115TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 115–475
Part 1

FISA AMENDMENTS REAUTHORIZATION ACT OF 2017

DECEMBER 19, 2017.—Ordered to be printed

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

R E P O R T

together with

MINORITY AND ADDITIONAL VIEWS

[To accompany H.R. 4478]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 4478) to amend the Foreign Intelligence Surveillance Act of 1978 to improve foreign intelligence collection and the safeguards, accountability, and oversight of acquisitions of foreign intelligence, to extend title VII of such Act, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "FISA Amendments Reauthorization Act of 2017".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

79–006

SEC. 2. AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or a repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

TITLE I—ENHANCEMENTS TO FOREIGN INTELLIGENCE COLLECTION

SEC. 101. SECTION 705 EMERGENCY PROVISION.

Section 705 (50 U.S.C. 1881d) is amended by adding at the end the following:

"(c) EMERGENCY AUTHORIZATION.—

"(1) CONCURRENT AUTHORIZATION.—If the Attorney General authorized the emergency employment of electronic surveillance or a physical search pursuant to section 105 or 304, the Attorney General may authorize, for the effective period of the emergency authorization and subsequent order pursuant to section 105 or 304, without a separate order under section 703 or 704, the targeting of a United States person subject to such emergency employment for the purpose of acquiring foreign intelligence information while such United States person is reasonably believed to be located outside the United States.

"(2) USE OF INFORMATION.—If an application submitted to the Court pursuant to section 104 or 304 is denied, or in any other case in which the acquisition pursuant to paragraph (1) is terminated and no order with respect to the target of the acquisition is issued under section 105 or 304, all information obtained or evidence derived from such acquisition shall be handled in accordance with section 704(d)(4).".

SEC. 102. MODIFICATION TO DEFINITIONS OF FOREIGN POWER AND AGENT OF A FOREIGN POWER.

(a) FOREIGN POWER.—Subsection (a) of section 101 (50 U.S.C. 1801) is amended—

(1) in paragraph (6), by striking "; or" and inserting a semicolon;

(2) in paragraph (7), by striking the period at the end and inserting "; or"; and

(3) by adding at the end the following new paragraph:

"(8) an entity not substantially composed of United States persons that is engaged in international malicious cyber activity, or activities in preparation therefor, that threatens the national defense or security of the United States.".

(b) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of such section (50 U.S.C. 1801) is amended—

(1) in subparagraph (D), by striking "; or" and inserting a semicolon; and

(2) by adding at the end the following new subparagraph:

"(F) engages in international malicious cyber activity that threatens the national defense or security of the United States, 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 international malicious cyber activity or activities in preparation therefor, or knowingly conspires with any person to engage in such international malicious cyber activity or activities in preparation therefor; or".

(c) INTERNATIONAL MALICIOUS CYBER ACTIVITY DEFINED.—Such section (50 U.S.C. 1801) is further amended by adding at the end the following new subsection:

"(q)(1) The term 'international malicious cyber activity' means activity on or through an information system—

"(A) originating from, or directed by, persons located, in whole or in substantial part, outside the United States;

"(B) that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information systems or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon; and

"(C) that is not authorized by the United States Government or otherwise carried out in accordance with Federal law.

"(2) In paragraph (1), the term 'information system' has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501), and includes national security systems (as defined in section 11103 of title 40, United States Code).".

TITLE II—SAFEGUARDS, ACCOUNTABILITY, AND OVERSIGHT

SEC. 201. QUERYING PROCEDURES REQUIRED.

(a) QUERYING PROCEDURES.—

(1) IN GENERAL.—Section 702 (50 U.S.C. 1881a) is amended—

(A) by redesignating subsections (f) through (l) as subsections (g) through (m), respectively; and

(B) by inserting after subsection (e) the following new subsection:

"(f) QUERIES.—

"(1) PROCEDURES REQUIRED.—

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

"(B) RECORD OF UNITED STATES PERSON QUERY TERMS.—The Attorney General, in consultation with the Director of National Intelligence, shall ensure that the procedures adopted under subparagraph (A) include a technical procedure whereby a record is kept of each United States person query term used for a query.

