The order gave the government the authority to obtain the call detail records or "telephony metadata" for a 3-month period, ending on July 19, 2013.[3]

On March 27, 2014, President Obama announced several changes to the conduct of foreign intelligence activities in response to the unauthorized disclosure of classified information by Edward Snowden. The President announced changes that imposed both a substantive limit on the scope of NSA's access to telephony metadata as well as a procedural limit on when the NSA may access the data in the first place. The substantive limit restricts the results of queries of telephony metadata to two "hops" (a "hop" is a colloquial term for a connection between two telephone numbers). Prior to the President's speech, the program had been authorized to receive query results of up to three "hops."

The procedural limit also requires that the FISC approve queries of telephony metadata on a case-by-case basis and before any query is conducted. Under the bulk metadata collection program, the NSA was permitted to query the data without court approval and based on one of 22 NSA officials' determination that there was a reasonable articulable suspicion (RAS) that the selector is associated with an international terrorist organization. As described by the President, the new framework requires the FISC to approve each selector for use in queries. Such an arrangement was not un-

[1] 50 U.S.C. § 1861 (2012).

[2] *See Verizon forced to hand over telephone data—full court ruling,* THE GUARDIAN, Jun. 5, 2013, *available at* http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[3] *Id.*

precedented. For several months in 2009, the FISC had imposed a similar judicial pre-approval requirement after the government reported violations of the court-ordered privacy protections intended to prevent access to the metadata. This pre-approval requirement was subsequently lifted after the FISC was satisfied that sufficient changes had been made to correct the earlier compliance violations.

At the same time, the President announced that the government should no longer store telephone metadata in bulk; rather, the records should remain at the telephone companies for the length of time such records are stored in the ordinary course of business. Also, the President stated that the court-approved numbers could be used to query the data over a limited period of time without returning to the FISC for approval, the production of records would be ongoing and prospective, and the companies should be compelled by court order to provide technical assistance to ensure that the records can be queried and that results are transmitted to the government in a usable format and in a timely manner.[4]

In the 113th Congress, the House Judiciary Committee conducted aggressive oversight of these programs. In July 2013, the Committee held a public hearing at which testimony was received from officials with the Justice Department, the Office of the Director of National Intelligence, the NSA and the FBI and civil liberties groups. In September 2013, the Committee held a classified hearing where members were afforded the opportunity to further probe these programs with officials from DOJ, ODNI, NSA, and FBI. In February 2014, the Committee held a comprehensive hearing to examine the various recommendations to reform these programs offered by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board. The Committee reported H.R. 3361, the USA FREEDOM Act, with unanimous support. The bill passed the House on May 22, 2014, by a vote of 303–121.

Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[5] FISA provides a variety of authorities for the collection of foreign intelligence information in authorized investigations from sources inside the United States.

The law applied the judicial approval process to certain surveillance activities (almost all of which occur within the United States), but excluded the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets, from FISA's judicial process.[6] Put otherwise, the FISA protections were not extended to foreign communications abroad because the government has the inherent authority to collect such communications without constitutional constraints.

FISA authorizes investigations to obtain foreign intelligence not concerning a U.S. person, investigations to protect against international terrorism, and investigations of clandestine intelligence

---

[4] Press Release, The White House, Office of the Press Secretary, *Statement by the President on the Section 215 Bulk Metadata Program* (Mar. 27, 2014), available at http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

[5] H.R. Rep. No. 95–1283, pt. 1, at 22 (1978).

[6] Prepared Statement of Kenneth L. Weinstein on the Foreign Intelligence Surveillance Act before the House Permanent Select Committee on Intelligence on Sept. 6, 2007.

activities. FISA authorities can be used to target both U.S. and non-U.S. persons, although there are limitations on the use of FISA authorities against U.S. persons.

Title I of FISA governs the use of electronic surveillance if there is probable cause to believe that the target is a foreign power or agent of a foreign power and that the facilities or locations of the surveillance is being used, or about to be used, by a foreign power or agent of a foreign power.[7] Title I provides, however, that no United States person (i.e. citizen or lawful permanent resident) may be considered a foreign power or agent of a foreign power based solely upon First Amendment protected activities.[8] An application for electronic surveillance must specify proposed minimization procedures.

FISA defines electronic surveillance as:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication 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;
>
> (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.[9]

The intent of paragraph (1) of the definition is clear—if the government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA's original scope.[10] The definition also makes clear

---

[7] 50 U.S.C. § 1801 *et seq.* (2012).
[8] *Id.*
[9] 50 U.S.C. § 1801(f) (2012).
[10] *See supra* note 6 at 4.

that the opposite is true—if the government targets someone overseas, it is outside FISA's scope.[11]

Title III of FISA authorizes physical searches based upon probable cause similar to that for Title I electronic surveillance.[12]

Title IV of FISA authorizes the use of pen register and trap and trace devices based upon a certification 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." [13]

Title V of FISA authorizes the production of business records or other tangible things based upon "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence, international terrorism, or espionage investigation]" and an "enumeration of minimization procedures" to be applied. These provisions also include recipient non-disclosure provisions, grounds for recipients to challenge such production or non-disclosure requirements, and government reporting requirements.[14]

Title VII of FISA authorizes the government to acquire foreign intelligence information from sources inside the U.S. to target foreign persons outside the U.S.[15] In 1978, satellite or "radio" technologies carried almost all transoceanic communications. Surveillance of these international communications would only become "electronic surveillance" under FISA if (1) the government intentionally targeted a U.S. person inside the United States, or (2) all of the participants to the conversation were inside the United States.[16] Therefore, in 1978, the government did not have to first acquire a FISA surveillance order to acquire the communications of a foreign target overseas—even if one of the communicants was in the United States.

FISA establishes two courts—the FISC and the U.S. Foreign Intelligence Surveillance Court of Review (FISCR), which are comprised of Federal judges to address applications for FISA court orders.[17]

FISA directs that the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the FISC, which has jurisdiction over applications for and orders approving electronic surveillance, physical searches, pen registers or trap and trace devices, or orders for production of tangible things anywhere within the United States under FISA.

The Chief Justice also publicly designates three U.S. district court or U.S. court of appeals judges who together make up the FISA Court of Review.[18] This court has jurisdiction to review any denial of an order under FISA. If the United States appeals a FISC

---

[11] *Id.*
[12] 50 U.S.C. § 1821 *et seq.* (2012).
[13] 50 U.S.C. § 1841 *et seq.* (2012).
[14] 50 U.S.C. § 1861 *et seq.* (2012).
[15] 50 U.S.C. § 1881 *et seq.* (2012).
[16] *See supra* note 6 at 4–5.
[17] 50 U.S.C. § 1803(a) (2012).
[18] 50 U.S.C. §§ 1803(a), 1822(c) (2012).

denial of an application, the record from the FISC must be transmitted under seal to the Court of Review.

Section 215 of the USA PATRIOT Act expanded the scope of documents that could be sought under a Section 501 FISA court order and amended the standard required before a court order could be issued compelling the production of documents.

In 1976, the Supreme Court held that an individual's bank account records did not fall within the protection of the Fourth Amendment's prohibition on unreasonable searches and seizures.[19] Subsequently, Congress passed laws protecting various types of transactional information, but built in exceptions providing some access to statutorily protected records for counter intelligence purposes. Similar statutory protections were also enacted for electronic communications records and credit bureau records.

As with financial records, these later statutes also included exceptions for access to records relevant to counterintelligence investigations. These exceptions comprise the authority for National Security Letters (NSLs), which can be used to compel the production of certain types of records. In 1998, Congress amended FISA to provide access to certain records that were not available through NSLs.[20] Specifically, it created a mechanism for Federal investigators to compel the production of records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[21] Applications for orders under this section had to be made by FBI agents with a rank of Assistant Special Agent in Charge or higher and investigations could not be conducted solely on the basis of activities protected by the First Amendment.[22]

Under these procedures the FISC would issue an order if the application contained "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."[23] Recipients of an order under this section were required to comply with it, and were also prohibited from disclosing to others that an order had been issued.[24]

In 2001, Section 215 of the USA PATRIOT Act made several changes to the procedures under FISA for obtaining business records.[25] Among these was an expansion of the scope of records that were subject to compulsory production. Prior to enactment of the USA PATRIOT Act, only records from four explicit categories of businesses could be obtained. Section 215 expanded business records to "any tangible things."[26]

In response to concerns that this expanded scope might have a chilling effect on rights protected by the First, Second, and Fourth Amendments, the USA PATRIOT Improvement and Reauthorization Act of 2005 created additional protections for certain "tangible things." Under this amendment, if the records sought were "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, edu-

[19] *U.S. v. Miller*, 425 U.S. 435 (1976).
[20] Intelligence Authorization Act for FY 1999, Pub. L. 105–272, 112 STAT. 2396, tit. VI, § 602 (Oct. 20, 1998).
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] P.L. 107–56, § 215 *codified at* 50 U.S.C. § 1862(a)-(b) (2012).
[26] *Id., codified at* 50 U.S.C. § 1861(a)(1) (2012).

cational records, or medical records containing information that would identify a person," the application has to be approved by one of three high-ranking FBI officers.[27]

Section 215 of the USA PATRIOT ACT also modified the standard that had to be met before an order compelling production of documents could issue from the FISC. Prior to enactment of Section 215, an applicant had to have "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."[28] In contrast, under Section 215, the applicant only needed to "specify that the records concerned [were] sought for a [foreign intelligence investigation.]"[29]

As part of the 2005 reauthorization, Congress further amended FISA procedures for obtaining business records. The applicable standard was again changed to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation.]"[30] Records are presumptively relevant if they pertain to:

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;

Orders issued under Section 215 are accompanied by nondisclosure orders prohibiting the recipients from disclosing that the FBI has sought or obtained any tangible things pursuant to a FISA order. However, the recipient may discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons as permitted by the FBI.[31] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except that attorneys with whom the recipient has consulted do not need to be identified.[32]

The 2005 reauthorization also provided procedures for recipients of Section 215 orders to challenge the judicial review of orders compelling the production of business records.[33] Once a petition for review is submitted by a recipient, a FISC judge must determine whether the petition is frivolous within 72 hours.[34] If the petition is frivolous, it must be denied and the order affirmed.[35] Otherwise the order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[36] Appeals by either

---

[27] Applications for these records could be made only by the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security. This authority cannot be further delegated. *See* 50 U.S.C. § 1861(a)(3) (2012).

[28] *See supra* note 20.

[29] P.L. 107–56, § 215, *codified at* 50 U.S.C. § 1861(b)(2) (2012).

[30] P.L. 109–177, § 106(b) (effective Mar. 9, 2006).

[31] *Id., codified at* 50 U.S.C. § 1861(d)(1) (2012).

[32] *Id., codified at* 50 U.S.C. § 1861(d)(2)(C) (2012).

[33] *Id., codified at* 50 U.S.C. § 1861(f)(2)(A)(i) (2012).

[34] *Id., codified at* 50 U.S.C. § 1861(f)(2)(A)(ii) (2012).

[35] *Id.*

[36] P.L. 109–177, § 106(b), *codified at* 50 U.S.C. § 1861(f)(2)(B) (2012).

party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[37]

The June 2013 Snowden leaks revealed the existence of a program operated by the NSA under Section 215 of the PATRIOT Act (Section 501 of FISA). The program was initiated in 2001, brought under the supervision of the FISC in 2006, and entailed the ongoing, daily collection of bulk telephony metadata from certain U.S. telecommunications carriers.

Telephony metadata includes communications routing information, including session identifying information (e.g., originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of a call.[38]

The FISC approved this type of collection relying on the Section 215 standard. The court noted in its August 2013 order that "[a]s an initial matter and as a point of clarification, the government's burden under Section 215 is not to prove that the records sought are, in fact, relevant to an authorized investigation. The explicit terms of the statute require 'a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant. . .'"[39] The court adopted an interpretation of this standard from the government's initial application and accompanying memorandum of law that "[i]nformation is 'relevant' to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation."[40]

In support of an interpretation of the Section 215 standard, the government argued—and the FISC agreed—that "[a]nalysts know that the terrorists' communications are located somewhere in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries . . . [a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection."[41] The FISC concluded that "[t]he fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to obtain a production of records."[42]

On May 7, 2015, the U.S. Court of Appeals for the Second Circuit issued a decision in *ACLU v. Clapper,*[43] holding that Section 215 "and the statutory scheme to which it relates do not preclude judicial review, and the bulk telephone metadata program is not authorized by Section 215."[44] Specifically, the court declined to read the "relevance" standard of Section 215 as authorizing the broad-sweeping, nationwide collection of telephone metadata that is then

---

[37] *Id., codified at* 50 U.S.C. § 1861(f)(3) (2012).
[38] *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things,* Doc. No. BR 13–109 (FISC Aug. 22, 2013).
[39] *Id* at 18. (emphasis in original).
[40] *Id.*
[41] *Id.* at 21.
[42] *Id.* at 22–23.
[43] Case No. 14–42–cv (2d Cir. May 7, 2015).
[44] *Id.* at 2.

queried by the NSA in authorized international terrorism investigations. The court stated that

> The records demanded are all-encompassing; the government does not even suggest that all of the records sought, or even necessarily any of them, are relevant to any specific defined inquiry. Rather, the parties ask the Court to decide whether § 215 authorizes the "creation of a historical repository of information that bulk aggregation of the metadata allows" because bulk collection to create such a repository is "necessary to the application of certain analytic techniques." That is not the language in which grand jury subpoenas are traditionally discussed.
>
> Thus, the government takes the position that the metadata collected—a vast amount of which does not contain directly "relevant" information, as the government concedes—are nevertheless "relevant" because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant. We agree with appellants that such an expansive concept of "relevance" is unprecedented and unwarranted.[45]

The court noted, however, that

> [W]e are not unmindful that a full debate by Congress of the appropriateness of a program such as that now operated by the government may result in the approval of a program with greater safeguards for privacy, or with other limitations, that are not now in place and that could alter or even moot the issues presented by appellants. In the last Congress, for example, a bill to authorize a modified version of the telephone metadata program, supported by the Administration, passed the House of Representatives; a similar bill failed in the Senate after a majority of senators—but not the required 60 to cut off debate—sought to bring the bill to a vote. As noted above, more recently, on April 30, 2015, a modified version of the USA FREEDOM Act, which would limit the bulk metadata program in various ways, was passed by the House Judiciary Committee and a vote in that Chamber is expected later this month. An identical bill has been introduced in the Senate and referred to the Senate Judiciary Committee.[46]

Although the Second Circuit reversed the district court's grant of the government's motion to dismiss, the court declined to issue a preliminary injunction against the bulk telephone metadata program.

> We note that at the present time, § 215 is scheduled to expire in just several weeks. The government vigorously contends that the program is necessary for maintaining national security, which of course is a public interest of the highest order. Allowing the program to remain in place for

[45] *Id.* at 58–59 (internal citations omitted).
[46] *Id.* at 92–93 (internal citations omitted).

> a few weeks while Congress decides whether and under what conditions it should continue is a lesser intrusion on appellants' privacy than they faced at the time this litigation began. In light of the asserted national security interests at stake, we deem it prudent to pause to allow an opportunity for debate in Congress that may (or may not) profoundly alter the legal landscape.[47]

Hearings

The Committee on the Judiciary held no hearings on H.R. 2048.

Committee Consideration

On April 30, 2015, the Committee met in open session and ordered the bill H.R. 2048 favorably reported without amendment, by a rollcall vote of 25 to 2, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee's consideration of H.R. 2048.

1. Amendment #1, offered by Mr. King. This amendment allows the head of an element of the intelligence community to enter into a voluntary agreement with a person to compensate such person for retaining call detail records for a period of time. This amendment was defeated by a rollcall vote of 4 to 24.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman		X	
Mr. Sensenbrenner, Jr. (WI)		X	
Mr. Smith (TX)			
Mr. Chabot (OH)			
Mr. Issa (CA)		X	
Mr. Forbes (VA)		X	
Mr. King (IA)	X		
Mr. Franks (AZ)		X	
Mr. Gohmert (TX)	X		
Mr. Jordan (OH)	X		
Mr. Poe (TX)	X		
Mr. Chaffetz (UT)			
Mr. Marino (PA)		X	
Mr. Gowdy (SC)		X	
Mr. Labrador (ID)		X	
Mr. Farenthold (TX)			
Mr. Collins (GA)		X	
Mr. DeSantis (FL)			
Ms. Walters (CA)		X	
Mr. Buck (CO)		X	
Mr. Ratcliffe (TX)		X	

[47] *Id.* at 95.