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

"(2) COURT ORDERS FOR ACCESS OF CONTENTS FROM CERTAIN QUERIES.—

"(A) DISCRETION FOR FBI TO APPLY FOR COURT ORDER.—Before the Federal Bureau of Investigation accesses the contents of communications acquired under subsection (a) that were retrieved using a United States person query term that was not designed to find and extract foreign intelligence information, the Bureau may apply for an order of the Court under subparagraph (C).

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

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

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

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

"(I) criminal activity;

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

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

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

"(E) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to prohibit the Federal Bureau of Investigation from querying information acquired under subsection (a), or accessing the results of such a

query, regardless of whether the Bureau applies for or receives an order under this paragraph.

"(3) QUERY DEFINED.—In this subsection, the term 'query' means the use of one or more terms to retrieve the unminimized contents (as defined in section 2510(8) of title 18, United States Code) or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under subsection (a).".

(2) APPLICATION.—Subsection (f) of section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), as added by paragraph (1), shall apply with respect to certifications submitted under subsection (h) of such section to the Foreign Intelligence Surveillance Court after January 1, 2018.

(b) CONFORMING AMENDMENTS.—

(1) AMENDMENTS TO SECTION 702 OF FISA.—Such section 702 is further amended—

(A) in subsection (a), by striking "with subsection (i)(3)" and inserting "with subsection (j)(3)";

(B) in subsection (c)—

(i) in paragraph (1)(B), by striking "with subsection (g)" and inserting "with subsection (h)";

(ii) in paragraph (2), by striking "to subsection (i)(3)" and inserting "to subsection (j)(3)"; and

(iii) in paragraph (3)—

(I) in subparagraph (A), by striking "with subsection (g)" and inserting "with subsection (h)"; and

(II) in subparagraph (B)—

(aa) by striking "to subsection (i)(1)(C)" and inserting "to subsection (j)(1)(C)"; and

(bb) by striking "under subsection (i)" and inserting "under subsection (j)";

(C) in subsection (d)(2), by striking "to subsection (i)" and inserting "to subsection (j)";

(D) in subsection (e)(2), by striking "to subsection (i)" and inserting "to subsection (j)";

(E) in subsection (h), as redesignated by subsection (a)(1)—

(i) in paragraph (2)(A)(iii), by striking "with subsection (f)" and inserting "with subsection (g)";

(ii) in paragraph (3), by striking "with subsection (i)(1)(C)" and inserting "with subsection (j)(1)(C)"; and

(iii) in paragraph (6), by striking "to subsection (i)" and inserting "to subsection (j)";

(F) in subsection (j), as redesignated by subsection (a)(1)—

(i) in paragraph (1)—

(I) in subparagraph (A), by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)";

(II) in subparagraph (B), by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)"; and

(III) in subparagraph (C), by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)";

(ii) in paragraph (2)—

(I) in subparagraph (A), by striking "with subsection (g)" and inserting "with subsection (h)"; and

(II) by adding at the end the following:

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

(iii) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking "with subsection (g)" and inserting "with subsection (h)"; and

(bb) by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)"; and

(II) in subparagraph (B), in the matter before clause (i)—

(aa) by striking "with subsection (g)" and inserting "with subsection (h)"; and

(bb) by striking "with subsections (d) and (e)" and inserting "with subsections (d), (e), and (f)(1)"; and

(iv) in paragraph (5)(A)—

(I) by striking "with subsection (g)" and inserting "with subsection (h)"; and

(II) by striking "with subsections (d) and (e)" and inserting "with subsections (d), (e), and (f)(1)"; and

(G) in subsection (m), as redesignated by subsection (a)(1)—

(i) in paragraph (1), in the matter before subparagraph (A)—

(I) by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)"; and

(II) by striking "with subsection (f)" and inserting "with subsection (g)"; and

(ii) in paragraph (2)(A)—

(I) by striking "targeting and minimization procedures adopted in accordance with subsections (d) and (e)" and inserting "targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)"; and

(II) by striking "with subsection (f)" and inserting "with subsection (g)".

(2) AMENDMENTS TO FISA.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—

(A) by striking "section 702(h)" each place it appears and inserting "section 702(i)";

(B) by striking "section 702(g)" each place it appears and inserting "section 702(h)"; and

(C) in section 707(b)(1)(G)(ii), by striking "subsections (d), (e), and (f)" and inserting "subsections (d), (e), (f)(1), and (g)".

(3) AMENDMENTS TO FISA AMENDMENTS ACT OF 2008.—Section 404 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (Public Law 110–261; 50 U.S.C. 1801 note) is amended—

(A) in subsection (a)(7)(B)—

(i) by striking "under section 702(i)(3)" and inserting "under section 702(j)(3)"; and

(ii) by striking "of section 702(i)(4)" and inserting "of section 702(j)(4)";

(B) in subsection (b)—

(i) in paragraph (3)—

(I) in subparagraph (A), by striking "to section 702(h)" and inserting "to section 702(i)"; and

(II) in subparagraph (B)—

(aa) by striking "section 702(h)(3) of" and inserting "section 702(i)(3) of"; and

(bb) by striking "to section 702(h)" and inserting "to section 702(i)"; and

(ii) in paragraph (4)—

(I) in subparagraph (A), by striking "and sections 702(l)" and inserting "and sections 702(m)"; and

(II) in subparagraph (B)(iv), by striking "or section 702(l)" and inserting "or section 702(m)".

SEC. 202. USE AND DISCLOSURE PROVISIONS.

(a) END USE RESTRICTION.—Section 706(a) (50 U.S.C. 1881e(a)) is amended—

(1) by striking "Information acquired" and inserting the following:

"(1) IN GENERAL.—Information acquired"; and

(2) by adding at the end the following:

"(2) UNITED STATES PERSONS.—

"(A) IN GENERAL.—Any information concerning a United States person acquired under section 702 shall not be used in evidence against that United States person pursuant to paragraph (1) in any criminal proceeding unless—

"(i) the Federal Bureau of Investigation obtained an order of the Foreign Intelligence Surveillance Court to access such information pursuant to section 702(f)(2); or

"(ii) the Attorney General determines that—

"(I) the criminal proceeding affects, involves, or is related to the national security of the United States; or

"(II) the criminal proceeding involves—

"(aa) death;

"(bb) kidnapping;

"(cc) serious bodily injury, as defined in section 1365 of title 18, United States Code;

"(dd) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006 (34 U.S.C. 20911);

"(ee) incapacitation or destruction of critical infrastructure, as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e));

"(ff) cybersecurity, including conduct described in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) or section 1029, 1030, or 2511 of title 18, United States Code;

"(gg) transnational crime, including transnational narcotics trafficking and transnational organized crime; or

"(hh) human trafficking.

"(B) NO JUDICIAL REVIEW.—A determination by the Attorney General under subparagraph (A)(ii) is not subject to judicial review.".

(b) INTELLIGENCE COMMUNITY DISCLOSURE PROVISION.—Section 603 (50 U.S.C. 1873) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking "good faith estimate of the number of targets of such orders;" and inserting the following: "good faith estimate of—

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

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

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

(B) in paragraph (2)—

(i) by redesignating subparagraphs (A) and (B) as subparagraphs (B) and (C), respectively;

(ii) by inserting before subparagraph (B), as so redesignated, the following:

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

(iii) in subparagraph (B), as so redesignated, by striking "and" at the end; and

(iv) by adding at the end the following:

"(D) the number of instances in which the Federal Bureau of Investigation has received and reviewed the unminimized contents of electronic communications or wire communications concerning a United States person obtained through acquisitions authorized under such section in response to a search term that was not designed to find and extract foreign intelligence information; and

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

(C) in paragraph (3)(A), by striking "orders; and" and inserting the following: "orders, including—

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

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

(D) by redesignating paragraphs (4), (5), and (6) as paragraphs (5), (6), and (7), respectively; and

(E) by inserting after paragraph (3) the following:

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

information obtained or derived from electronic surveillance, physical search, or an acquisition conducted pursuant to this Act;"; and

(2) in subsection (d)—

(A) in paragraph (1), by striking "(4), or (5)" and inserting "(5), or (6)";

(B) in paragraph (2)(A), by striking "(2)(A), (2)(B), and (5)(C)" and inserting "(2)(B), (2)(C), and (6)(C)"; and

(C) in paragraph (3)(A), in the matter preceding clause (i), by striking "subsection (b)(2)(B)" and inserting "subsection (b)(2)(C)".

SEC. 203. CONGRESSIONAL REVIEW AND OVERSIGHT OF ABOUTS COLLECTION.