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Mr. Trott (MI)		X	
Mr. Bishop (MI)		X	
Mr. Conyers, Jr. (MI), Ranking Member		X	
Mr. Nadler (NY)		X	
Ms. Lofgren (CA)		X	
Ms. Jackson Lee (TX)			
Mr. Cohen (TN)		X	
Mr. Johnson (GA)			
Mr. Pierluisi (PR)			
Ms. Chu (CA)			
Mr. Deutch (FL)		X	
Mr. Gutierrez (IL)			
Ms. Bass (CA)		X	
Mr. Richmond (LA)			
Ms. DelBene (WA)		X	
Mr. Jeffries (NY)		X	
Mr. Cicilline (RI)		X	
Mr. Peters (CA)		X	
Total	4	24	

2. Amendment #2, offered by Mr. Poe, Ms. Lofgren, Mr. Jordan, Ms. DelBene, Mr. Labrador, and Mr. Jeffries. This amendment prohibits searching a database containing information collected under Section 702 of FISA using a U.S. Person Search Query except with a showing of FISA probable cause, in an emergency, or with such U.S. Person's consent. This amendment also prohibits a Federal Agency from mandating or requesting a "backdoor" into commercial products that can be used for surveillance. This amendment was defeated by a rollcall vote of 9 to 24.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman		X	
Mr. Sensenbrenner, Jr. (WI)		X	
Mr. Smith (TX)		X	
Mr. Chabot (OH)		X	
Mr. Issa (CA)		X	
Mr. Forbes (VA)		X	
Mr. King (IA)		X	
Mr. Franks (AZ)		X	
Mr. Gohmert (TX)	X		
Mr. Jordan (OH)	X		
Mr. Poe (TX)	X		
Mr. Chaffetz (UT)		X	
Mr. Marino (PA)		X	
Mr. Gowdy (SC)		X	
Mr. Labrador (ID)	X		
Mr. Farenthold (TX)			

ROLLCALL NO. 2—Continued

	Ayes	Nays	Present
Mr. Collins (GA)			
Mr. DeSantis (FL)			
Ms. Walters (CA)		X	
Mr. Buck (CO)	X		
Mr. Ratcliffe (TX)		X	
Mr. Trott (MI)		X	
Mr. Bishop (MI)		X	
Mr. Conyers, Jr. (MI), Ranking Member		X	
Mr. Nadler (NY)		X	
Ms. Lofgren (CA)	X		
Ms. Jackson Lee (TX)		X	
Mr. Cohen (TN)		X	
Mr. Johnson (GA)			
Mr. Pierluisi (PR)			
Ms. Chu (CA)		X	
Mr. Deutch (FL)		X	
Mr. Gutierrez (IL)			
Ms. Bass (CA)		X	
Mr. Richmond (LA)		X	
Ms. DelBene (WA)	X		
Mr. Jeffries (NY)	X		
Mr. Cicilline (RI)	X		
Mr. Peters (CA)		X	
Total	9	24	

3. Motion to report H.R. 2048 favorably to the House. The motion was agreed to by a vote of 25 to 2.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman	X		
Mr. Sensenbrenner, Jr. (WI)	X		
Mr. Smith (TX)			
Mr. Chabot (OH)	X		
Mr. Issa (CA)			
Mr. Forbes (VA)	X		
Mr. King (IA)			
Mr. Franks (AZ)	X		
Mr. Gohmert (TX)			
Mr. Jordan (OH)		X	
Mr. Poe (TX)		X	
Mr. Chaffetz (UT)	X		
Mr. Marino (PA)	X		
Mr. Gowdy (SC)	X		
Mr. Labrador (ID)			
Mr. Farenthold (TX)			
Mr. Collins (GA)	X		
Mr. DeSantis (FL)	X		

ROLLCALL NO. 3—Continued

	Ayes	Nays	Present
Ms. Walters (CA)	X		
Mr. Buck (CO)			
Mr. Ratcliffe (TX)	X		
Mr. Trott (MI)	X		
Mr. Bishop (MI)	X		
Mr. Conyers, Jr. (MI), Ranking Member	X		
Mr. Nadler (NY)	X		
Ms. Lofgren (CA)	X		
Ms. Jackson Lee (TX)			
Mr. Cohen (TN)	X		
Mr. Johnson (GA)			
Mr. Pierluisi (PR)			
Ms. Chu (CA)	X		
Mr. Deutch (FL)	X		
Mr. Gutierrez (IL)			
Ms. Bass (CA)			
Mr. Richmond (LA)	X		
Ms. DelBene (WA)	X		
Mr. Jeffries (NY)	X		
Mr. Cicilline (RI)	X		
Mr. Peters (CA)	X		
Total	25	2	

Committee Oversight Findings

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 2048, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 8, 2015.

Hon. BOB GOODLATTE, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2048, the "USA FREEDOM Act of 2015."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226–2840.

Sincerely,

KEITH HALL,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 2048—USA FREEDOM Act of 2015.

As ordered reported by the House Committee on the Judiciary on April 30, 2015.

H.R. 2048 would make several amendments to the investigative and surveillance authorities of the United States government, and would specify the conditions under which the Federal Government may conduct certain types of surveillance. CBO does not provide estimates for the cost of classified programs; therefore, this estimate addresses only the unclassified aspects of the bill. Under that limitation, CBO estimates that implementing H.R. 2048 would cost $15 million over the 2016–2020 period, subject to the appropriation of the necessary amounts.

Enacting H.R. 2048 also could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. The bill could result in the collection of additional criminal penalties because it would extend the authority of the government to conduct surveillance in certain instances for four years and would establish new crimes relating to certain acts of terrorism. Such penalties are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO anticipates that any additional amounts collected under the bill would be minimal and the net impact on the deficit of any additional collections and spending would be insignificant.

Effects on the Federal Budget

The bill would amend the Foreign Intelligence Surveillance Act (FISA). Those amendments would affect the operations of the Foreign Intelligence Surveillance Court (FISC) and the Judiciary. First, H.R. 2048 would require the FISC to designate at least five amici curiae, or "friends of the court," to assist the court when the government makes an application under FISA that presents a novel or significant interpretation of FISA. Second, the bill would limit the collection of telephone call records, thereby requiring the

intelligence agencies—acting through the Department of Justice—to seek additional warrants from the FISC to access such data. Finally, the bill would require an annual report by the Director of the Administrative Office of the U.S. Courts (AOUSC) that includes data on certain types of FISA orders. Based on information from the AOUSC, CBO estimates that implementing those requirements would cost $5 million over the 2016–2020 period, assuming appropriation of the necessary amounts.

In addition, the bill would require Federal agencies to conduct several program assessments and reviews, and would establish new reporting requirements. Section 108 would require the Inspectors General of the Justice Department and the Intelligence Community to assess the effectiveness of the surveillance programs affected by the bill; section 402 would require the Director of National Intelligence to conduct declassification reviews of certain court decisions, orders, and opinions related to FISA. CBO estimates that fulfilling those requirements would cost $10 million over the 2016–2020 period, assuming appropriation of the necessary amounts.

Intergovernmental and Private-Sector Mandates

H.R. 2048 would impose two mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on both private and intergovernmental entities. The bill would expand liability protections and limit the ability of plaintiffs to sue in cases where a defendant provides information to the Federal Government pursuant to a FISA order. It also would require entities, when compelled to provide information about telephone calls to Federal officials, to protect the secrecy of the records and to minimize any disruption of services.

CBO estimates that the costs of those mandates would be small. The change in expanded liability protection is a slight modification to current law, and CBO estimates that the elimination of any legal right of action for future plaintiffs would affect a limited number of potential lawsuits. Information from the Department of Justice indicates that public entities receive few requests for call records, and the costs to those entities of providing that information are negligible. In addition, since public and private entities already take action to protect private information in complying with requests from the government, the incremental cost to those entities would be insignificant. Further, public and private entities would be compensated by the Federal Government at the prevailing rate for the services they would be required to provide. Consequently, CBO estimates that the total costs to public and private entities of all the mandates in the bill would fall below the intergovernmental and private-sector thresholds established in UMRA ($77 million and $154 million in 2015, respectively, adjusted annually for inflation).

Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for the ratification or implementation of international treaty obligations. CBO has determined that Title VIII of the bill fits within that exclusion, because that title would implement the obligations of various treaties for maritime and nuclear activities to which the U.S. is a party.

Staff Contacts

The CBO staff contacts for this estimate are Mark Grabowicz, Marin Burnett, and Bill Ma (for Federal costs), J'nell L. Blanco (for the intergovernmental effects), and Logan Smith (for the private-sector effects). This estimate was approved by Theresa Gullo, Assistant Director for Budget Analysis.

Duplication of Federal Programs

No provision of H.R. 2048 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

Disclosure of Directed Rule Makings

No provision of H.R. 2048 directs a specific rule making within the meaning of 5 U.S.C. § 551.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 2048, the USA FREEDOM Act, reforms Section 215 of the USA PATRIOT Act (Section 501 of FISA), clarifies several other national security authorities, expands existing oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 2048 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

The following discussion describes the bill as reported by the Committee.

Sec. 1—Short title; table of contents.

This section provides that the short title of the bill is the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015" or the "USA FREEDOM Act of 2015." This section also provides a table of contents for the bill.

Sec. 2—Amendments to the Foreign Intelligence Surveillance Act of 1978.

This section provides that a reference to an amendment to or repeal of this Act is considered to be a reference to the Foreign Intelligence Surveillance Act of 1978 (FISA), except as otherwise provided.

Title I—FISA Business Record Reforms

Sec. 101—Additional requirements for call detail records.

On January 17, 2014, President Obama announced reforms to the collection of signals intelligence by the Federal Government [48] and issued Presidential Policy Directive (PPD) 28. The President directed that the queries of telephone metadata collected by the National Security Agency (NSA) under Section 501 of FISA must first be approved by a judge with the Foreign Intelligence Surveillance Court (FISC) and such queries would be limited to two "hops." [49]

This section relies on these reforms to establish a new, narrowly-tailored mechanism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized investigation to protect against international terrorism. This new mechanism is the only circumstance in which Congress contemplates the prospective, ongoing use of Section 501 of FISA in this manner.

Under this section, if the government can demonstrate a reasonable, articulable suspicion that a specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation therefor, the FISC may issue an order for the ongoing, daily production of call detail records held by telephone companies. The prospective collection of call detail records is limited to 180 days.

The government may require the production of up to two "hops"—i.e., the call detail records associated with the initial seed telephone number and call detail records (CDRs) associated with the CDRs identified in an initial "hop." Subparagraph (F)(iii) provides that the government can obtain the first set of CDRs using the specific selection term approved by the FISC. In addition, the government can use the FISC-approved specific selection term to identify CDRs from metadata it already lawfully possesses. Together, the CDRs produced by the phone companies and those identified independently by the government constitute the first "hop." Under subparagraph (F)(iv), the government can then present session identifying information or calling card numbers (which are components of a CDR, as defined in section 107) identified in the first "hop" CDRs to phone companies to serve as the basis for companies to return the second "hop" of CDRs. As with the first "hop," a second "hop" cannot be based on, nor return, cell site or GPS location information. It also does not include an individual listed in a telephone contact list, or on a personal device that uses the same wireless router as the seed, or that has similar calling patterns as the seed. Nor does it exist merely because a personal device has been in the proximity of another personal device. These types of information are not maintained by telecommunications carriers in the normal course of business and, regardless, are prohibited under the definition of "call detail records."

"Call detail records" include "session identifying information (including originating or terminating telephone number, International

[48] Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[49] *Id.*

Mobile Subscriber Identity number, or International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call." The Act explicitly excludes from that term the contents of any communication; the name, address, or financial information of a subscriber or customer; and cell site location or GPS information, and the Act should not be construed to permit the government to obtain any of this type of information through either of the two "hops."

This new authority—designed to allow the government to search telephone metadata for possible connections to international terrorism—does not preclude the government's use of standard business records orders under Section 501 to compel the production of business records, including call detail records.

This section does not require any private entity to retain any record or information other than in the ordinary course of business. However, nothing in current law or this Act prohibits the government and telecommunications providers from agreeing voluntarily to retain records for periods longer than required for their business purposes.

This section requires the government to adopt minimization procedures that require the prompt destruction of call detail records that are not foreign intelligence information.

Sec. 102—Emergency authority.

This section creates a new emergency authority in Section 501 for both standard business records orders under Section 501(b)(2)(B) and the new call detail records orders under Section 501(b)(2)(C). The Attorney General may authorize the emergency production of tangible things, provided that an application for an order under Section 501 is presented to the court within 7 days. If the court denies an emergency application, the government may not use any of the information obtained under the emergency authority except in instances of a threat of death or serious bodily harm.

Sec. 103. Prohibition on bulk collection of tangible things

This section requires that each application for the production of tangible things include "a specific selection term to be used as the basis for the production." In so doing, the Act makes clear that the government may not engage in indiscriminate bulk collection of any tangible thing or any type of record under Section 501 of FISA.

Section 501(b)(2)(A) of FISA will continue to require the government to make "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation. . . ."[50] Section 103 requires the government to make an additional showing, beyond relevance, of a specific selection term as the basis for the production of the tangible things sought, thus ensuring that the government cannot collect tangible things based on the assertion that the requested collection "is thus relevant, because the success of [an] investigative tool depends on bulk collection."[51] Congress' decision to leave in

[50] 50 U.S.C. § 501(b)(2)(A).

[51] Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted],* No. BR 13–09 (FISA Ct. Aug. 29, 2013), at 21 (citing Mem. of Law at 15, Docket No. BR 06–05).

place the "relevance" standard for Section 501 orders should not be construed as Congress' intent to ratify the FISA Court's interpretation of that term. These changes restore meaningful limits to the "relevance" requirement of Section 501, consistent with the opinion of the U.S. Court of Appeals for the Second Circuit in *ACLU v. Clapper*.

Although this Act eliminates bulk collection, this section maintains Section 501 as a business records authority. The additional showing of a "specific selection term" that will be required in all Section 501 applications does not provide any new authority, but it is defined in such a way as to allow for standard business records collection to continue while prohibiting the use of this authority for indiscriminate, bulk collection.

Sec. 104—Judicial review.

This section provides that the court may evaluate the adequacy of minimization procedures under Section 501. Under current law, the court is only empowered to determine whether the government has minimization procedures in place. This section also makes clear that the FISC may require additional, particularized minimization procedures beyond those required under Section 501 with regard to the production, retention, or dissemination of certain business records, including requiring the destruction of such records within a reasonable time period. This language is intended to capture an existing practice by the FISC to require heightened minimization procedures when appropriate.

Sec. 105—Liability protection.

This section provides liability protections to third parties who provide information, facilities, or technical assistance to the government in compliance with an order issued under Section 501. This provision mirrors the liability provisions in Titles I and VII of FISA.

Sec. 106—Compensation for assistance.

This section explicitly permits the government to compensate third parties for producing tangible things or providing information, facilities, or assistance in accordance with an order issued under Section 501. It is customary for the government to enter into contractual agreements with third parties in order to compensate them for products and services provided to the government.

Sec. 107—Definitions.

This section provides definitions for the terms "address," "call detail record," and "specific selection term." This section also incorporates by reference to Section 101 of FISA definitions for "foreign power," "agent of a foreign power," "international terrorism," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State."

The "specific selection term" required in each Section 501 application is the mechanism by which the Act prohibits the indiscriminate, bulk collection of any type of tangible thing under Section 501. The term "specific selection term," for purposes of a standard Section 501 order, is defined to mean a term that specifically identifies a person, account, address, or personal device, or any other

specific identifier that is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought, consistent with the purpose for seeking the tangible things. It does not include terms that are not so limited, such as terms based on a broad geographic region, such as a state, city, or zip code, (when not used as part of a specific identifier) or terms identifying a service provider (when not used as part of a specific identifier) unless the provider is itself the subject of an investigation.

This definition makes clear that the government may satisfy the requirements of the "specific selection term" definition through use of one or more terms or identifiers as may be necessary to meet the standard set forth in the definition—and as provided for in Section 1 of Title 1, United States Code.

For purposes of the call detail record authority, the term "specific selection term" is defined as a term specifically identifying an individual, account, or personal device.

The term "address" means a physical address or electronic address, such as an electronic mail address, temporarily assigned network address, or Internet protocol address. This definition may overlap with the term "account," which also can be considered a "specific selection term" under the bill. These terms are not mutually exclusive, and an electronic mail address or account also qualifies as an "account" for purposes of the bill.

The term "personal device" refers to a device that can reasonably be expected to be used by an individual or a group of individuals affiliated with one another. For example, "personal device" would include a telephone used by an individual, family, or housemates, a telephone or computer provided by an employer to an employee or employees, a home computer or tablet shared by a family or housemates, and a Wi-Fi access point that is exclusively available to the inhabitants of a home, the employees of a business, or members of an organization. It would also include a local area network server that is used by a business to provide e-mail to its employees. The term "personal device" does not include devices that are made available for use by the general public or by multiple people not affiliated with one other, such as a pay phone available to the public, a computer available to library patrons to access the Internet, or a Wi-Fi access point made available to all customers at an Internet café. Depending on the circumstances, however, such devices could qualify as "any other specific identifier" that is used to limit the scope of the tangible things sought consistent with the purpose for seeking the tangible things. The term "personal device" also does not include devices that are used by companies to direct public communications, such as a router used by an Internet service provider to route e-mails sent by its customers, or a switch used by a telecommunications carrier to route calls made by its customers.

Sec. 108—Inspector General reports on business records orders.

This section requires the Inspector General of the Department of Justice to conduct a comprehensive review of the use of Section 501 with respect to calendar years 2012 to 2014. It also requires the Inspector General of the Intelligence Community to assess the value and use of intelligence obtained under Section 501 over the same time period.

Sec. 109—Effective date.

This section provides that the new call detail records authority, the new Section 501 emergency authority, and the prohibition on bulk collection of tangible things under Section 501 take effect 180 days after enactment.

Sec. 110—Rule of construction.

This section provides a rule of construction that nothing in this Act shall be construed to authorize the production of the contents of electronic communications by electronic communication service providers under Title V of FISA.

Title II—FISA Pen Register and Trap and Trace Device Reform

Sec. 201—Prohibition on bulk collection.

This section prohibits the use of the pen register and trap and trace device authority for bulk collection by requiring each application under this section to include a specific selection term as the basis for the use of a pen register or trap and trace device.

The definition of "specific selection term" is similar to the definition of that term for Section 501 orders. Specifically, it is defined to mean a term that specifically identifies a person, account, address, or personal device, or any other specific identifier that is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for the use of a pen register or trap and trace device. It does not include terms that are not so limited, such as terms based on broad geographic region (when not used as part of a specific identifier) or terms identifying a service provider (when not used as part of a specific identifier) unless the provider is itself the subject of an investigation.

The term "address" means a physical address or electronic address, such as an electronic mail address, temporarily assigned network address, or Internet protocol address. This definition may overlap with the term "account," which also can be considered a "specific selection term" under the bill. These terms are not mutually exclusive, and an electronic mail address or account also qualifies as an "account" for purposes of the bill.

The term "personal device" refers to a device that can reasonably be expected to be used by an individual or a group of individuals affiliated with one another. For example, "personal device" would include a telephone used by an individual, family, or housemates, a telephone or computer provided by an employer to an employee or employees, a home computer or tablet shared by a family or housemates, and a Wi-Fi access point that is exclusively available to the inhabitants of a home, the employees of a business, or members of an organization. It would also include a local area network server that is used by a business to provide e-mail to its employees. The term "personal device" does not include devices that are made available for use by the general public or by multiple people not affiliated with one other, such as a pay phone available to the public, a computer available to library patrons to access the Internet, or a Wi-Fi access point made available to all customers at an Internet café. Depending on the circumstances, however, such devices could qualify as "any other specific identifier" that is used to limit the

scope of the tangible things sought consistent with the purpose for seeking the tangible things. The term "personal device" also does not include devices that are used by companies to direct public communications, such as a router used by an Internet service provider to route e-mails sent by its customers, or a switch used by a telecommunications carrier to route calls made by its customers.