(a) IN GENERAL.—Section 702(b) (50 U.S.C. 1881a(b)) is amended—

(1) in paragraph (4), by striking "and" at the end;

(2) by redesignating paragraph (5) as paragraph (6); and

(3) by inserting after paragraph (4) the following:

"(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a facility, place, premises, or property at which an acquisition authorized under subsection (a) is directed or conducted, except as provided under section 203(b) of the FISA Amendments Reauthorization Act of 2017; and".

(b) CONGRESSIONAL REVIEW AND OVERSIGHT OF ABOUTS COLLECTION.—

(1) DEFINITIONS.—In this subsection:

(A) The term "abouts communication" means a communication that contains reference to, but is not to or from, a facility, a place, premises, or property at which an acquisition authorized under section 702(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(a)) is directed or conducted.

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

(2) SUBMISSION TO CONGRESS.—

(A) REQUIREMENT.—Notwithstanding any other provision of law, and except as provided in paragraph (4), if the Attorney General and the Director of National Intelligence intend to implement the authorization of the intentional acquisition of abouts communications, before the first such implementation after the date of enactment of this Act, the Attorney General and the Director of National Intelligence 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 written notice of the intent to implement the authorization of such an acquisition, and any supporting materials in accordance with this subsection.

(B) CONGRESSIONAL REVIEW PERIOD.—During the 30-day period beginning on the date written notice is submitted under subparagraph (A), 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 shall, as appropriate, hold hearings and briefings and otherwise obtain information in order to fully review the written notice.

(C) LIMITATION ON ACTION DURING CONGRESSIONAL REVIEW PERIOD.—Notwithstanding any other provision of law, and subject to paragraph (4), unless the Attorney General and the Director of National Intelligence make a determination pursuant to section 702(c)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(c)(2)), the Attorney General and the Director of National Intelligence may not implement the authorization of the intentional acquisition of abouts communications before the end of the period described in subparagraph (B).

(3) WRITTEN NOTICE.—Written notice under paragraph (2)(A) shall include the following:

(A) A copy of any certification submitted to the Foreign Intelligence Surveillance Court pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), or amendment thereto, authorizing the intentional acquisition of abouts communications, including all affidavits, procedures, exhibits, and attachments submitted therewith.

(B) The decision, order, or opinion of the Foreign Intelligence Surveillance Court approving such certification, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion.

(C) A summary of the protections in place to detect any material breach.

(D) Data or other results of modeling, simulation, or auditing of sample data demonstrating that any acquisition method involving the intentional

acquisition of abouts communications shall be conducted in accordance with title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.), if such data or other results exist at the time the written notice is submitted and were provided to the Foreign Intelligence Surveillance Court.

(E) Except as provided under paragraph (4), a statement that no acquisition authorized under subsection (a) of such section 702 shall include the intentional acquisition of an abouts communication until after the end of the 30-day period described in paragraph (2)(B).

(4) EXCEPTION FOR EMERGENCY ACQUISITION.—

(A) NOTICE OF DETERMINATION.—If the Attorney General and the Director of National Intelligence make a determination pursuant to section 702(c)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(c)(2)) with respect to the intentional acquisition of abouts communications, the Attorney General and the Director of National Intelligence shall notify 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 as soon as practicable, but not later than 7 days after the determination is made.

(B) IMPLEMENTATION OR CONTINUATION.—

(i) IN GENERAL.—If the Foreign Intelligence Surveillance Court approves a certification that authorizes the intentional acquisition of abouts communications before the end of the 30-day period described in paragraph (2)(B), the Attorney General and the Director of National Intelligence may authorize the immediate implementation or continuation of that certification if the Attorney General and the Director of National Intelligence jointly determine that exigent circumstances exist such that without such immediate implementation or continuation intelligence important to the national security of the United States may be lost or not timely acquired.

(ii) NOTICE.—The Attorney General and Director of National Intelligence 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 notification of a determination pursuant to clause (i) as soon as practicable, but not later than 3 days after the determination is made.

(5) REPORTING OF MATERIAL BREACH.—Subsection (m) of section 702 (50 U.S.C. 1881a), as redesignated by section 201, is amended—

(A) in the heading by striking "AND REVIEWS" and inserting "REVIEWS, AND REPORTING"; and

(B) by adding at the end the following new paragraph:

"(4) REPORTING OF MATERIAL BREACH.—

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

"(B) DEFINITIONS.—In this paragraph:

"(i) The term 'abouts communication' means a communication that contains reference to, but is not to or from, a facility, a place, premises, or property at which an acquisition authorized under subsection (a) is directed or conducted.

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

(6) APPOINTMENT OF AMICI CURIAE BY FOREIGN INTELLIGENCE SURVEILLANCE COURT.—For purposes of section 103(i)(2)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)(A)), the Foreign Intelligence Surveillance Court shall treat the first certification under section 702(g) of such Act (50 U.S.C. 1881a(g)) or amendment thereto that authorizes the acquisition of abouts communications as presenting a novel or significant interpretation of the law, unless the court determines otherwise.

SEC. 204. PUBLICATION OF MINIMIZATION PROCEDURES UNDER SECTION 702.

Section 702(e) (50 U.S.C. 1881a(e)) is amended by adding at the end the following new paragraph:

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

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

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

SEC. 205. COMPENSATION OF AMICI CURIAE AND TECHNICAL EXPERTS.

Subsection (i) of section 103 (50 U.S.C. 1803) is amended by adding at the end the following:

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

SEC. 206. ADDITIONAL REPORTING REQUIREMENTS.

(a) ELECTRONIC SURVEILLANCE.—Section 107 (50 U.S.C. 1807) is amended to read as follows:

"SEC. 107. REPORT OF ELECTRONIC SURVEILLANCE.

"(a) ANNUAL REPORT.—In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding calendar year—

"(1) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title;

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

"(3) the total number of persons who were subject to electronic surveillance conducted under an order or emergency authorization under this title, rounded to the nearest 500, including the number of such individuals who are United States persons, reported to the nearest band of 500, starting with 0–499.

"(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits each such report, the Attorney General shall make the report publicly available, or, if the Attorney General determines that the report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.".

(b) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 406 (50 U.S.C. 1846) is amended—

(1) in subsection (b)—

(A) in paragraph (4), by striking "; and" and inserting a semicolon;

(B) in paragraph (5), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(6) a good faith estimate of the total number of subjects who were targeted by the installation and use of a pen register or trap and trace device under an order or emergency authorization issued under this title, rounded to the nearest 500, including—

"(A) the number of such subjects who are United States persons, reported to the nearest band of 500, starting with 0–499; and

"(B) of the number of United States persons described in subparagraph (A), the number of persons whose information acquired pursuant to such order was reviewed or accessed by a Federal officer, employee, or agent, reported to the nearest band of 500, starting with 0–499."; and

(2) by adding at the end the following new subsection:

"(c) Each report under subsection (b) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits such a report, the Attorney General shall make the report publicly available, or, if the Attorney General determines that the report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.".

SEC. 207. PROCEDURES REGARDING DISSEMINATION OF NONPUBLICLY AVAILABLE INFORMATION CONCERNING UNITED STATES PERSONS.

(a) PROCEDURES.—

(1) IN GENERAL.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) is amended by adding at the end the following new section:

"SEC. 512. PROCEDURES REGARDING DISSEMINATION OF NONPUBLICLY AVAILABLE INFORMATION CONCERNING UNITED STATES PERSONS.

"(a) PROCEDURES.—The head of each element of the intelligence community, in consultation with the Director of National Intelligence, shall develop and maintain procedures for that element to respond to covered requests.

"(b) REQUIREMENTS.—The procedures under subsection (a) shall ensure, at a minimum, the following:

"(1) The originating element documents in writing each covered request received by the element, including—

"(A) the name or title of the individual of the requesting element who is making the request;

"(B) the name or title of each individual who will receive the United States person identity information sought by the covered request; and

"(C) a fact-based justification describing why such United States person identity information is required by each individual described in subparagraph (B) to carry out the duties of the individual.

"(2) A covered request may only be approved by the head of the originating element or by officers or employees of such element to whom the head has specifically delegated such authority.

"(3) The originating element retains records on covered requests, including the disposition of such requests, for not less than 5 years.

"(4) The records described in paragraph (3) include, with respect to approved covered requests, the name or title of the individual of the originating element who approved such request.