Sec. 202—Privacy procedures.

This section directs the Attorney General to adopt procedures to safeguard nonpublicly available information concerning U.S. persons consistent with the need to protect national security. This section also makes clear that the FISC may require additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.

Title III—FISA Acquisitions Targeting Persons outside the United States Reforms

Sec. 301—Limits on use of unlawfully obtained information.

This section limits the government's use of information about U.S. persons that is obtained under Section 702 procedures that the FISA Court later determines to be unlawful, while still giving the FISA Court flexibility to allow such information to be used in appropriate cases. It is similar to the existing law that limits the use of information collected pursuant to FISA's emergency authority if the FISA Court determines after the fact that the FISA standard was not met.

Title IV—Foreign Intelligence Surveillance Court Reforms

Sec. 401—Appointment of amicus curiae.

This section provides that both the FISC and the FISA Court of Review (FISCR) shall, if deemed appropriate, appoint an individual to serve as amicus curiae in a case involving a novel or significant interpretation of law. In addition, this section permits the court to appoint amicus curiae in any case or permit an individual or organization leave to file as amicus curiae.

The presiding judges of the courts will jointly designate a panel of no fewer than five individuals who are eligible to serve as amicus curiae. In designating such individuals, the presiding judges may consider individuals recommended from any source, including members of the Privacy and Civil Liberties Oversight Board, that the judges deem appropriate. These individuals shall possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area of law that may lend legal or technical expertise to the courts, and shall be eligible for access to classified information necessary to participate as amicus curiae.

A novel or significant interpretation of law involves application of settled law to novel technologies or circumstances materially different from those in prior cases, or any other novel or significant construction or interpretation of any provision of law or of the U.S. Constitution. It is not intended to include routine, fact-based FISA applications that do not present novel legal or technological issues.

An instance in which it may apply, however, is to novel and significant interpretations of "specific selection term."

The duties of an amicus curiae may include, as appropriate, legal arguments that advance the protection of individual privacy and civil liberties, information related to intelligence collection or communications technology, or legal arguments or information regarding any other area relevant to the issue presented to the FISC or FISCR.

An individual appointed as an amicus curiae by the FISC or FISCR may request appointment of additional amicus curiae, have access to all relevant legal precedent and any application, certification, petition, motion or such other materials that the court determines are relevant to the duties of an amicus curiae, and have access to classified materials to the extent consistent with national security. This section excludes access to privileged materials and makes clear that the authorization for the appointment of amicus curiae does not affect the ability of the courts to continue to receive information or materials from, or otherwise communicate with, the government or amicus curiae on an *ex parte* basis.

The Attorney General may brief individuals designated as amicus curiae regarding constructions or legal interpretations of FISA, and legal, technological, and other issues related to actions authorized by FISA. The FISC or FISCR must notify the Attorney General when it appoints an individual to serve as amicus curiae and may seek the assistance of the Executive Branch in implementation of this authority. The courts may provide for the designation, appointment, removal, training, or other support for amicus curiae.

This section also authorizes the FISC, in the judge's discretion and following issuance of a FISA order, to certify a question of law to the FISCR if such question of law may affect the resolution of the matter in controversy because of a need for uniformity or to serve the interests of justice. This section also permits the FISCR to certify questions of law to the U.S. Supreme Court and authorizes the Supreme Court to appoint an individual to serve as amicus curiae from among those designated by the FISC and FISCR under this section. This provision is based upon and conforms to existing procedures for certified questions of law from the Federal courts of appeals to the U.S. Supreme Court in Section 1254(2) of Title 28, United States Code.

Sec. 402—Declassification of decisions, orders, and opinions.

This section requires the Attorney General to conduct a declassification review of each decision, order, or opinion of the FISC or FISCR that includes a significant construction or interpretation of law. In the interest of national security, the Director of National Intelligence (DNI) may waive the declassification requirement, in which case the Attorney General shall provide a public summary of the decision. The Attorney General is instructed to summarize significant constructions or interpretations of law which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the FISC. Any such summary would not be considered to be part of the court's opinion.

Title V—National Security Letter Reform

Sec. 501—Prohibition on bulk collection.

This section prohibits the use of various national security letter (NSL) authorities (contained in the Electronic Communications Privacy Act, Right to Financial Privacy Act, and Fair Credit Reporting Act) without the use of a specific selection term as the basis for the NSL request. It specifies that for each NSL authority, the government must specifically identify the target or account.

While the overall objective is the same, each of the NSL authorities is amended with slightly different language in order to account for differences in the underlying statutes. For example, Section 501(a) amends the Electronic Communications Privacy Act to require "a term that specifically identifies a person, entity, telephone number, or account," while Section 501(b) amends the Right to Financial Privacy Act to require "a term that specifically identifies a customer, entity, or account." These differences in amendments to the NSL authorities simply conform the new language to the original statutory structure.

Sec. 502—Limitations on Disclosure of National Security Letters.

This section corrects the constitutional defects in the issuance of NSL nondisclosure orders found by the Second Circuit Court of Appeals in *Doe v. Mukasey,* 549 F.3d 861 (2d Cir. 2008), and adopts the concepts suggested by that court for a constitutionally sound process.

It permits the government to impose a nondisclosure order on the recipient of an NSL if a senior FBI official certifies that danger to the national security, interference with an investigation, interference with diplomatic security, or danger to the life or safety of a person may result from public disclosure of the order. It also permits disclosure to persons to whom disclosure is necessary to comply with the NSL; an attorney; or others as permitted by the FBI.

This section allows the recipient of an NSL nondisclosure order to challenge the nondisclosure order by notifying the government or by filing a petition for judicial review. If the recipient notifies the government, the government then has 30 days to seek a court order in Federal district court to compel compliance with the nondisclosure order. This option is intended to ease the burden on the recipient in challenging the nondisclosure order. If the court determines there is reason to believe that certain harms may result if the gag order is not imposed, the court shall issue the nondisclosure order.

This section repeals a provision stating that a conclusive presumption in favor of the government shall apply where a high-level official certifies that disclosure of the NSL would endanger national security or interfere with diplomatic relations.

This section also provides that the Attorney General shall adopt procedures for the review of nondisclosure requirements issued pursuant to an NSL. These procedures require the government to review at appropriate intervals whether the facts supporting nondisclosure continue to exist; the termination of such nondisclosure requirement if the facts no longer support nondisclosure; and appropriate notice to the recipient of the NSL, and the applicable court as appropriate, when the nondisclosure requirement has been terminated. These procedures are based upon nondisclosure re-

forms proposed by President Obama in January 2014. In remarks accompanying the issuance of PPD–28, President Obama directed the Attorney General "to amend how we use National Security Letters so that [their] secrecy will not be indefinite, and will terminate within a fixed time unless the government demonstrates a real need for further secrecy." [52]

In January 2015, as part of its Signals Intelligence Reform 2015 Anniversary Report, the Director of National Intelligence announced that:

> In response to the President's new direction, the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of 3 years after the opening of a fully predicated investigation or the investigation's close. Continued nondisclosures orders beyond this period are permitted only if a Special Agent in Charge or a Deputy Assistant Director determines that the statutory standards for nondisclosure continue to be satisfied and that the case agent has justified, in writing, why continued nondisclosure is appropriate.

Sec. 503—Judicial Review.

This section modifies each of the national security letter statutes to specify that judicial review of NSLs and NSL nondisclosure orders is governed by 18 U.S.C. § 3511, and that each NSL issued shall notify the recipient of the availability of judicial review of the NSL itself, as well as the nondisclosure order.

Title VI—FISA Transparency and Reporting Requirements

Sec. 601—Additional Reporting on Orders Requiring Production of Business Records; Business Records Compliance Reports to Congress.

In addition to existing annual reporting requirements, this section requires the government to provide to Congress a summary of all compliance reports related to the use of Section 501. It also requires the government to report on the number of applications made for call detail records under the new call detail record authority and the number of orders granted, modified or denied, as well as the number of standard Section 501 applications and orders granted, modified, or denied. It further requires the government to report on the number of Section 501 applications based on a specific selection term that does not specifically identify an individual, account or personal device; the number of those applications granted, modified, or denied; and for those applications that were granted or modified, whether the FISA Court adopted additional, particularized minimization procedures.

Sec. 602—Annual Reports by the Government.

This section requires the Administrative Office of the U.S. Courts to report to Congress annually the number of FISA orders and cer-

[52] Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

tifications applied for, issued, modified, and denied, and the number of appointments by the FISA Court of amici curiae under section 103. This information must also be posted on a public website, subject to a declassification review. The Administrative Office must also report to Congress the instances in which the FISC issued a finding that appointment of amicus curiae was not appropriate and the text of such findings.

This section also requires the government to report annually to the public key information about the scope of collection under the FISA pen register, business records, call detail records, and Section 702 authorities, as well as the national security letter statutes. For FISA pen register, business records, and call detail records, the government must annually report a good faith estimate of the number of targets of these orders, and the number of unique identifiers collected pursuant to those orders. The phrase "unique identifiers used to communicate information collected pursuant to such orders" means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders—not just the number of target email addresses or telephone numbers.

For Section 702 collection, the government must report the number of orders, the number of search terms concerning known U.S. persons used to retrieve unminimized contents of wire or electronic communications acquired under Section, and the number of queries concerning known U.S. persons of unminimized noncontents information acquired under Section 702. This requirement is consistent with how the Intelligence Community counted these figures for purposes of a June 27, 2014, letter from the Office of the Director of National Intelligence to Senator Wyden.

For national security letters, the government must annually report the number of letters issued, the number of requests for information in those letters, and a good faith estimate of the number of requests concerning U.S. persons and non-U.S. persons.

This section has limited exceptions. The FBI is exempted from reporting requirements that the agency has indicated it lacks the capacity to provide. Additionally, while the government is required to estimate the number of known U.S. person queries of non-contents information collected under Section 702, if the Director of National Intelligence determines that these estimates cannot be determined accurately because some but not all relevant elements can comply, the Director must report the estimate for those elements able to comply, and provide a public, unclassified certification to the Senate and House Intelligence and Judiciary Committees each year explaining why the Intelligence Community is unable to report these figures and when it is reasonably anticipated that such an estimate can be determined fully and accurately.

Finally, this section requires annual reporting on the number of accounts from which the Department of Justice receives voluntary disclosures in an emergency for non-content information.

Sec. 603—Public Reporting by Persons Subject to FISA Orders.

Companies subject to FISA orders or National Security Letters (NSLs) may publicly report information about the number of such orders or NSLs they receive and how many of their customers are targeted by these national security processes. This provision is

modeled on the January 2014 settlement between various technology companies and the Justice Department, which allowed for companies to publicly report data concerning government requests for customer information. This provision is intended to capture reporting by companies as it was agreed to in the settlement.

The bill provides four options for this reporting: (1) a semiannual report on the number of NSLs, FISA content orders and FISA non-content orders in bands of 1000, with some breakdowns by authority for non-content information; (2) a semiannual report on the number of NSLs, FISA content orders and FISA non-content orders in bands of 500; (3) a semiannual report on the total national security process received in bands of 250; or (4) an annual report on the total national security process received in bands of 100. For the options permitting disclosures in bands of 500 and 1000, providers must wait 18 months before reporting on any FISA orders or directives received with respect to a platform, product, or service for which the provider has not previously received an order or directive. It is anticipated that companies may have a necessary delay between the end of certain reporting periods required under this section and the date a report may be issued by a company pursuant to this section.

By permitting companies to report the number of "customer selectors targeted" for each of the relevant authorities, this provision is intended to capture circumstances in which the government asks the company for information about a single identifier or selector, but the company returns multiple accounts associated with that identifier or selector, or the reverse situation where multiple identifiers or selectors are tied to a single account. In such a circumstance, the company is permitted to report the total number of accounts returned based on the identifiers and selectors specified in the government request, because all of those accounts have been targeted by the government's process.

Sec. 604—Reporting Requirements for Decisions, Orders, and Opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.

This section requires the Attorney General to provide a copy of each decision, order, or opinion, including a modification or denial of an application that includes a significant construction or interpretation of any provision of law to the relevant committees, within 45 days.

Sec. 605—Submission of reports under FISA.

This section includes the House Judiciary Committee in several existing reporting requirements.

Title VII—Enhanced National Security Provisions

Sec. 701—Emergencies Involving Non-United States Persons.

This section provides for the lawful targeting of a non-United States person who was previously believed to be located outside the United States for a period not to exceed 72 hours when it is determined that the non-United States person is reasonably believed to be located inside the United States, in certain limited cir-

cumstances. Among other requirements, the head of an element of the Intelligence Community must reasonably determine that a lapse in targeting such non-United States person poses a threat of death or serious bodily harm.

This provision should not be construed as creating broad new surveillance authorities. Rather, the purpose of this section is to allow the intelligence community to continue to target a non-United States person, in certain narrowly limited circumstances, for up to 72 hours after that person is reasonably believed to be located inside the United States, to provide time to compile the information needed to ask the Attorney General to approve emergency FISA authority under Title I or Title III of FISA. If the Attorney General does not approve an emergency authority, or if the FISA Court turns down a subsequent application, the information acquired during the 72-hour period must be purged unless it indicates a threat of death or serious bodily harm. This section also provides for a semiannual report to Congress of the total number of authorizations under this section along with the number of accompanying subsequent emergency employments of electronic surveillance under FISA.

Sec. 702—Preservation of treatment of non-United States persons travelling outside United States as agents of foreign powers.

This section addresses an anomaly in FISA that has been interpreted to require the government to terminate electronic surveillance under Title I of FISA or terminate physical search under Title III of FISA because a non-U.S. person, who is known to be acting inside the U.S. as an agent of a foreign power, exits the United States.

As currently written, subparagraphs (A) and B) of section 101(b)(1) of FISA require that a non-U.S. person who is an officer or employee of a foreign power or acts on behalf of a foreign power engaging in clandestine intelligence activities must be acting in the United States in one of those capacities in order to be considered an agent of the foreign power for purposes of Title I and Title III of FISA. As a result of these definitions, in certain circumstances, the government must terminate electronic surveillance or physical search pursuant to Titles I and III of FISA because the target has left the United States or may not be able to initiate Title I electronic surveillance and Title III physical searches until the target enters the United States. Although collection on such individuals overseas may be permitted under authorities other than Titles I and III, this section revises the definitions of subparagraphs (A) and (B) of section 101(b)(1) of FISA to permit the government to conduct Title I electronic surveillance and Title III physical searches targeting certain individuals regardless of whether they are physically located in the United States or abroad.

The revisions of subparagraphs (A) and (B) of section 101(b)(1) are not intended to alter the definition of electronic surveillance under FISA. The revisions are solely intended to afford the government the operational flexibility to initiate and maintain Title I electronic surveillance or Title III physical search authorities in the above circumstances.

Sec. 703—Improving investigations of international proliferation of weapons of mass destruction.

This section amends the definition of "agent of a foreign power" in Section 101(b)(1)(E) of FISA, pertaining to the international proliferation of weapons of mass destruction, to include those who knowingly aid and abet, or knowingly conspire with, persons engaged in such proliferation or activities in furtherance of such proliferation on behalf of a foreign power. This amendment, which is applicable only to non-U.S. persons, is intended to ensure that those who facilitate the international proliferation of weapons of mass destruction on behalf of a foreign power by knowingly procuring or selling components or ancillary materials for the purpose of constructing weapons of mass destruction may be targeted under FISA.

Sec. 704—Increase in penalties for material support of foreign terrorist organizations.

This section increases the statutory maximum penalty from 15 to 20 years for material support of designated foreign terrorist organizations.

Sec. 705—Sunsets.

This section reauthorizes Section 215 (business records) and Section 206 (roving wiretap authority) of the PATRIOT Act and Section 6001 (lone wolf definition) of the Intelligence Reform and Terrorism Prevention Act of 2004 to December 15, 2019.

Title VIII—Safety of Maritime Navigation and Nuclear Terrorism Conventions Implementation

Subtitle A—Safety of Maritime Navigation

These amendments implement the changes to 18 U.S.C. § 2280 required by the 2005 Protocol to the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation ("2005 Protocol") and the changes to 18 U.S.C. § 2281 required by the 2005 Protocol to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf ("2005 Platforms Protocol").

Sec. 801—Amendment to section 2280 of title 18, United States Code.

This section amends Section 2280, Violence Against Maritime Navigation in subsection (1)(A)(i) by expanding jurisdiction over prohibited activity against U.S. ships to include not just those flying the flag of the United States, but also "a vessel of the United States or a vessel subject to the jurisdiction of the United States." In (b)(1)(A)ii jurisdiction is expanded by adding "including the territorial seas." The current statute just refers to "in the United States."

In (b)(1)(A)(iii) jurisdiction over prohibited activities against maritime navigation by including activity committed by a United States corporation or legal entity, in addition to the current language giving jurisdiction over a national of the United States or by a stateless person whose habitual residence is the United States.

In subsection (c) a correction is made to an error in the cross-reference to the Norris-LaGuardia Act by substituting "section 13 (c) for the current 2 (c)" of that Act.

The current subsection (d) relating to the delivery of a suspected offender is updated and moved to (f). The new subsection (d) identifies nine applicable treaties and contains the existing definitions for Section 2280 as well as the definitions for some new terms utilized by the 2005 Protocol. Terms defined include biological weapon, chemical weapon, explosive material, and infrastructure facility, among others. It also updates the definitional sections by adding a definition of "international organization," to be consistent with 18 U.S.C. § 831. This subsection also adopts the definition of "military forces of a state" used in the 2005 Protocol. Consistent with the understanding included in the instrument of ratification for the 2005 Protocols, the exemption provided by this bill to subsection(e)(2) of Section 2280, includes civilians who direct or organize the official activities of military forces of a State. Subsection (e) of 2280 creates an exception for the activities of armed forces during an armed conflict, as those terms are understood under the law of war and for activities undertaken by military forces of a state in the exercise of their official duties.