"(5) The procedures include an exception that—

"(A) allows for the immediate disclosure of United States person identity information in the event of exigent circumstances or where a delay could result in the loss of intelligence; and

"(B) requires that promptly after such disclosure the requesting element makes a covered request with respect to such information.

"(6) If a covered request is made during a period beginning on the date of a general election for President and ending on the date on which such President is inaugurated—

"(A) the documentation under paragraph (1) includes whether—

"(i) the individual of a requesting element who is making the request knows or believes that any United States person identity sought by the request is of an individual who is a member of the transition team of the President-elect and Vice-President-elect; or

"(ii) based on the intelligence community report to which the request pertains, the originating element knows or reasonably believes that any United States person identity sought by the request is of an individual who is a member of the transition team of the President-elect and Vice-President-elect;

"(B) the approval made pursuant to paragraph (2) of a covered request that contains a United States person identity described in subparagraph (A) is subject to the concurrence of the general counsel of the originating element (or, in the absence of the general counsel, the first assistant general counsel) that the dissemination of such identity information is in accordance with the procedures under subsection (a); and

"(C) consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the head of the originating element notifies the chairmen and ranking minority members of the congressional intelligence committees of any approval described in subparagraph (B) by not later than 14 days after the date of such approval.

"(c) ANNUAL REPORTS.—Not later than April 30 of each year, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report documenting, with respect to the year covered by the report—

"(1) the total number of covered requests received by that element;

"(2) of such total number, the number of requests approved;

"(3) of such total number, the number of requests denied; and

"(4) for each number calculated under paragraphs (1) through (3), the number listed by each requesting element.

"(d) CERTAIN PROCEDURES REGARDING CONGRESSIONAL IDENTITY INFORMATION.—

"(1) REQUIREMENTS.—With respect to the dissemination of congressional identity information, the head of each element of the intelligence community shall carry out this section in accordance with annex A of Intelligence Community Directive 112, or successor annex or directive.

"(2) NOTIFICATION.—The Director of National Intelligence may not modify or supersede annex A of Intelligence Community Directive 112, or successor annex or directive, unless—

"(A) the Director notifies the congressional intelligence committees of the proposed modifications or new annex or directive; and

"(B) a period of 30 days elapses following such notification.

"(e) EFFECT ON MINIMIZATION PROCEDURES.—The requirements of this section are in addition to any minimization procedures established pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), Executive Order No. 12333 (50 U.S.C. 3001 note), or successor order, or other relevant provision of law or executive order.

"(f) DEFINITIONS.—In this section:

"(1) The term 'covered request' means a request by a requesting element to an originating element for nonpublic identifying information with respect to a known unconsenting United States person that was omitted from an intelligence community report disseminated by the originating element.

"(2) The term 'originating element' means an element of the intelligence community that disseminates an intelligence community report that contains a reference to a known unconsenting United States person but omits nonpublic identifying information with respect to such person.

"(3) The term 'requesting element' means an element of the United States Government that receives an intelligence community report from an originating element and makes a covered request with respect to such report.

"(4) The term 'United States person' has the meaning given the term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).".

(2) CLERICAL AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 511 the following new item:

"Sec. 512. Procedures regarding dissemination of nonpublicly available information concerning United States persons.".

(b) DEVELOPMENT OF PROCEDURES.—The head of each element of the intelligence community shall develop the procedures required by section 512(a) of the National Security Act of 1947, as added by subsection (a)(1), by not later than 90 days after the date of the enactment of this Act.

(c) REPORT.—Not later than December 31, 2018, the Director of National Intelligence shall submit to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report assessing the compliance with the procedures required by section 512(a) of the National Security Act of 1947, as added by subsection (a)(1).

SEC. 208. IMPROVEMENTS TO PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.

(a) APPOINTMENT OF STAFF.—Subsection (j) of section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(j)) is amended—

(1) by redesignating paragraphs (2) and (3) as paragraphs (3) and (4), respectively; and

(2) by inserting after paragraph (1) the following new paragraph:

"(2) APPOINTMENT IN ABSENCE OF CHAIRMAN.—If the position of chairman of the Board is vacant, during the period of the vacancy, the Board, at the direction of the unanimous vote of the serving members of the Board, may exercise the authority of the chairman under paragraph (1).".