Subsection (f) updates the grounds permitting the master of a ship to deliver an offender to another state, under certain conditions, to include the new offenses added by these amendments. It provides authority for the master of a covered ship flying the flag of the United States, who has reasonable grounds to believe a person on board has committed an offense under 18 U.S.C. 2280 or 2280a, to deliver that person to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation. This change is required under the 2005 Protocol, Article 8 as amended.

Subsection (g) establishes a Civil Forfeiture provisions against any real or personal property used or intended for use in committing violations under section 2280. This would include gross proceeds of such violations, and real or personal property traceable to such property or proceeds. These forfeitures are governed by the provisions of chapter 46 of Title 18, but may also be performed by agents or officers designated by the Secretary of homeland Security, the Attorney General, or the Secretary of Defense.

Sec. 802—New section 2280A of title 18, United States Code.

This section establishes a new section 2280a to Title 18. The 2005 Protocol forbids enumerated maritime terrorism acts and the maritime transport of biological, chemical, or nuclear weapons ("BCN weapons") or certain of their components, delivery means, or materials, under specified circumstances. The 2005 Protocol also forbids the maritime transport of terrorist fugitives. The 2005 Protocol does not affect the rights or obligations of parties under the Treaty on the Non-Proliferation of Nuclear Weapons, the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, or the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. There are exceptions for armed forces

and military actions in accordance with the 2005 Protocol, Article 2*bis,* paragraph 2.

Subsection (a)(1)(A) implements paragraph 1(a)(i), (ii), and (iii) of Article 3*bis* of the 2005 Protocol. Under these provisions, it is an offense to, unlawfully and with the intent to intimidate a population or compel a government or an international organization to do or refrain from doing an act, (i) use against or on, or discharge from, a ship any explosive or radioactive material, or BCN weapon, in a manner that causes or is likely to cause death or serious injury or damage; (ii) discharge from a ship oil, liquefied natural gas, or another hazardous or noxious substance, in a manner that causes or is likely to cause death or serious injury or damage; or (iii) otherwise use a ship in a manner that causes death or serious injury or damage.

Subsection (a)(1)(B) implements paragraphs 1(b) and 2 of Article 3*bis.* Subsection (a)(1)(B)(i) forbids the transport of explosive or radioactive material intended for a terrorist act. Subsection (a)(1)(B)(ii) forbids the transport of BCN weapons. Subsection (a)(1)(B)(iii) forbids the transport of source or special fissionable material or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material where intended for use in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an International Atomic Energy Agency comprehensive safeguards agreement (except where not contrary to obligations of parties to the Treaty on the Non-Proliferation of Nuclear Weapons ("NPT")). For example, transport would be permitted if no safeguards are required, as in the case of a Nuclear Weapon State Party recipient, or if an NPT State Party sends such materials or equipment to a country that is not an NPT State Party for use in an activity under "facility-specific" International Atomic Energy Agency ("IAEA") safeguards. At the same time, transport, even by an NPT State Party to a country that is not an NPT State Party, would be forbidden if the resulting transfer violated the NPT party's obligations under the NPT. For example, the obligations of NPT States Parties under the NPT include, among other things, the obligation not to provide source or special fissionable material or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material to any non-nuclear weapon state for peaceful purposes, unless the source or special fissionable material is subject to IAEA safeguards.

Subsections (a)(1)(B)(iv)-(vi) forbid transport of certain dual use items that will significantly contribute to and are intended for the design or manufacture of a BCN weapon or its means of delivery. Subparagraph (B) reflects the conduct forbidden by paragraphs 1(b) of Article 3*bis* as well as the savings provision of paragraph 2 of Article 3*bis* but is reorganized to provide a clearer exposition of the exceptions applicable to each category of forbidden conduct. The offenses prohibited are consistent with the obligations under the Treaty on the Non-Proliferation of Nuclear Weapons and complementary with the obligations set out in U.N. Security Council Resolution 1540 regarding prohibitions against the transport of BCN weapons.

Subsection (a)(1)(C) implements Article 3*ter* of the 2005 Protocol to prohibit the transportation of a terrorist fugitive (*i.e.,* perpetra-

tors of an act prohibited under the amended SUA or one of nine other UN terrorism conventions), with the intent to help the fugitive evade prosecution.

Subsections (a)(1)(D) and (E) add provisions regarding conspiracy, attempt, and injury or death in connection with one of the listed offenses. The amendments reflect the amendments in the 2005 Protocol (*see* Article 3*quater*). It should be noted that the current provisions found in 18 U.S.C. §§ 2, 371, and 2339A, and the conspiracy offenses in Section 2280, implement the obligations under subparagraphs (c), (d), and (e) of Article 3*quater* of the 2005 Protocol.

Subsection (a)(2) criminalizing threats is updated to implement the 2005 Protocol's requirement to criminalize threats to commit the terrorism-related offenses described in subparagraph (G) (*see* 2005 Protocol, Article 3*bis,* paragraph (1)(a)(iv)).

Subsection (b) establishes jurisdiction over prohibited activity consistent with that found in 18 U.S.C. 2280.

Subsection (c) of inserts exceptions (as does Section 801 supra) specifying that the statute does not apply to armed forces during an armed conflict or to the official exercise of military duties, as specified in Article 2*bis* of the 2005 Protocol.

Subsection (d) establishes a Civil Forfeiture provisions against any real or personal property used or intended for use in committing violations under section 2280. This would include gross proceeds of such violations, and real or personal property traceable to such property or proceeds. These forfeitures are governed by the provisions of chapter 46 of Title 18, but may also be performed by agents or officers designated by the Secretary of homeland Security, the Attorney General, or the Secretary of Defense.

The penalties for violations of 18 U.S.C. 2280a are a fine, imprisonment for not more than 20 years, or both. If the death of any person results from prohibited conduct under this new section, the punishment is imprisonment for any term of years or life (this does not have the death penalty provision contained in Section 2280).

Sec. 803—Amendments to section 2281 of title 18, United States Code.

This section makes amendments to Section 2281 of Title 18, United States Code. It corrects an error in subsection (c) in the cross-reference to the Norris-LaGuardia Act by substituting "section 13 (c) for the current 2 (c)" of that Act. This section strikes the definitions found in subsection (d), of "national of the United States," "territorial sea of the United States," and "United States."

This section adds a new subsection (e) that creates an exception to the provisions of the section for the activities of armed forces during an armed conflict as those terms are understood under the law of war. This exception is identical to that found in other sections of this Act.

Sec. 804—New section 2281A of title 18, United States Code.

This section establishes a new section 2281a in Title 18 that implements requirements in accordance with the 2005 Platforms Protocol. The 2005 Platforms Protocol criminalizes terrorist acts involving a fixed maritime platform.

New subsection (a)(1)(A) makes it an offense to, unlawfully and with the intent to intimidate a population or compel a government or an international organization to do or refrain from doing an act, (i) use against or discharge from a fixed platform, any explosive or radioactive material, or biological, chemical, or nuclear weapon, in a manner that causes or is likely to cause death or serious injury or damage; or (ii) discharge from a fixed platform oil, liquefied natural gas, or another hazardous or noxious substance, in a manner that causes or is likely to cause death or serious injury or damage.

Subsection (a)(1)(B) extends the penalties for injuring or killing a person in connection with the commission of an enumerated offense to the new crimes in subparagraph (E), as required by the 2005 Platforms Protocol, Article 2*ter,* paragraph 1.

Subsections (a)(1)(C) and (a)(2) implement the 2005 Platforms Protocol's application of attempt, conspiracy, and threat provisions to the new terrorist crimes. (*See* 2005 Platforms Protocol, Articles 2*bis,* 2*ter*).

Subsection (b) establishes jurisdiction over the prohibited activity, identical to the jurisdictional requirements of 2281.

Subsection (c) establishes exceptions that the statute does not apply to armed forces during an armed conflict or to the official exercise of military duties, as specified in Article 2*bis* of the 2005 Platforms Protocol.

Subsection (d) adds definitions of "continental shelf" and "fixed platform" that are not included in 18 U.S.C. § 2280.

The penalties for violations of 18 U.S.C. 2281a are a fine, imprisonment for not more than 20 years, or both. If the death of any person results from prohibited conduct under this new section, the punishment is imprisonment for any term of years or life (this does not have the death penalty provision contained in Section 2281).

Sec. 805—Ancillary Measure.

This section amends the meaning of the term "Federal Crime of Terrorism" to include violations of the new section 2280a and 2281a, created by sections 802 and 804 of this Act.

Subtitle B—Prevention of Nuclear Terrorism

Sec. 811—New Section 2332i of Title 18 of the U.S. Code.

This section creates a new section in the U.S. Code in Chapter 113B, Terrorism, of Title 18, to implement certain provisions of the International Convention for the Suppression of Acts of Nuclear Terrorism ("NTC") and the amendment to the Convention on the Physical Protection of Nuclear Material ("CPPNM"). Some of the conduct prohibited by the treaties is already covered by existing provisions in the U.S. Code. For instance, the NTC's prohibition against the possession or use of a nuclear explosive or radiation dispersal device with the intent to cause death or serious bodily injury may be covered by 18 U.S.C. § 832(c) (prohibiting the unlawful possession or use of a "radiological weapon") and/or 18 U.S.C. § 2332h (prohibiting the unlawful possession or use of a "weapon" or "device" designed to release radiation). Similarly, the prohibitions contained in both the NTC and the amendment to the CPPNM against causing damage to a nuclear facility overlap with

42 U.S.C. § 2284, which prohibits sabotage of nuclear facilities. The CPPNM amendment was also largely anticipated in the existing 18 U.S.C. § 831, which implemented the original CPPNM as well as additional prohibitions regarding nuclear material. However, the existing statutory coverage is not entirely coextensive with the offenses set forth in the new treaties. For example, the possession of radioactive material other than nuclear material, or threatening to cause damage to a nuclear facility, with the intent to cause death or serious bodily injury, damage to property or the environment, or to compel a person, international organization, or country to do or refrain from doing such an act, may not be prohibited by existing law.

Section 2332i(a) would therefore implement the provisions in Articles 2 and 5(a) of the NTC by creating two new criminal offenses regarding the possession and use of radioactive material, along with criminalizing, as required by the two treaties, attempts, threats, and conspiracies to commit the offenses. The provisions on damaging or interfering with a nuclear facility would also implement the CPPNM amendment's provision on nuclear facility sabotage. While nuclear facility sabotage is also addressed at 42 U.S.C. § 2284, that statute does not include a jurisdictional provision for offenders "found in" the United States and thus would not fully implement the obligations of the CPPNM amendment.

Specifically, section 2332i(a)(1)(A) would make it a criminal offense to knowingly possess radioactive material or make or possess a nuclear explosive, radiation exposure device or radiological dispersal device, with the intent to cause death or serious bodily injury or substantial damage to property or the environment. Section 2332i(a)(1)(B) would make it a criminal offense to knowingly use radioactive material or a nuclear explosive or radiological dispersal device or radiation exposure device, or damage or interfere with a nuclear facility in a manner that risks or causes contamination or exposure to radioactive material or radiation, with the intent to cause death or serious bodily injury or substantial damage to property or the environment, or with the knowledge that such effect is likely. With respect to this offense, the acts may also constitute offenses if they are done with the intent to compel a person, international organization, or state to do or refrain from doing an act. These offenses implement the NTC Article 2(1) and the acts of sabotage described in the amendment to Article 7 of the CPPNM. The CPPNM amendment also includes a specific exception for such sabotage acts "undertaken in conformity with the national law of the State Party in the territory of which the nuclear facility is situated." Such an exception would protect, for example, first responders but is not necessary in domestic law because the statute only criminalizes unlawful activity. Moreover, the government would not prosecute first responders for acts within their official duties in responding to an incident.

Section 2332i(a)(2) would criminalize a threat to commit either offense in subsection (a)(1) and a demand for possession of or access to radioactive material, a nuclear explosive, or a radiological dispersal device or a radiation exposure device or a nuclear facility by means of a threat or use of force. This language implements Article 2(2) of the NTC, with slightly different but equivalent language for purposes of U.S. law. It also implements the threat provi-

sion of the CPPNM amendment as applied to nuclear facility sabotage. Threats to commit the other acts identified in the CPPNM amendment are criminalized at 18 U.S.C. § 831.

Section 2332i(a)(3) would criminalize attempts to commit the offenses in subsection (a)(1) and conspiracies to commit the offenses in subsections (a)(1) and (a)(2). This language implements Article 2(3) and 2(4) of the NTC, as well as the amendment to Article 7 of the CPPNM as it pertains to sabotage attempts and participation. Attempts to threaten are not included in the NTC and therefore not included in the legislation. The NTC and CPPNM amendment do include the offense of "participation" in an attempt, but the legislation does not criminalize conspiracy to attempt since the crime does not have an analogue in U.S. law. Statutory provisions for conspiracy and attempt, as well as aiding and abetting liability through 18 U.S.C. § 2, are sufficient to implement the conventions' provisions on attempt and participation.

Section 2332i(b) would create jurisdiction for the offenses in subsection (a). Article 9 of the NTC and Article 8 of the CPPNM require jurisdiction over offenses occurring on the territory of a signatory, on board vessels flying the flag of a signatory, and on aircraft registered in a signatory, and over offenses committed by nationals of a signatory. Subsections (b)(1), (b)(2)(A), and (b)(2)(B) implement these jurisdictional grounds in the new legislation and include the special aircraft jurisdiction of the United States. The statute uses the term "vessel of the United States" and "vessel subject to the jurisdiction of the United States" (both terms defined in 46 U.S.C. § 70502) to define jurisdiction over vessels. The treaties also require that a State Party establish jurisdiction over the offenses in cases where the alleged offender is present in its territory and it does not extradite that person to a State Party that has implemented procedures in compliance with the treaties. Accordingly, the statute includes in subsection (b)(4) jurisdiction if an offender is found in the United States. The NTC also permits jurisdiction in a number of other cases, which this legislation adopts. There is jurisdiction over offenses committed against a U.S. national abroad; by a stateless person whose habitual residence is in the United States; against state or government facilities abroad; or in an attempt to compel the United States to do or abstain from doing any act.

In most respects, the adoption of these bases of jurisdiction parallels those in 18 U.S.C. § 831, which implements the United States' obligations under the CPPNM. There are nevertheless a few differences. First, 18 U.S.C. § 831 includes jurisdiction based on import or export activities, in accordance with the CPPNM. This jurisdictional basis, however, is not included in the NTC and therefore not included in section 2332i.

Section 2332i(c) would impose penalties for the commission of the offenses in subsection (a), in accordance with the obligation under Article 5(b) of the NTC and Article 7 of the CPPNM. The penalties prescribed here are a fine of not more than $2,000,000 and imprisonment for any term of years or life.

Section 2332i(d) deals with nonapplicability. Article 4(2) of the NTC and the amendment to Article 2 of the CPPNM specify that activities of armed forces are not covered by the conventions. The statutory exemption in section 2332i(d) implements this exception.

The statute draws on the definition of "military forces of a state" used in the Nuclear Terrorism Convention, Paragraph 6 of Article I. Consistent with the understandings included in the instruments of ratification for both the NTC and CPNNM (Treaty Doc. 110–4 at IX and Treaty Doc. 110–6 at 7) and with the Administration's interpretation of 18 U.S.C. 2332f, the exemption in section 2332i(d) is understood to include civilians who direct or organize the official activities of military forces of a State.

Section 2332i(e) defines relevant terms in the section, most importantly, "radioactive material," "nuclear material," "nuclear facility," and "device." The definitions of "radioactive material" and "device" are adopted directly from the NTC. The definition of "nuclear material" is adopted from existing section 831(f) in order to provide consistency among the statutes. It is slightly broader than the definition in the CPPNM or the NTC because it covers all plutonium, rather than "plutonium, except that with isotopic concentration exceeding 80 percent in plutonium-238." When amending section 831 in 1996, Congress expanded the definition in that statute beyond the CPPNM definition in order to address other hazardous materials that might be used in radioactive dispersal devices or in other terrorist activity.

The definition of "nuclear facility" is adopted partly from the NTC, in subsections (e)(6)(A) and (e)(6)(B), and partly, in subsection (e)(6)(C), from the definition of the same term in the CPPNM amendment because the statute covers offenses from both conventions involving nuclear facilities. A nuclear facility would include a nuclear reactor or plant used for nuclear material, as well as a conveyance for radioactive material. It would also include facilities that use nuclear material, provided that damage to or interference with the facility could lead to a significant release of radiation or radioactive material.

Sec. 812—Amendment to Section 831 of Title 18 of the U.S. Code.

Section 831 is amended to implement certain provisions of the CPPNM amendment. New subsection (a)(3) would criminalize the additional acts of nuclear smuggling required to be prohibited under the CPPNM amendment As with the other offenses in section 831, since 1996, slightly more material would be covered in the statute than in the treaty: section 831 includes "nuclear byproduct material" where the CPPNM does not, and section 831, as explained above, has a somewhat broader definition of nuclear material than the CPPNM. Congress's findings in 1996 supported this expansion.

Renumbered subsection (a)(8) retains the previous attempt offenses and adds an attempt offense with respect to the new smuggling offense (new subsection (a)(3)), consistent with the CPPNM amendment. Renumbered subsection (a)(9) would include conspiracies to commit the substantive offenses criminalized in the statute, as required by the CPPNM and its amendment.

The jurisdictional provisions in subsection (c) would be expanded to include some of the grounds listed in the new section 2332i to promote consistency in the implementation of these two conventions and the full assertion of permissible authority over potential nuclear material offenses. The amendment would add, consistent with section 2332i, jurisdiction over offenses committed by stateless

persons with their habitual residence in the United States. It would also extend jurisdiction over offenses against state or government facilities abroad and offenses committed on board an aircraft or vessel registered in the United States. Simpler language borrowed from the new section 2332i would replace current subsection (c)(5) to achieve the same effect of jurisdiction over terrorist acts done to influence the United States government or that constitute a threat directed at the United States.

Similarly to section 2332i(d), and elsewhere in this Act, a new subsection (d) in section 831 would provide exemptions to jurisdiction for activities of armed forces, implementing the amendment to Article 2 of the CPPNM. The statute also draws on the definition of "military forces of a state" used in the Nuclear Terrorism Convention, Paragraph 6 of Article I. Consistent with the understandings included in the instruments of ratification for both the NTC and CPNNM (Treaty Doc. 110–4 at IX and Treaty Doc. 110–6 at 7) and with the interpretation of 18 U.S.C. 2332f, the exemption in section 2332i(d) is understood to include civilians who direct or organize the official activities of military forces of a State.

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

* * * * * * *

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

* * * * * * *

[TITLE VI—REPORTING REQUIREMENT

TITLE VI—OVERSIGHT

* * * * * * *

Sec. 602. Declassification of significant decisions, orders, and opinions.
Sec. 603. Annual reports.
Sec. 604. Public reporting by persons subject to orders.

* * * * * * *

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 [of such person's presence in the United States] indicate that such person may engage in [such activities in the United States] *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]

(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

(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, an 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(h), 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 designate 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 immediately 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. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.

(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 jurisdiction 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 the court established under subsection (a) 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 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) shall appoint an individual who has 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) may appoint an individual or organization 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.

(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), the amicus curiae shall provide to the court, as appropriate—

(A) legal arguments that advance the protection of individual privacy and civil liberties;

(B) information related to intelligence collection or communications technology; or

(C) 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)(A), the amicus curiae—

(i) shall have access to all relevant legal precedent, and any 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 amicus curiae 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 proceedings 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 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.

(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.

* * * * * * *

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 activi-

ties 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) DIRECTIONS.—An order approving an electronic surveillance under this section shall 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, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, 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 National 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), 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, 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) 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.

(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.

[(f)**]** *(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.

[(g)**]** *(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.

[(h)**]** *(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.

[(i)**]** *(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).

USE OF INFORMATION

SEC. 106. (a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No

otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to

discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) If the United States district court pursuant to subsection (f) determine that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any 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, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person.

(j) If an emergency employment of electronic surveillance is authorized under ⟦section 105(e)⟧ *subsection (e) or (f) of section 105* and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or sus-

pended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or 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.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 108. (a)(1) On a semiannual basis the Attorney General shall fully inform **[**the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate,**]** *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* concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(2) Each report under the first sentence of paragraph (1) shall include a description of—

(A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;

(B) each criminal case in which information acquired under this Act has been authorized for use at trial during the period covered by such report; **[**and**]**

(C) the total number of emergency employments of electronic surveillance under section 105(e) and the total number of subsequent orders approving or denying such electronic surveillance**[**.**]***; and*

(D) the total number of authorizations under section 105(f) and the total number of subsequent emergency em-

ployments of electronic surveillance under section 105(e) or emergency physical searches pursuant to section 301(e).

(b) On or before one year after the effective date of this Act and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

* * * * * * *

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

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 306. On a semiannual basis the Attorney General shall fully inform the [Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the Senate,] *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* concerning all physical searches conducted pursuant to this title. On a semiannual basis the Attorney General shall also provide to those committees [and the Committee on the Judiciary of the House of Representatives] a report setting forth with respect to the preceding six-month period—

(1) the total number of applications made for orders approving physical searches under this title;

(2) the total number of such orders either granted, modified, or denied;

(3) the number of physical searches which involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where the Attorney General provided notice pursuant to section 305(b); and

(4) the total number of emergency physical searches authorized by the Attorney General under section 304(e) and the total number of subsequent orders approving or denying such physical searches.

* * * * * * *

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

DEFINITIONS

SEC. 401. As used in this title:

(1) The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 101 of this Act.

(2) The terms "pen register" and "trap and trace device" have the meanings given such terms in section 3127 of title 18, United States Code.

(3) The term "aggrieved person" means any person—

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this title; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this title to capture incoming electronic or other communications impulses.

(4)(A) The term "specific selection term"—

(i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

(ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.

(B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that—

(i) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or

(ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

(C) For purposes of subparagraph (A), the term "address" means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).

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**[**; and**]***;*

(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.

(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 network 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.

(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.

AUTHORIZATION DURING EMERGENCIES

SEC. 403. (a) Notwithstanding any other provision of this title, when the Attorney General makes a determination described in subsection (b), the Attorney General may authorize the installation

and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information 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 if—

(1) a judge referred to in section 402(b) of this Act is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and

(2) an application in accordance with section 402 of this Act is made to such judge as soon as practicable, but not more than 7 days, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.

(b) A determination under this subsection is a reasonable determination by the Attorney General that—

(1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information 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 before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 402 of this Act; and

(2) the factual basis for issuance of an order under such section 402 to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.

(c)(1) In the absence of an order applied for under subsection (a)(2) approving the installation and use of a pen register or trap and trace device authorized under this section, the installation and use of the pen register or trap and trace device, as the case may be, shall terminate at the earlier of—

(A) when the information sought is obtained;

(B) when the application for the order is denied under section 402 of this Act; or

(C) 7 days after the time of the authorization by the Attorney General.

(2) In the event that an application for an order applied for under subsection (a)(2) is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 402 of this Act is issued approving the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, 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 the

use of the pen register or trap and trace device, as the case may be, 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.

(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 406. (a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all uses of pen registers and trap and trace devices pursuant to this title.

(b) On a semiannual basis, the Attorney General shall also provide to the committees referred to in subsection (a) and to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving the use of pen registers or trap and trace devices under this title;

(2) the total number of such orders either granted, modified, or denied**[**; and**]***;*

(3) the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 403, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices**[**.**]***;*

(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this title; and

(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).

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

SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a)(1) Subject to paragraph (3), 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 requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence infor-

mation 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.

(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a); 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 production of tangible things under this section on behalf of a judge of that court; and

(2) shall include—

(A) a specific selection term to be used as the basis for the production of the tangible things sought;

[(A) a statement**]** *(B) in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement* of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation[; and]*;*

(C) in the case of an application for the production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism, a statement of facts showing that—

(i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and

(ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and

[(B)] *(D)* an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) *and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g)*, the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified[;], *including each specific selection term to be used as the basis for the production;*

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things[; and]*;*

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a)[.]*; and*

(F) in the case of an application described in subsection (b)(2)(C), shall—

(i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;

(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection;

(iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii);

(iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii);

(v) provide that, when produced, such records be in a form that will be useful to the Government;

(vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production; and

(vii) direct the Government to—

(I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and

(II) destroy all call detail records produced under the order as prescribed by such procedures.

(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2).

(d)(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things **[**pursuant to an order**]** *pursuant to an order issued or an emergency production required* under this section, other than to—

(A) those persons to whom disclosure is necessary to comply with **[**such order**]** *such order or such emergency production*;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to **[**the order**]** *the order or the emergency production*; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom **[**an order**]** *an order or emergency production* is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to [an order] *an order or emergency production* under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

[(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.]

(e)(1) No cause of action shall lie in any court against a person who—

(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f)(1) In this subsection—

(A) the term "production order" means an order to produce any tangible thing under this section; and

(B) the term "nondisclosure order" means an order imposed under subsection (d).

(2)(A)(i) A person receiving a production order may challenge the legality of [that order] *the production order or any nondisclosure order imposed in connection with the production order* by filing a petition with the pool established by section 103(e)(1). [Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 103(e)(1).]

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 103(e)(1). Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 103(e)(2).

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

[(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.**]**

[(iii)**]** *(ii)* If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 103(b), which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) MINIMIZATION PROCEDURES.—

(1) IN GENERAL.—[Not later than 180 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the] *The* Attorney General shall adopt*, and update as appropriate,* specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title.

(2) DEFINED.—In this section, the term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the 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;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(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; and

(C) notwithstanding subparagraphs (A) and (B), 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.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall limit the authority of the court established under section 103(a) to impose additional, particularized minimization procedures with regard to the production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.

(h) USE OF INFORMATION.—Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this title shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(i) EMERGENCY AUTHORITY FOR PRODUCTION OF TANGIBLE THINGS.—

(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General—

(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this subsection; and

(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production 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 the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

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

(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production 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 a political subdivision thereof, and no information concerning any United States person acquired from such production 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).

(j) COMPENSATION.—The Government shall compensate a person for reasonable expenses incurred for—

(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

(k) DEFINITIONS.—In this section:

(1) IN GENERAL.—The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" have the meanings provided those terms in section 101.

(2) ADDRESS.—The term "address" means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(3) CALL DETAIL RECORD.—The term "call detail record"—

(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and

(B) does not include—

(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

(ii) the name, address, or financial information of a subscriber or customer; or

(iii) cell site location or global positioning system information.

(4) SPECIFIC SELECTION TERM.—

(A) TANGIBLE THINGS.—

(i) IN GENERAL.—Except as provided in subparagraph (B), a "specific selection term"—

(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

(II) identifies a broad geographic region, including the United States, a city, a county, a State,

a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term "specific selection term" means a term that specifically identifies an individual, account, or personal device.

SEC. 502. CONGRESSIONAL OVERSIGHT.

(a) On an annual basis, the Attorney General shall fully inform the [Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate] *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* concerning all requests for the production of tangible things under section 501.

(b) In April of each year, the Attorney General shall submit to the House and Senate Committees on the Judiciary and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence a report setting forth with respect to the preceding calendar year—

(1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;

(2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;

(3) the total number of such orders either granted, modified, or denied;

(4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;

(5) the total number of such orders either granted, modified, or denied;

[(1)] *(6)* the total number of applications made for orders approving requests for the production of tangible things under section 501;

[(2)] *(7)* the total number of such orders either granted, modified, or denied; and

[(3)] *(8)* the number of such orders either granted, modified, or denied for the production of each of the following:

(A) Library circulation records, library patron lists, book sales records, or book customer lists.

(B) Firearms sales records.

(C) Tax return records.

(D) Educational records.

(E) Medical records containing information that would identify a person.

(c)(1) In April of each year, the Attorney General shall submit to Congress a report setting forth with respect to the preceding year—

(A) the total number of applications made for orders approving requests for the production of tangible things under section 501; [and]

(B) the total number of such orders either granted, modified, or denied[.]*;*

(C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;

(D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and

(E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).

(2) Each report under this subsection shall be submitted in unclassified form.

* * * * * * *

TITLE VI—[REPORTING REQUIREMENT] *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) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this Act, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and]

(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).

(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. 602. DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS.

(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as

defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term "specific selection term", and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

(b) REDACTED FORM.—The Director of National Intelligence, in consultation with the Attorney General, may satisfy the requirement under subsection (a) to make a decision, order, or opinion described in such subsection publicly available to the greatest extent practicable by making such decision, order, or opinion publicly available in redacted form.

(c) NATIONAL SECURITY WAIVER.—The Director of National Intelligence, in consultation with the Attorney General, may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a), if—

(1) the Director of National Intelligence, in consultation with the Attorney General, determines that a waiver of such requirement is necessary to protect the national security of the United States or properly classified intelligence sources or methods; and

(2) the Director of National Intelligence makes publicly available an unclassified statement prepared by the Attorney General, in consultation with the Director of National Intelligence—

(A) summarizing the significant construction or interpretation of any provision of law, which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision; and

(B) that specifies that the statement has been prepared by the Attorney General and constitutes no part of the opinion of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review.

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 the number of targets of such orders;

(2) the total number of orders issued pursuant to section 702 and a good faith estimate of—

(A) the number of search terms concerning a known United States person used to retrieve the unminimized contents 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; and

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

(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; and

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

(4) 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;

(5) 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

(6) 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), (4), or (5) 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)(A), (2)(B), and (5)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

(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.

(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)(B) 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) 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.

SEC. 604. PUBLIC REPORTING BY PERSONS SUBJECT TO ORDERS.

(a) REPORTING.—A person subject to a nondisclosure requirement accompanying an order or directive under this Act or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

(A) the number of national security letters received, reported in bands of 1000 starting with 0–999;

(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0–999;

(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0–999;

(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents reported in bands of 1000 starting with 0–999;

(E) the number of orders received under this Act for noncontents, reported in bands of 1000 starting with 0–999; and

(F) the number of customer selectors targeted under orders under this Act for noncontents, reported in bands of 1000 starting with 0–999, pursuant to—

(i) title IV;

(ii) title V with respect to applications described in section 501(b)(2)(B); and

(iii) title V with respect to applications described in section 501(b)(2)(C).

(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

(A) the number of national security letters received, reported in bands of 500 starting with 0–499;

(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0–499;

(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

(E) the number of orders received under this Act for noncontents, reported in bands of 500 starting with 0–499; and

(F) the number of customer selectors targeted under orders received under this Act for noncontents, reported in bands of 500 starting with 0–499.

(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the into separate categories of—

(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249.

(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of—

(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0–99; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0–99.

(b) PERIOD OF TIME COVERED BY REPORTS.—

(1) A report described in paragraph (1) or (2) of subsection (a) shall include only information—

(A) relating to national security letters for the previous 180 days; and

(B) relating to authorities under this Act for the 180-day period of time ending on the date that is not less than 180 days prior to the date of the publication of such report, except that with respect to a platform, product, or service for which a person did not previously receive an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received.

(2) A report described in paragraph (3) of subsection (a) shall include only information relating to the previous 180 days.

(3) A report described in paragraph (4) of subsection (a) shall include only information for the 1-year period of time ending on the date that is not less than 1 year prior to the date of the publication of such report.

(c) OTHER FORMS OF AGREED TO PUBLICATION.—Nothing in this section prohibits the Government and any person from jointly agreeing to the publication of information referred to in this subsection in a time, form, or manner other than as described in this section.

(d) 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) NATIONAL SECURITY LETTER.—The term "national security letter" has the meaning given that term under section 603.

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

* * * * * * *

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 (i)(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; and

(5) 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 (g), 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 (i)(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 (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) 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 (i).

(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 (i).

(f) 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.

(g) 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 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 (f) 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 (i)(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 (i).

(h) 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 directive, 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.

(i) 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 and minimization procedures adopted in accordance with subsections (d) and (e), 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 and minimization procedures adopted in accordance with subsections (d) and (e) 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 and minimization procedures adopted in accordance with subsections (d) and (e) 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 (g) 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.

(3) ORDERS.—

(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) 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 (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) 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 information 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 (g) and the procedures adopted in accordance with subsections (d) and (e) 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 related 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.

(j) 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.

(k) 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.

(l) ASSESSMENTS AND REVIEWS.—

(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 and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) 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 and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(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.

* * * * * * *

USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005

* * * * * * *

TITLE I—USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT

* * * * * * *

SEC. 102. USA PATRIOT ACT SUNSET PROVISIONS.

(a) IN GENERAL.—Section 224 of the USA PATRIOT Act is repealed.

(b) SECTIONS 206 AND 215 SUNSET.—

(1) IN GENERAL.—Effective [June 1, 2015] *December 15, 2019*, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

(2) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

* * * * * * *

SEC. 106A. AUDIT ON ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES.

(a) AUDIT.—The Inspector General of the Department of Justice shall perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided to the Federal Bureau of Investigation under title

V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

(b) REQUIREMENTS.—The audit required under subsection (a) shall include—

(1) an examination of each instance in which the Attorney General, any other officer, employee, or agent of the Department of Justice, the Director of the Federal Bureau of Investigation, or a designee of the Director, submitted an application to the Foreign Intelligence Surveillance Court (as such term is defined in section 301(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(3))) for an order under section 501 of such Act during the calendar years of 2002 through 2006 *and calendar years 2012 through 2014*, including—

(A) whether the Federal Bureau of Investigation requested that the Department of Justice submit an application and the request was not submitted to the court (including an examination of the basis for not submitting the application);

(B) whether the court granted, modified, or denied the application (including an examination of the basis for any modification or denial);

[(2) the justification for the failure of the Attorney General to issue implementing procedures governing requests for the production of tangible things under such section in a timely fashion, including whether such delay harmed national security;

[(3) whether bureaucratic or procedural impediments to the use of such requests for production prevent the Federal Bureau of Investigation from taking full advantage of the authorities provided under section 501 of such Act;**]**

[(4)**]** *(2)* any noteworthy facts or circumstances relating to orders under such section, including any improper or illegal use of the authority provided under such section; and

[(5)**]** *(3)* an examination of the effectiveness of such section as an investigative tool, including—

(A) the categories of records obtained and the importance of the information acquired to the intelligence activities of the Federal Bureau of Investigation or any other Department or agency of the Federal Government;

(B) the manner in which such information is collected, retained, analyzed, and disseminated by the Federal Bureau of Investigation, including any direct access to such information (such as access to "raw data") provided to any other Department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

[(C) with respect to calendar year 2006, an examination of the minimization procedures adopted by the Attorney General under section 501(g) of such Act and whether such minimization procedures protect the constitutional rights of United States persons;**]**

(C) with respect to calendar years 2012 through 2014, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and

whether the minimization procedures adequately protect the constitutional rights of United States persons;

(D) whether, and how often, the Federal Bureau of Investigation utilized information acquired pursuant to an order under section 501 of such Act to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community [(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)))], or to other Federal, State, local, or tribal government Departments, agencies, or instrumentalities; and

(E) whether, and how often, the Federal Bureau of Investigation provided such information to law enforcement authorities for use in criminal proceedings.

(c) SUBMISSION DATES.—

(1) PRIOR YEARS.—Not later than one year after the date of the enactment of this Act, or upon completion of the audit under this section for calendar years 2002, 2003, and 2004, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2002, 2003, and 2004.

(2) CALENDAR YEARS 2005 AND 2006.—Not later than December 31, 2007, or upon completion of the audit under this section for calendar years 2005 and 2006, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2005 and 2006.

(3) CALENDAR YEARS 2012 THROUGH 2014.—Not later than 1 year after the date of enactment of the USA FREEDOM Act of 2015, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under subsection (a) for calendar years 2012 through 2014.

(d) INTELLIGENCE ASSESSMENT.—

(1) IN GENERAL.—For the period beginning on January 1, 2012, and ending on December 31, 2014, the Inspector General of the Intelligence Community shall assess—

(A) the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community;

(B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;

(C) the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and

(D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)).

(2) SUBMISSION DATE FOR ASSESSMENT.—Not later than 180 days after the date on which the Inspector General of the Department of Justice submits the report required under subsection (c)(3), the Inspector General of the Intelligence Community shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2012 through 2014.

[(d)**]** *(e)* PRIOR NOTICE TO ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE; COMMENTS.—

(1) NOTICE.—Not less than 30 days before the submission of **[**a report under subsection (c)(1) or (c)(2)**]** *any report under subsection (c) or (d)*, the **[**Inspector General of the Department of Justice**]** *Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, and any Inspector General of an element of the intelligence community that prepares a report to assist the Inspector General of the Department of Justice or the Inspector General of the Intelligence Community in complying with the requirements of this section* shall provide such report to the Attorney General and the Director of National Intelligence.

(2) COMMENTS.—The Attorney General or the Director of National Intelligence may provide comments to be included in **[**the reports submitted under subsections (c)(1) and (c)(2)**]** *any report submitted under subsection (c) or (d)* as the Attorney General or the Director of National Intelligence may consider necessary.

[(e)**]** *(f)* UNCLASSIFIED FORM.—**[**The reports submitted under subsections (c)(1) and (c)(2)**]** *Each report submitted under subsection (c)* and any comments included under **[**subsection (d)(2)**]** *subsection (e)(2)* shall be in unclassified form, but may include a classified annex.

(g) DEFINITIONS.—In this section:

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

(2) UNITED STATES PERSON.—The term "United States person" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

* * * * * * *

SEC. 118. REPORTS ON NATIONAL SECURITY LETTERS.

(a) EXISTING REPORTS.—Any report made to a committee of Congress regarding national security letters under section 2709(c)(1) of title 18, United States Code, section 626(d) or 627(c) of the Fair Credit Reporting Act (15 U.S.C. 1681u(d) or 1681v(c)),

section 1114(a)(3) or 1114(a)(5)(D) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(3) or 3414(a)(5)(D)), or section 802(b) of the National Security Act of 1947 (50 U.S.C. 436(b)) shall also be made to the Committees on the Judiciary of the House of Representatives and the Senate.

(b) ENHANCED OVERSIGHT OF FAIR CREDIT REPORTING ACT COUNTERTERRORISM NATIONAL SECURITY LETTER.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681(v)) is amended by inserting at the end the following new subsection:

"(f) REPORTS TO CONGRESS.—(1) On a semi-annual basis, the Attorney General shall fully inform the Committee on the Judiciary, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to subsection (a).

"(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947 (50 U.S.C. 415b).".

(c) REPORT ON REQUESTS FOR NATIONAL SECURITY LETTERS.—

(1) IN GENERAL.—In April of each year, the Attorney General shall submit to Congress an aggregate report setting forth with respect to the preceding year the total number of requests made by the Department of Justice for information concerning different [United States] persons under—

(A) section 2709 of title 18, United States Code (to access certain communication service provider records)[, excluding the number of requests for subscriber information];

(B) section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414) (to obtain financial institution customer records);

(C) section 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports);

(D) section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports); and

(E) section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

(2) CONTENT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include a good faith estimate of the total number of requests described in paragraph (1) requiring disclosure of information concerning—

(i) United States persons; and

(ii) persons who are not United States persons.

(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title

18, United States Code, a report required under this subsection need not separate the number of requests into each of the categories described in subparagraph (A).

[(2)**]** *(3)* UNCLASSIFIED FORM.—The report under this section shall be submitted in unclassified form.

(d) NATIONAL SECURITY LETTER DEFINED.—In this section, the term "national security letter" means a request for information under one of the following provisions of law:

(1) Section 2709(a) of title 18, United States Code (to access certain communication service provider records).

(2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)(A)) (to obtain financial institution customer records).

(3) Section 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports).

(4) Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports).

(5) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

* * * * * * *

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 39—EXPLOSIVES AND OTHER DANGEROUS ARTICLES

§ 831. Prohibited transactions involving nuclear materials

(a) Whoever, if one of the circumstances described in subsection (c) of this section occurs—

(1) without lawful authority, intentionally receives, possesses, uses, transfers, alters, disposes of, or disperses any nuclear material or nuclear byproduct material and—

(A) thereby knowingly causes the death of or serious bodily injury to any person or substantial damage to property or to the environment; or

(B) circumstances exist, or have been represented to the defendant to exist, that are likely to cause the death or serious bodily injury to any person, or substantial damage to property or to the environment;

(2) with intent to deprive another of nuclear material or nuclear byproduct material, knowingly—

(A) takes and carries away nuclear material or nuclear byproduct material of another without authority;

(B) makes an unauthorized use, disposition, or transfer, of nuclear material or nuclear byproduct material belonging to another; or

(C) uses fraud and thereby obtains nuclear material or nuclear byproduct material belonging to another;

(3) without lawful authority, intentionally carries, sends or moves nuclear material into or out of a country;

⟦(3)⟧ *(4)* knowingly—

(A) uses force; or

(B) threatens or places another in fear that any person other than the actor will imminently be subject to bodily injury;

and thereby takes nuclear material or nuclear byproduct material belonging to another from the person or presence of any other;

⟦(4)⟧ *(5)* intentionally intimidates any person and thereby obtains nuclear material or nuclear byproduct material belonging to another;

⟦(5)⟧ *(6)* with intent to compel any person, international organization, or governmental entity to do or refrain from doing any act, knowingly threatens to engage in conduct described in paragraph (2)(A) or (3) of this subsection;

⟦(6)⟧ *(7)* knowingly threatens to use nuclear material or nuclear byproduct material to cause death or serious bodily injury to any person or substantial damage to property or to the environment under circumstances in which the threat may reasonably be understood as an expression of serious purposes;

⟦(7)⟧ *(8)* attempts to commit ⟦an offense under paragraph (1), (2), (3), or (4)⟧ *any act prohibited under paragraphs (1) through (5)* of this subsection; or

⟦(8)⟧ *(9)* is a party to a conspiracy of two or more persons to commit ⟦an offense under paragraph (1), (2), (3), or (4)⟧ *any act prohibited under paragraphs (1) through (7)* of this subsection, if any of the parties intentionally engages in any conduct in furtherance of such offense;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under—

(1) paragraphs (1) through ⟦(7)⟧ *(8)* of subsection (a) of this section is—

(A) a fine under this title; and

(B) imprisonment—

(i) for any term of years or for life (I) if, while committing the offense, the offender knowingly causes the death of any person; or (II) if, while committing an offense under paragraph (1) or (3) of subsection (a) of this section, the offender, under circumstances manifesting extreme indifference to the life of an individual, knowingly engages in any conduct and thereby recklessly causes the death of or serious bodily injury to any person; and

(ii) for not more than 20 years in any other case; and

(2) paragraph ⟦(8)⟧ *(9)* of subsection (a) of this section is—

(A) a fine under this title; and

(B) imprisonment—

(i) for not more than 20 years if the offense which is the object of the conspiracy is punishable under paragraph (1)(B)(i); and

(ii) for not more than 10 years in any other case.

(c) The circumstances referred to in subsection (a) of this section are that—

(1) the offense is committed in the United States or the special maritime and territorial jurisdiction of the United States, or the special aircraft jurisdiction of the United States (as defined in section 46501 of title 49);

(2) an offender or a victim is—

(A) a national of the United States *or a stateless person whose habitual residence is in the United States*; or

(B) a United States corporation or other legal entity;

(3) after the conduct required for the offense occurs the defendant is found in the United States, even if the conduct required for the offense occurs outside the United States;

(4) the conduct required for the offense occurs with respect to the carriage of a consignment of nuclear material or nuclear byproduct material for peaceful purposes by any means of transportation intended to go beyond the territory of the state where the shipment originates beginning with the departure from a facility of the shipper in that state and ending with the arrival at a facility of the receiver within the state of ultimate destination and either of such states is the United States; **[**or**]**

[(5) either—

[(A) the governmental entity under subsection (a)(5) is the United States; or

[(B) the threat under subsection (a)(6) is directed at the United States.**]**

(5) the offense is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed;

(6) the offense is committed outside the United States and against any state or government facility of the United States; or

(7) the offense is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States.

(d) NONAPPLICABILITY.—This section does not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

[(d)**]** *(e)* The Attorney General may request assistance from the Secretary of Defense under chapter 18 of title 10 in the enforcement of this section and the Secretary of Defense may provide such assistance in accordance with chapter 18 of title 10, except that the Secretary of Defense may provide such assistance through any Department of Defense personnel.

[(e)**]** *(f)*(1) The Attorney General may also request assistance from the Secretary of Defense under this subsection in the enforcement of this section. Notwithstanding section 1385 of this title, the

Secretary of Defense may, in accordance with other applicable law, provide such assistance to the Attorney General if—

(A) an emergency situation exists (as jointly determined by the Attorney General and the Secretary of Defense in their discretion); and

(B) the provision of such assistance will not adversely affect the military preparedness of the United States (as determined by the Secretary of Defense in such Secretary's discretion).

(2) As used in this subsection, the term "emergency situation" means a circumstance—

(A) that poses a serious threat to the interests of the United States; and

(B) in which—

(i) enforcement of the law would be seriously impaired if the assistance were not provided; and

(ii) civilian law enforcement personnel are not capable of enforcing the law.

(3) Assistance under this section may include—

(A) use of personnel of the Department of Defense to arrest persons and conduct searches and seizures with respect to violations of this section; and

(B) such other activity as is incidental to the enforcement of this section, or to the protection of persons or property from conduct that violates this section.

(4) The Secretary of Defense may require reimbursement as a condition of assistance under this section.

(5) The Attorney General may delegate the Attorney General's function under this subsection only to a Deputy, Associate, or Assistant Attorney General.

[(f)] *(g)* As used in this section—

(1) the term "nuclear material" means material containing any—

(A) plutonium;

(B) uranium not in the form of ore or ore residue that contains the mixture of isotopes as occurring in nature;

(C) enriched uranium, defined as uranium that contains the isotope 233 or 235 or both in such amount that the abundance ratio of the sum of those isotopes to the isotope 238 is greater than the ratio of the isotope 235 to the isotope 238 occurring in nature; or

(D) uranium 233;

(2) the term "nuclear byproduct material" means any material containing any radioactive isotope created through an irradiation process in the operation of a nuclear reactor or accelerator;

(3) the term "international organization" means a public international organization designated as such pursuant to section 1 of the International Organizations Immunities Act (22 U.S.C. 288) or a public organization created pursuant to treaty or other agreement under international law as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs;

(4) the term "serious bodily injury" means bodily injury which involves—

(A) a substantial risk of death;
(B) extreme physical pain;
(C) protracted and obvious disfigurement; or
(D) protracted loss or impairment of the function of a bodily member, organ, or mental faculty;
(5) the term "bodily injury" means—
(A) a cut, abrasion, bruise, burn, or disfigurement;
(B) physical pain;
(C) illness;
(D) impairment of a function of a bodily member, organ, or mental faculty; or
(E) any other injury to the body, no matter how temporary;
(6) the term "national of the United States" has the same meaning as in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)); **[**and**]**
(7) the term "United States corporation or other legal entity" means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession, or district of the United States**[**.**]***;*
(8) the term "armed conflict" has the meaning given that term in section 2332f(e)(11) of this title;
(9) the term "military forces of a state" means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;
(10) the term "state" has the same meaning as that term has under international law, and includes all political subdivisions thereof;
(11) the term "state or government facility" has the meaning given that term in section 2332f(e)(3) of this title; and
(12) the term "vessel of the United States" has the meaning given that term in section 70502 of title 46.

* * * * * * *

CHAPTER 111—SHIPPING

§ 2280. Violence against maritime navigation

(a) OFFENSES.—
(1) IN GENERAL.—A person who unlawfully and intentionally—
(A) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation;

(B) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship;

(C) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship;

(D) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship;

(E) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if such act is likely to endanger the safe navigation of a ship;

(F) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safe navigation of a ship;

(G) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (F); or

(H) attempts or conspires to do any act prohibited under subparagraphs (A) through (G),

shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life.

(2) THREAT TO NAVIGATION.—A person who threatens to do any act prohibited under paragraph (1)(B), (C) or (E), with apparent determination and will to carry the threat into execution, if the threatened act is likely to endanger the safe navigation of the ship in question, shall be fined under this title, imprisoned not more than 5 years, or both.

(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a)—

(1) in the case of a covered ship, if—

(A) such activity is committed—

(i) against or on board ⟦a ship flying the flag of the United States⟧ *a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46)* at the time the prohibited activity is committed;

(ii) in the United States*, including the territorial seas*; or

(iii) by a national of the United States*, by a United States corporation or legal entity,* or by a stateless person whose habitual residence is in the United States;

(B) during the commission of such activity, a national of the United States is seized, threatened, injured or killed; or

(C) the offender is later found in the United States after such activity is committed;

(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; and

(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

(c) BAR TO PROSECUTION.—It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in [section 2(c)] *section 13(c)* of the Norris-LaGuardia Act, as amended (29 U.S.C. 113(c)).

[(d) DELIVERY OF SUSPECTED OFFENDER.—The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under Article 3 of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation may deliver such person to the authorities of a State Party to that Convention. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a State Party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense.

[(e) DEFINITIONS.—In this section—

["covered ship" means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country.]

["national of the United States" has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)).]

["territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law.]

["ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up.]

[“United States”, when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and all territories and possessions of the United States.]

(d) DEFINITIONS.—As used in this section, section 2280a, section 2281, and section 2281a, the term—

(1) “applicable treaty” means—

(A) the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

(B) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;

(C) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;

(D) International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;

(E) the Convention on the Physical Protection of Nuclear Material, done at Vienna on 26 October 1979;

(F) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;

(G) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;

(H) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997; and

(I) International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9 December 1999;

(2) “armed conflict” does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature;

(3) “biological weapon” means—

(A) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes; or

(B) weapons, equipment, or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict;

(4) “chemical weapon” means, together or separately—

(A) toxic chemicals and their precursors, except where intended for—

(i) industrial, agricultural, research, medical, pharmaceutical, or other peaceful purposes;

(ii) protective purposes, namely those purposes directly related to protection against toxic chemicals and to protection against chemical weapons;

(iii) military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; or

(iv) law enforcement including domestic riot control purposes,

as long as the types and quantities are consistent with such purposes;

(B) munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in subparagraph (A), which would be released as a result of the employment of such munitions and devices; and

(C) any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (B);

(5) "covered ship" means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country;

(6) "explosive material" has the meaning given the term in section 841(c) and includes explosive as defined in section 844(j) of this title;

(7) "infrastructure facility" has the meaning given the term in section 2332f(e)(5) of this title;

(8) "international organization" has the meaning given the term in section 831(f)(3) of this title;

(9) "military forces of a state" means the armed forces of a state which are organized, trained, and equipped under its internal law for the primary purpose of national defense or security, and persons acting in support of those armed forces who are under their formal command, control, and responsibility;

(10) "national of the United States" has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

(11) "Non-Proliferation Treaty" means the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow on 1 July 1968;

(12) "Non-Proliferation Treaty State Party" means any State Party to the Non-Proliferation Treaty, to include Taiwan, which shall be considered to have the obligations under the Non-Proliferation Treaty of a party to that treaty other than a Nuclear Weapon State Party to the Non-Proliferation Treaty;

(13) "Nuclear Weapon State Party to the Non-Proliferation Treaty" means a State Party to the Non-Proliferation Treaty that is a nuclear-weapon State, as that term is defined in Article IX(3) of the Non-Proliferation Treaty;

(14) "place of public use" has the meaning given the term in section 2332f(e)(6) of this title;

(15) "precursor" has the meaning given the term in section 229F(6)(A) of this title;

(16) "public transport system" has the meaning given the term in section 2332f(e)(7) of this title;

(17) "serious injury or damage" means—

(A) serious bodily injury,

(B) extensive destruction of a place of public use, State or government facility, infrastructure facility, or public transportation system, resulting in major economic loss, or

(C) substantial damage to the environment, including air, soil, water, fauna, or flora;

(18) "ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up;

(19) "source material" has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

(20) "special fissionable material" has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

(21) "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law;

(22) "toxic chemical" has the meaning given the term in section 229F(8)(A) of this title;

(23) "transport" means to initiate, arrange or exercise effective control, including decisionmaking authority, over the movement of a person or item; and

(24) "United States", when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and all territories and possessions of the United States.

(e) EXCEPTIONS.—This section shall not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

(f) DELIVERY OF SUSPECTED OFFENDER.—The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under section 2280 or section 2280a may deliver such person to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a state party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense.

(g)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.

§ 2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction

(a) OFFENSES.—

(1) IN GENERAL.—Subject to the exceptions in subsection (c), a person who unlawfully and intentionally—

(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

(i) uses against or on a ship or discharges from a ship any explosive or radioactive material, biological, chemical, or nuclear weapon or other nuclear explosive device in a manner that causes or is likely to cause death to any person or serious injury or damage;

(ii) discharges from a ship oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death to any person or serious injury or damage; or

(iii) uses a ship in a manner that causes death to any person or serious injury or damage;

(B) transports on board a ship—

(i) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, death to any person or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act;

(ii) any biological, chemical, or nuclear weapon or other nuclear explosive device, knowing it to be a biological, chemical, or nuclear weapon or other nuclear explosive device;

(iii) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an International Atomic Energy Agency comprehensive safeguards agreement, except where—

(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of the Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

(iv) any equipment, materials, or software or related technology that significantly contributes to the design or manufacture of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

(I) the country to the territory of which or under the control of which such item is transferred is a Nuclear Weapon State Party to the Non-Proliferation Treaty; and

(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of a Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

(v) any equipment, materials, or software or related technology that significantly contributes to the delivery of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

(II) such item is intended for the delivery system of a nuclear weapon or other nuclear explosive device of a Nuclear Weapon State Party to the Non-Proliferation Treaty; or

(vi) any equipment, materials, or software or related technology that significantly contributes to the design, manufacture, or delivery of a biological or chemical weapon, with the intention that it will be used for such purpose;

(C) transports another person on board a ship knowing that the person has committed an act that constitutes an offense under section 2280 or subparagraph (A), (B), (D), or (E) of this section or an offense set forth in an applicable treaty, as specified in section 2280(d)(1), and intending to assist that person to evade criminal prosecution;

(D) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (C), or subsection (a)(2), to the extent that the subsection (a)(2) offense pertains to subparagraph (A); or

(E) attempts to do any act prohibited under subparagraph (A), (B) or (D), or conspires to do any act prohibited by subparagraphs (A) through (E) or subsection (a)(2),

shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

(2) THREATS.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A) shall be fined under this title, imprisoned not more than 5 years, or both.

(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a)—

(1) in the case of a covered ship, if—

(A) such activity is committed—

(i) against or on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) at the time the prohibited activity is committed;

(ii) in the United States, including the territorial seas; or

(iii) by a national of the United States, by a United States corporation or legal entity, or by a stateless person whose habitual residence is in the United States;

(B) during the commission of such activity, a national of the United States is seized, threatened, injured, or killed; or

(C) the offender is later found in the United States after such activity is committed;

(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; or

(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

(c) EXCEPTIONS.—This section shall not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

(d)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.

§ 2281. Violence against maritime fixed platforms

(a) OFFENSES.—

(1) IN GENERAL.—A person who unlawfully and intentionally—

(A) seizes or exercises control over a fixed platform by force or threat thereof or any other form of intimidation;

(B) performs an act of violence against a person on board a fixed platform if that act is likely to endanger its safety;

(C) destroys a fixed platform or causes damage to it which is likely to endanger its safety;

(D) places or causes to be placed on a fixed platform, by any means whatsoever, a device or substance which is likely to destroy that fixed platform or likely to endanger its safety;

(E) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (D); or

(F) attempts or conspires to do anything prohibited under subparagraphs (A) through (E),

shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life.

(2) THREAT TO SAFETY.—A person who threatens to do anything prohibited under paragraph (1)(B) or (C), with apparent determination and will to carry the threat into execution, if the threatened act is likely to endanger the safety of the fixed platform, shall be fined under this title, imprisoned not more than 5 years, or both.

(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a) if—

(1) such activity is committed against or on board a fixed platform—

(A) that is located on the continental shelf of the United States;

(B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or

(C) in an attempt to compel the United States to do or abstain from doing any act;

(2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured or killed; or

(3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States.

(c) BAR TO PROSECUTION.—It is a bar to Federal prosecution under subsection (a) for conduct that occurred within the United States that the conduct involved was during or in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed. For purposes of this section, the term "labor dispute" has the meaning set forth in [section 2(c)] *section 13(c)* of the Norris-LaGuardia Act, as amended

(29 U.S.C. 113(c)), and the term "State" means a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(d) DEFINITIONS.—In this section—

"continental shelf" means the sea-bed and subsoil of the submarine areas that extend beyond a country's territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea.

"fixed platform" means an artificial island, installation or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.

["national of the United States" has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)).

["territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law.

["United States", when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and all territories and possessions of the United States.**]**

(e) EXCEPTIONS.—This section does not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

§ 2281a. Additional offenses against maritime fixed platforms

(a) OFFENSES.—

(1) IN GENERAL.—A person who unlawfully and intentionally—

(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

(i) uses against or on a fixed platform or discharges from a fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage; or

(ii) discharges from a fixed platform oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death or serious injury or damage;

(B) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraph (A); or

(C) attempts or conspires to do anything prohibited under subparagraph (A) or (B),

shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

(2) THREAT TO SAFETY.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A), shall be fined under this title, imprisoned not more than 5 years, or both.

(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a) if—

(1) such activity is committed against or on board a fixed platform—

(A) that is located on the continental shelf of the United States;

(B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or

(C) in an attempt to compel the United States to do or abstain from doing any act;

(2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured, or killed; or

(3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States.

(c) EXCEPTIONS.—This section does not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

(d) DEFINITIONS.—In this section—

(1) "continental shelf" means the sea-bed and subsoil of the submarine areas that extend beyond a country's territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea; and

(2) "fixed platform" means an artificial island, installation, or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.

* * * * * * *

CHAPTER 113B—TERRORISM

Sec.
2331. Definitions.

* * * * * * *

2332i. Acts of nuclear terrorism.

* * * * * * *

§ 2332b. Acts of terrorism transcending national boundaries

(a) PROHIBITED ACTS.—

(1) OFFENSES.—Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)—

(A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or

(B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States;

in violation of the laws of any State, or the United States, shall be punished as prescribed in subsection (c).

(2) TREATMENT OF THREATS, ATTEMPTS AND CONSPIRACIES.—Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under subsection (c).

(b) JURISDICTIONAL BASES.—

(1) CIRCUMSTANCES.—The circumstances referred to in subsection (a) are—

(A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense;

(B) the offense obstructs, delays, or affects interstate or foreign commerce, or would have so obstructed, delayed, or affected interstate or foreign commerce if the offense had been consummated;

(C) the victim, or intended victim, is the United States Government, a member of the uniformed services, or any official, officer, employee, or agent of the legislative, executive, or judicial branches, or of any department or agency, of the United States;

(D) the structure, conveyance, or other real or personal property is, in whole or in part, owned, possessed, or leased to the United States, or any department or agency of the United States;

(E) the offense is committed in the territorial sea (including the airspace above and the seabed and subsoil below, and artificial islands and fixed structures erected thereon) of the United States; or

(F) the offense is committed within the special maritime and territorial jurisdiction of the United States.

(2) CO-CONSPIRATORS AND ACCESSORIES AFTER THE FACT.—Jurisdiction shall exist over all principals and co-conspirators of an offense under this section, and accessories after the fact to any offense under this section, if at least one of the circumstances described in subparagraphs (A) through (F) of paragraph (1) is applicable to at least one offender.

(c) PENALTIES.—

(1) PENALTIES.—Whoever violates this section shall be punished—

(A) for a killing, or if death results to any person from any other conduct prohibited by this section, by death, or by imprisonment for any term of years or for life;

(B) for kidnapping, by imprisonment for any term of years or for life;

(C) for maiming, by imprisonment for not more than 35 years;

(D) for assault with a dangerous weapon or assault resulting in serious bodily injury, by imprisonment for not more than 30 years;

(E) for destroying or damaging any structure, conveyance, or other real or personal property, by imprisonment for not more than 25 years;

(F) for attempting or conspiring to commit an offense, for any term of years up to the maximum punishment that would have applied had the offense been completed; and

(G) for threatening to commit an offense under this section, by imprisonment for not more than 10 years.

(2) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section; nor shall the term of imprisonment imposed under this section run concurrently with any other term of imprisonment.

(d) PROOF REQUIREMENTS.—The following shall apply to prosecutions under this section:

(1) KNOWLEDGE.—The prosecution is not required to prove knowledge by any defendant of a jurisdictional base alleged in the indictment.

(2) STATE LAW.—In a prosecution under this section that is based upon the adoption of State law, only the elements of the offense under State law, and not any provisions pertaining to criminal procedure or evidence, are adopted.

(e) EXTRATERRITORIAL JURISDICTION.—There is extraterritorial Federal jurisdiction—

(1) over any offense under subsection (a), including any threat, attempt, or conspiracy to commit such offense; and

(2) over conduct which, under section 3, renders any person an accessory after the fact to an offense under subsection (a).

(f) INVESTIGATIVE AUTHORITY.—In addition to any other investigative authority with respect to violations of this title, the Attorney General shall have primary investigative responsibility for all Federal crimes of terrorism, and any violation of section 351(e), 844(e), 844(f)(1), 956(b), 1361, 1366(b), 1366(c), 1751(e), 2152, or 2156 of this title, and the Secretary of the Treasury shall assist the Attorney General at the request of the Attorney General. Nothing in this section shall be construed to interfere with the authority of the United States Secret Service under section 3056.

(g) DEFINITIONS.—As used in this section—

(1) the term "conduct transcending national boundaries" means conduct occurring outside of the United States in addition to the conduct occurring in the United States;

(2) the term "facility of interstate or foreign commerce" has the meaning given that term in section 1958(b)(2);

(3) the term "serious bodily injury" has the meaning given that term in section 1365(g)(3);

(4) the term "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the

baselines of the United States, determined in accordance with international law; and

(5) the term "Federal crime of terrorism" means an offense that—

(A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and

(B) is a violation of—

(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and weapons of mass destruction threats to the United States) 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), *2280a (relating to maritime safety),* [2281] *2281 through 2281a* (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of ter-

rorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), *2332i (relating to acts of nuclear terrorism),* 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a foreign terrorist organization), or 2340A (relating to torture) of this title;

(ii) sections 92 (relating to prohibitions governing atomic weapons) or 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2122 or 2284);

(iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49; or

(iv) section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).

* * * * * * *

§ 2332i. Acts of nuclear terrorism

(a) OFFENSES.—

(1) IN GENERAL.—Whoever knowingly and unlawfully—

(A) possesses radioactive material or makes or possesses a device—

(i) with the intent to cause death or serious bodily injury; or

(ii) with the intent to cause substantial damage to property or the environment; or

(B) uses in any way radioactive material or a device, or uses or damages or interferes with the operation of a nuclear facility in a manner that causes the release of or increases the risk of the release of radioactive material, or causes radioactive contamination or exposure to radiation—

(i) with the intent to cause death or serious bodily injury or with the knowledge that such act is likely to cause death or serious bodily injury;

(ii) with the intent to cause substantial damage to property or the environment or with the knowledge that such act is likely to cause substantial damage to property or the environment; or

(iii) with the intent to compel a person, an international organization or a country to do or refrain from doing an act,

shall be punished as prescribed in subsection (c).

(2) THREATS.—Whoever, under circumstances in which the threat may reasonably be believed, threatens to commit an offense under paragraph (1) shall be punished as prescribed in subsection (c). Whoever demands possession of or access to radioactive material, a device or a nuclear facility by threat or by use of force shall be punished as prescribed in subsection (c).

(3) ATTEMPTS AND CONSPIRACIES.—Whoever attempts to commit an offense under paragraph (1) or conspires to commit an offense under paragraph (1) or (2) shall be punished as prescribed in subsection (c).

(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

(1) the prohibited conduct takes place in the United States or the special aircraft jurisdiction of the United States;

(2) the prohibited conduct takes place outside of the United States and—

(A) is committed by a national of the United States, a United States corporation or legal entity or a stateless person whose habitual residence is in the United States;

(B) is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed; or

(C) is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States;

(3) the prohibited conduct takes place outside of the United States and a victim or an intended victim is a national of the United States or a United States corporation or legal entity, or the offense is committed against any state or government facility of the United States; or

(4) a perpetrator of the prohibited conduct is found in the United States.

(c) PENALTIES.—Whoever violates this section shall be fined not more than $2,000,000 and shall be imprisoned for any term of years or for life.

(d) NONAPPLICABILITY.—This section does not apply to—

(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

(2) activities undertaken by military forces of a state in the exercise of their official duties.

(e) DEFINITIONS.—As used in this section, the term—

(1) "armed conflict" has the meaning given that term in section 2332f(e)(11) of this title;

(2) "device" means:

(A) any nuclear explosive device; or

(B) any radioactive material dispersal or radiation-emitting device that may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or the environment;

(3) "international organization" has the meaning given that term in section 831(f)(3) of this title;

(4) "military forces of a state" means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

(5) "national of the United States" has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

(6) "nuclear facility" means:

(A) any nuclear reactor, including reactors on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose;

(B) any plant or conveyance being used for the production, storage, processing or transport of radioactive material; or

(C) a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material;

(7) "nuclear material" has the meaning given that term in section 831(f)(1) of this title;

(8) "radioactive material" means nuclear material and other radioactive substances that contain nuclides that undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionizing radiation, such as alpha-, beta-, neutron particles and gamma rays) and that may, owing to their radiological or fissile properties, cause death, serious bodily injury or substantial damage to property or to the environment;

(9) "serious bodily injury" has the meaning given that term in section 831(f)(4) of this title;

(10) "state" has the same meaning as that term has under international law, and includes all political subdivisions thereof;

(11) "state or government facility" has the meaning given that term in section 2332f(e)(3) of this title;

(12) "United States corporation or legal entity" means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession or district of the United States;

(13) "vessel" has the meaning given that term in section 1502(19) of title 33; and

(14) "vessel of the United States" has the meaning given that term in section 70502 of title 46.

* * * * * * *

§ 2339B. Providing material support or resources to designated foreign terrorist organizations

(a) PROHIBITED ACTIVITIES.—

(1) UNLAWFUL CONDUCT.—Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than [15 years] *20 years*, or both,

and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

(2) FINANCIAL INSTITUTIONS.—Except as authorized by the Secretary, any financial institution that becomes aware that it has possession of, or control over, any funds in which a foreign terrorist organization, or its agent, has an interest, shall—

(A) retain possession of, or maintain control over, such funds; and

(B) report to the Secretary the existence of such funds in accordance with regulations issued by the Secretary.

(b) CIVIL PENALTY.—Any financial institution that knowingly fails to comply with subsection (a)(2) shall be subject to a civil penalty in an amount that is the greater of—

(A) $50,000 per violation; or

(B) twice the amount of which the financial institution was required under subsection (a)(2) to retain possession or control.

(c) INJUNCTION.—Whenever it appears to the Secretary or the Attorney General that any person is engaged in, or is about to engage in, any act that constitutes, or would constitute, a violation of this section, the Attorney General may initiate civil action in a district court of the United States to enjoin such violation.

(d) EXTRATERRITORIAL JURISDICTION.—

(1) IN GENERAL.—There is jurisdiction over an offense under subsection (a) if—

(A) an offender is a national of the United States (as defined in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22))) or an alien lawfully admitted for permanent residence in the United States (as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(20)));

(B) an offender is a stateless person whose habitual residence is in the United States;

(C) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States;

(D) the offense occurs in whole or in part within the United States;

(E) the offense occurs in or affects interstate or foreign commerce; or

(F) an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exists under this paragraph to commit an offense under subsection (a).

(2) EXTRATERRITORIAL JURISDICTION.—There is extraterritorial Federal jurisdiction over an offense under this section.

(e) INVESTIGATIONS.—

(1) IN GENERAL.—The Attorney General shall conduct any investigation of a possible violation of this section, or of any license, order, or regulation issued pursuant to this section.

(2) COORDINATION WITH THE DEPARTMENT OF THE TREASURY.—The Attorney General shall work in coordination with the Secretary in investigations relating to—

(A) the compliance or noncompliance by a financial institution with the requirements of subsection (a)(2); and

(B) civil penalty proceedings authorized under subsection (b).

(3) REFERRAL.—Any evidence of a criminal violation of this section arising in the course of an investigation by the Secretary or any other Federal agency shall be referred immediately to the Attorney General for further investigation. The Attorney General shall timely notify the Secretary of any action taken on referrals from the Secretary, and may refer investigations to the Secretary for remedial licensing or civil penalty action.

(f) CLASSIFIED INFORMATION IN CIVIL PROCEEDINGS BROUGHT BY THE UNITED STATES.—

(1) DISCOVERY OF CLASSIFIED INFORMATION BY DEFENDANTS.—

(A) REQUEST BY UNITED STATES.—In any civil proceeding under this section, upon request made ex parte and in writing by the United States, a court, upon a sufficient showing, may authorize the United States to—

(i) redact specified items of classified information from documents to be introduced into evidence or made available to the defendant through discovery under the Federal Rules of Civil Procedure;

(ii) substitute a summary of the information for such classified documents; or

(iii) substitute a statement admitting relevant facts that the classified information would tend to prove.

(B) ORDER GRANTING REQUEST.—If the court enters an order granting a request under this paragraph, the entire text of the documents to which the request relates shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

(C) DENIAL OF REQUEST.—If the court enters an order denying a request of the United States under this paragraph, the United States may take an immediate, interlocutory appeal in accordance with paragraph (5). For purposes of such an appeal, the entire text of the documents to which the request relates, together with any transcripts of arguments made ex parte to the court in connection therewith, shall be maintained under seal and delivered to the appellate court.

(2) INTRODUCTION OF CLASSIFIED INFORMATION; PRECAUTIONS BY COURT.—

(A) EXHIBITS.—To prevent unnecessary or inadvertent disclosure of classified information in a civil proceeding brought by the United States under this section, the

United States may petition the court ex parte to admit, in lieu of classified writings, recordings, or photographs, one or more of the following:

(i) Copies of items from which classified information has been redacted.

(ii) Stipulations admitting relevant facts that specific classified information would tend to prove.

(iii) A declassified summary of the specific classified information.

(B) DETERMINATION BY COURT.—The court shall grant a request under this paragraph if the court finds that the redacted item, stipulation, or summary is sufficient to allow the defendant to prepare a defense.

(3) TAKING OF TRIAL TESTIMONY.—

(A) OBJECTION.—During the examination of a witness in any civil proceeding brought by the United States under this subsection, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible.

(B) ACTION BY COURT.—In determining whether a response is admissible, the court shall take precautions to guard against the compromise of any classified information, including—

(i) permitting the United States to provide the court, ex parte, with a proffer of the witness's response to the question or line of inquiry; and

(ii) requiring the defendant to provide the court with a proffer of the nature of the information that the defendant seeks to elicit.

(C) OBLIGATION OF DEFENDANT.—In any civil proceeding under this section, it shall be the defendant's obligation to establish the relevance and materiality of any classified information sought to be introduced.

(4) APPEAL.—If the court enters an order denying a request of the United States under this subsection, the United States may take an immediate interlocutory appeal in accordance with paragraph (5).

(5) INTERLOCUTORY APPEAL.—

(A) SUBJECT OF APPEAL.—An interlocutory appeal by the United States shall lie to a court of appeals from a decision or order of a district court—

(i) authorizing the disclosure of classified information;

(ii) imposing sanctions for nondisclosure of classified information; or

(iii) refusing a protective order sought by the United States to prevent the disclosure of classified information.

(B) EXPEDITED CONSIDERATION.—

(i) IN GENERAL.—An appeal taken pursuant to this paragraph, either before or during trial, shall be expedited by the court of appeals.

(ii) APPEALS PRIOR TO TRIAL.—If an appeal is of an order made prior to trial, an appeal shall be taken not

later than 14 days after the decision or order appealed from, and the trial shall not commence until the appeal is resolved.

(iii) APPEALS DURING TRIAL.—If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved, and the court of appeals—

(I) shall hear argument on such appeal not later than 4 days after the adjournment of the trial, excluding intermediate weekends and holidays;

(II) may dispense with written briefs other than the supporting materials previously submitted to the trial court;

(III) shall render its decision not later than 4 days after argument on appeal, excluding intermediate weekends and holidays; and

(IV) may dispense with the issuance of a written opinion in rendering its decision.

(C) EFFECT OF RULING.—An interlocutory appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a final judgment, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.

(6) CONSTRUCTION.—Nothing in this subsection shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information, including the invocation of the military and State secrets privilege.

(g) DEFINITIONS.—As used in this section—

(1) the term "classified information" has the meaning given that term in section 1(a) of the Classified Information Procedures Act (18 U.S.C. App.);

(2) the term "financial institution" has the same meaning as in section 5312(a)(2) of title 31, United States Code;

(3) the term "funds" includes coin or currency of the United States or any other country, traveler's checks, personal checks, bank checks, money orders, stocks, bonds, debentures, drafts, letters of credit, any other negotiable instrument, and any electronic representation of any of the foregoing;

(4) the term "material support or resources" has the same meaning given that term in section 2339A (including the definitions of "training" and "expert advice or assistance" in that section);

(5) the term "Secretary" means the Secretary of the Treasury; and

(6) the term "terrorist organization" means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act.

(h) PROVISION OF PERSONNEL.—No person may be prosecuted under this section in connection with the term "personnel" unless that person has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization. Indi-

viduals who act entirely independently of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction and control.

(i) RULE OF CONSTRUCTION.—Nothing in this section shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution of the United States.

(j) EXCEPTION.—No person may be prosecuted under this section in connection with the term "personnel", "training", or "expert advice or assistance" if the provision of that material support or resources to a foreign terrorist organization was approved by the Secretary of State with the concurrence of the Attorney General. The Secretary of State may not approve the provision of any material support that may be used to carry out terrorist activity (as defined in section 212(a)(3)(B)(iii) of the Immigration and Nationality Act).

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * * * *

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime;

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8)**[**; and**]***;*

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges**[**.**]***; and*

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

* * * * * * *

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, [may] *may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request*—

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[(c) PROHIBITION OF CERTAIN DISCLOSURE.—

[(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

[(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

[(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

[(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).]

(c) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

(2) NOTICE.—A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).

[(d)**]** *(e)* DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

[(e)**]** *(f)* REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

[(f)**]** *(g)* LIBRARIES.—A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

* * * * * * *

PART II—CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 223—WITNESSES AND EVIDENCE

* * * * * * *

§ 3511. Judicial review of requests for information

(a) The recipient of a request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947 may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request. The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.

[(b)(1) The recipient of a request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, may petition any court described in subsection (a) for an order modifying or setting aside a nondisclosure requirement imposed in connection with such a request.

[(2) If the petition is filed within one year of the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If, at the time of the petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of such department, agency, or instrumentality, certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive unless the court finds that the certification was made in bad faith.

[(3) If the petition is filed one year or more after the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government

other than the Federal Bureau of Investigation, the head or deputy head of such department, agency, or instrumentality, within ninety days of the filing of the petition, shall either terminate the nondisclosure requirement or re-certify that disclosure may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. In the event of re-certification, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If the recertification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, such certification shall be treated as conclusive unless the court finds that the recertification was made in bad faith. If the court denies a petition for an order modifying or setting aside a nondisclosure requirement under this paragraph, the recipient shall be precluded for a period of one year from filing another petition to modify or set aside such nondisclosure requirement.]

(b) NONDISCLOSURE.—

(1) IN GENERAL.—

(A) NOTICE.—If a recipient of a request or order for a report, records, or other information under section 2709 of this title, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), wishes to have a court review a nondisclosure requirement imposed in connection with the request or order, the recipient may notify the Government or file a petition for judicial review in any court described in subsection (a).

(B) APPLICATION.—Not later than 30 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of the existence or contents of the relevant request or order. An application under this subparagraph may be filed in the district court of the United States for the judicial district in which the recipient of the order is doing business or in the district court of the United States for any judicial district within which the authorized investigation that is the basis for the request is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.

(C) CONSIDERATION.—A district court of the United States that receives a petition under subparagraph (A) or an application under subparagraph (B) should rule expeditiously, and shall, subject to paragraph (3), issue a nondisclosure order that includes conditions appropriate to the circumstances.

(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof or a response to a petition filed under paragraph (1) shall include a certification from the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or a designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of the department, agency, or instrumentality, containing a statement of specific facts indicating that the absence of a prohibition of disclosure under this subsection may result in—

(A) a danger to the national security of the United States;

(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

(C) interference with diplomatic relations; or

(D) danger to the life or physical safety of any person.

(3) STANDARD.—A district court of the United States shall issue a nondisclosure order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period may result in—

(A) a danger to the national security of the United States;

(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

(C) interference with diplomatic relations; or

(D) danger to the life or physical safety of any person.

(c) In the case of a failure to comply with a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General may invoke the aid of any district court of the United States within the jurisdiction in which the investigation is carried on or the person or entity resides, carries on business, or may be found, to compel compliance with the request. The court may issue an order requiring the person or entity to comply with the request. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person or entity may be found.

(d) In all proceedings under this section, subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent an unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947. Petitions, filings, records, orders, and subpoenas must also be kept under seal to the extent and as long as necessary to prevent the unauthorized disclo-

sure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947.

(e) In all proceedings under this section, the court shall, upon request of the government, review ex parte and in camera any government submission or portions thereof, which may include classified information.

* * * * * * *

RIGHT TO FINANCIAL PRIVACY ACT OF 1978

* * * * * * *

TITLE XI—RIGHT TO FINANCIAL PRIVACY

* * * * * * *

SPECIAL PROCEDURES

SEC. 1114. (a)(1) Nothing in this title (except sections 1115, 1117, 1118, and 1121) shall apply to the production and disclosure of financial records pursuant to requests from—

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;

(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 3 U.S.C. 202, Public Law 90–331, as amended); or

(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 1103(b) signed by a supervisory official of a rank designated by the head of the Government authority**[**.**]** *and a term that specifically identifies a customer, entity, or account to be used as the basis for the production and disclosure of financial records.*

(3)(A) If the Government authority described in paragraph (1) or the Secret Service, as the case may be, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no financial institution, or officer, employee, or agent of such institution, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Government authority or the Secret Service has sought or obtained access to a customer's financial records.

(B) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under subparagraph (A).

(C) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under subparagraph (A).

(D) At the request of the authorized Government authority or the Secret Service, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized Government authority or the Secret Service the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the requesting official of the authorized Government authority or the Secret Service of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for financial records under this subsection.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(C) On the dates provided in section 507 of the National Security Act of 1947, the Attorney General shall fully inform the congressional intelligence committees (as defined in section 3 of that Act (50 U.S.C. 401a)) concerning all requests made pursuant to this paragraph.

[(D) PROHIBITION OF CERTAIN DISCLOSURE.—

[(i) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special

Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no financial institution, or officer, employee, or agent of such institution, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under subparagraph (A).

[(ii) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under clause (i).

[(iii) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under clause (i).

[(iv) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for financial records under subparagraph (A).]

(b)(1) Nothing in this title shall prohibit a Government authority from obtaining financial records from a financial institution if the Government authority determines that delay in obtaining access to such records would create imminent danger of—

(A) physical injury to any person;

(B) serious property damage; or

(C) flight to avoid prosecution.

(2) In the instances specified in paragraph (1), the Government shall submit to the financial institution the certificate required in section 1103(b) signed by a supervisory official of a rank designated by the head of the Government authority.

(3) Within five days of obtaining access to financial records under this subsection, the Government authority shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the Government authority setting forth the grounds for the emergency access. The Government authority shall thereafter comply with notice the provisions of section 1109(c).

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(c) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).

[(d)**]** *(e)* For purposes of this section, and sections 1115 and 1117 insofar as they relate to the operation of this section, the term "financial institution" has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of title 31, United States Code, except that, for purposes of this section, such term shall include only such a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

* * * * * * *

FAIR CREDIT REPORTING ACT

* * * * * * *

TITLE VI—CONSUMER CREDIT REPORTING

* * * * * * *

§ 626. Disclosures to FBI for counterintelligence purposes

(a) IDENTITY OF FINANCIAL INSTITUTIONS.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 1101 of the Right to Financial Privacy Act of 1978) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for **[**that information,**]** *that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,* signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) IDENTIFYING INFORMATION.—Notwithstanding the provisions of section 604 or any other provision of this title, a consumer reporting agency shall furnish identifying information respecting a

consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a [written request,] *written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,* signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) COURT ORDER FOR DISCLOSURE OF CONSUMER REPORTS.—Notwithstanding section 604 or any other provision of this title, if requested in writing by the Director of the Federal Bureau of Investigation, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, a court may issue an order ex parte*, which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information,* directing a consumer reporting agency to furnish a consumer report to the Federal Bureau of Investigation, upon a showing in camera that the consumer report is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

The terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation.

[(d) CONFIDENTIALITY.—

[(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no consumer reporting agency or officer, employee, or agent of a consumer reporting agency shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained the identity of financial institutions or a consumer report respecting any consumer under subsection (a), (b), or (c), and no consumer reporting agency or officer, employee, or

agent of a consumer reporting agency shall include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such information on a consumer report.

[(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

[(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

[(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for the identity of financial institutions or a consumer report respecting any consumer under this section.]

(d) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (e) is provided, no consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof,

may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) or (b) or an order under subsection (c) is issued in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (a) or (b) or an order under subsection (c) or a non-disclosure requirement imposed in connection with such request under subsection (d) shall be subject to judicial review under section 3511 of title 18, United States Code.

(2) NOTICE.—A request under subsection (a) or (b) or an order under subsection (c) shall include notice of the availability of judicial review described in paragraph (1).

[(e)**]** *(f)* PAYMENT OF FEES.—The Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing report or information in accordance with procedures established under this section a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this section.

[(f)**]** *(g)* LIMIT ON DISSEMINATION.—The Federal Bureau of Investigation may not disseminate information obtained pursuant to this section outside of the Federal Bureau of Investigation, except to other Federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation, or, where the information concerns a person subject to the Uniform Code of Military Justice, to appropriate investigative authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation.

[(g)**]** *(h)* RULES OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit information from being furnished by the Federal Bureau of Investigation pursuant to a subpoena or

court order, in connection with a judicial or administrative proceeding to enforce the provisions of this Act. Nothing in this section shall be construed to authorize or permit the withholding of information from the Congress.

[(h)] *(i)* REPORTS TO CONGRESS.—(1) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on Banking, Finance and Urban Affairs of the House of Representatives, and the Select Committee on Intelligence and the Committee on Banking, Housing, and Urban Affairs of the Senate concerning all requests made pursuant to subsections (a), (b), and (c).

(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947.

[(i)] *(j)* DAMAGES.—Any agency or department of the United States obtaining or disclosing any consumer reports, records, or information contained therein in violation of this section is liable to the consumer to whom such consumer reports, records, or information relate in an amount equal to the sum of—

(1) $100, without regard to the volume of consumer reports, records, or information involved;

(2) any actual damages sustained by the consumer as a result of the disclosure;

(3) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

(4) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney fees, as determined by the court.

[(j)] *(k)* DISCIPLINARY ACTIONS FOR VIOLATIONS.—If a court determines that any agency or department of the United States has violated any provision of this section and the court finds that the circumstances surrounding the violation raise questions of whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee who was responsible for the violation.

[(k)] *(l)* GOOD-FAITH EXCEPTION.—Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or identifying information pursuant to this subsection in good-faith reliance upon a certification of the Federal Bureau of Investigation pursuant to provisions of this section shall not be liable to any person for such disclosure under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

[(l)] *(m)* LIMITATION OF REMEDIES.—Notwithstanding any other provision of this title, the remedies and sanctions set forth in this section shall be the only judicial remedies and sanctions for violation of this section.

[(m)] *(n)* INJUNCTIVE RELIEF.—In addition to any other remedy contained in this section, injunctive relief shall be available to

require compliance with the procedures of this section. In the event of any successful action under this subsection, costs together with reasonable attorney fees, as determined by the court, may be recovered.

§ 627. Disclosures to governmental agencies for counterterrorism purposes

(a) DISCLOSURE.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or [analysis.] *analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information.*

(b) FORM OF CERTIFICATION.—The certification described in subsection (a) shall be signed by a supervisory official designated by the head of a Federal agency or an officer of a Federal agency whose appointment to office is required to be made by the President, by and with the advice and consent of the Senate.

[(c) CONFIDENTIALITY.—

[(1) If the head of a government agency authorized to conduct investigations of intelligence or counterintelligence activities or analysis related to international terrorism, or his designee, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no consumer reporting agency or officer, employee, or agent of such consumer reporting agency, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request), or specify in any consumer report, that a government agency has sought or obtained access to information under subsection (a).

[(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

[(3) Any recipient disclosing to those persons necessary to comply with the request or to any attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

[(4) At the request of the authorized government agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized government agency the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require

a person to inform the requesting official of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for information under subsection (a).]

(c) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that a government agency described in subsection (a) has sought or obtained access to information or records under subsection (a).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of the government agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the head of the government agency described in subsection (a) or a designee.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) is issued in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of the government agency described in subsection (a) or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).

[(d)**]** *(e)* RULE OF CONSTRUCTION.—Nothing in section 626 shall be construed to limit the authority of the Director of the Federal Bureau of Investigation under this section.

[(e)**]** *(f)* SAFE HARBOR.—Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a government agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

[(f)**]** *(g)* REPORTS TO CONGRESS.—(1) On a semi-annual basis, the Attorney General shall fully inform the Committee on the Judiciary, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to subsection (a).

(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947 (50 U.S.C. 415b).

* * * * * * *

NATIONAL SECURITY ACT OF 1947

* * * * * * *

TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

* * * * * * *

REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

SEC. 802. (a)(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where—

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request—

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that—

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

(C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b).

[(b) PROHIBITION OF CERTAIN DISCLOSURE.—

[(1) If an authorized investigative agency described in subsection (a) certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the re-

quest) that such entity has received or satisfied a request made by an authorized investigative agency under this section.

[(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

[(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

[(4) At the request of the authorized investigative agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized investigative agency the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the requesting official of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).]

(b) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head of the authorized investigative agency or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(c) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (b) shall be subject to judicial review under section 3511 of title 18, United States Code.

(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).

[(c)**]** *(d)*(1) Notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) shall, if the request satisfies the requirements of this section, make available such records or information within 30 days for inspection or copying, as may be appropriate, by the agency requesting such records or information.

(2) Any entity (including any officer, employee, or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the certifications made by an agency pursuant to this section shall not be liable for any such disclosure to any person under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

[(d)**]** *(e)* Any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

[(e)**]** *(f)* An agency receiving records or information pursuant to a request under this section may disseminate the records or information obtained pursuant to such request outside the agency only—

(1) to the agency employing the employee who is the subject of the records or information;

(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

(3) with respect to dissemination to an agency of the United States, if such information is clearly relevant to the authorized responsibilities of such agency.

[(f)] *(g)* Nothing in this section may be construed to affect the authority of an investigative agency to obtain information pursuant to the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

* * * * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * * * *

TITLE VI—TERRORISM PREVENTION

Subtitle A—Individual Terrorists as Agents of Foreign Powers

SEC. 6001. INDIVIDUAL TERRORISTS AS AGENTS OF FOREIGN POWERS.

(a) IN GENERAL.—Section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) is amended by adding at the end the following new subparagraph:

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

(b) SUNSET.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendment made by subsection (a) shall cease to have effect on [June 1, 2015] *December 15, 2019*.

(2) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which the provisions cease to have effect, such provisions shall continue in effect.

* * * * * * *

Committee Jurisdiction Letters

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

HVC–304, THE CAPITOL
WASHINGTON, DC 20515
(202) 225–4121

JEFF SHOCKEY
STAFF DIRECTOR

MICHAEL BAHAR
MINORITY STAFF DIRECTOR

May 4, 2015

The Honorable Bob Goodlatte
Chairman, U.S. House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Goodlatte:

On April 30, 2015, the Committee on the Judiciary ordered H.R. 2048, the USA Freedom Act of 2015, reported to the House.

As you know, H.R. 2048 contains provisions that amend the Foreign Intelligence Surveillance Act, which is within the jurisdiction of the Permanent Select Committee on Intelligence. As a result of your prior consultation with the Committee, and in order to expedite the House's consideration of H.R. 2048, the Permanent Select Committee on Intelligence will waive further consideration of the bill.

The Committee takes this action only with the understanding that this procedural route should not be construed to prejudice the jurisdictional interest of the House Permanent Select Committee on Intelligence over this bill or any similar bill. Furthermore, this waiver should not be considered as precedent for consideration of matters of jurisdictional interest to the Committee in the future, including in connection with any subsequent consideration of the bill by the House. The Permanent Select Committee on Intelligence will seek conferees on the bill during any House-Senate conference that may be convened on this legislation.

Finally, I would ask that you include a copy of our exchange of letters on this matter in the *Congressional Record* during the House debate on H.R. 2048. I appreciate the constructive work between our committees on this matter and thank you for your consideration.

Sincerely,

Devin Nunes

Devin Nunes
Chairman

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

May 7, 2015

The Honorable Devin Nunes
Chairman
House Permanent Select Committee on Intelligence
HVC-304
Washington, DC 20515

Dear Chairman Nunes,

Thank you for your letter regarding H.R. 2048, the "U.S.A. Freedom Act of 2015." As you noted, the Permanent Select Committee on Intelligence was granted an additional referral on the bill.

I am most appreciative of your decision to waive further consideration of H.R. 2048 so that it may proceed expeditiously to the House floor. I acknowledge that although you waived formal consideration of the bill, the Permanent Select Committee on Intelligence is in no way waiving its jurisdiction over the subject matter contained in those provisions of the bill that fall within your Rule X jurisdiction. Further, I understand the Committee reserves the right to seek the appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, for which you will have my support.

I will include a copy of your letter and this response in the Committee Report as well as in the *Congressional Record* during floor consideration of H.R. 2048.

Sincerely,

Bob Goodlatte

Bob Goodlatte
Chairman

cc: The Honorable John Boehner, Speaker
The Honorable John Conyers
The Honorable Adam Schiff
The Honorable Thomas J. Wickham, Jr., Parliamentarian

○