(b) MEETINGS.—Subsection (f) of such section (42 U.S.C. 2000ee(f)) is amended—

(1) by striking "The Board shall" and inserting "The Board";

(2) in paragraph (1) by striking "make its" and inserting "shall make its"; and

(3) in paragraph (2)—

(A) by striking "hold public" and inserting "shall hold public"; and

(B) by inserting before the period at the end the following: ", but may, notwithstanding section 552b of title 5, United States Code, meet or otherwise communicate in any number to confer or deliberate in a manner that is closed to the public".

SEC. 209. PRIVACY AND CIVIL LIBERTIES OFFICERS.

Section 1062(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee–1(a)) is amended by inserting ", the Director of the National Security Agency, the Director of the Federal Bureau of Investigation" after "the Director of the Central Intelligence Agency".

SEC. 210. WHISTLEBLOWER PROTECTIONS FOR CONTRACTORS OF THE INTELLIGENCE COMMUNITY.

(a) PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (a)—

(A) in paragraph (3), by inserting "or a contractor employee" after "character)"; and

(B) by adding at the end the following new paragraph:

"(4) CONTRACTOR EMPLOYEE.—The term 'contractor employee' means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element.";

(2) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively;

(3) by inserting after subsection (b) the following new subsection (c):

"(c) CONTRACTOR EMPLOYEES.—(1) Any employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take a personnel action with respect to any contractor employee as a reprisal for a lawful disclosure of information by the contractor employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, the head of the contracting agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the contracting agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the contractor employee reasonably believes evidences—

"(A) a violation of any Federal law, rule, or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or

"(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

"(2) A personnel action under paragraph (1) is prohibited even if the action is undertaken at the request of an agency official, unless the request takes the form of a nondiscretionary directive and is within the authority of the agency official making the request.";

(4) in subsection (b), by striking the heading and inserting "AGENCY EMPLOYEES.—"; and

(5) in subsection (e), as redesignated by paragraph (2), by inserting "contractor employee," after "any employee,".

(b) FEDERAL BUREAU OF INVESTIGATION.—

(1) IN GENERAL.—Any employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of the Federal Bureau of Investigation who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take a personnel action with respect to a contractor employee as a reprisal for a disclosure of information—

(A) made—

(i) to a supervisor in the direct chain of command of the contractor employee;

(ii) to the Inspector General;

(iii) to the Office of Professional Responsibility of the Department of Justice;

(iv) to the Office of Professional Responsibility of the Federal Bureau of Investigation;

(v) to the Inspection Division of the Federal Bureau of Investigation;

(vi) to the Office of Special Counsel; or

(vii) to an employee designated by any officer, employee, office, or division described in clauses (i) through (vii) for the purpose of receiving such disclosures; and

(B) which the contractor employee reasonably believes evidences—

(i) any violation of any law, rule, or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(2) ACTIONS BY REQUEST.—A personnel action under paragraph (1) is prohibited even if the action is undertaken at the request of an official of the Bureau, unless the request takes the form of a nondiscretionary directive and is within the authority of the official making the request.

(3) REGULATIONS.—The Attorney General shall prescribe regulations to ensure that a personnel action described in paragraph (1) shall not be taken against a contractor employee of the Bureau as a reprisal for any disclosure of information described in subparagraph (A) of such paragraph.

(4) ENFORCEMENT.—The President shall provide for the enforcement of this subsection.

(5) DEFINITIONS.—In this subsection:

(A) The term "contractor employee" means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of the Federal Bureau of Investigation.

(B) The term "personnel action" means any action described in clauses (i) through (x) of section 2302(a)(2)(A) of title 5, United States Code, with respect to a contractor employee.

(c) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—Section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)) is amended by adding at the end the following new paragraph:

"(8) INCLUSION OF CONTRACTOR EMPLOYEES.—In this subsection, the term 'employee' includes an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of an agency. With respect to such employees, the term 'employing agency' shall be deemed to be the contracting agency.".

SEC. 211. BRIEFING ON NOTIFICATION REQUIREMENTS.

Not later than 180 days after the date of the enactment of this Act, the Attorney General, in consultation with the Director of National Intelligence, shall provide 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 briefing with respect to how the Department of Justice interprets the requirements under sections 106(c), 305(d), and 405(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(c), 1825(d), and 1845(c)) to notify an aggrieved person under such sections of the use of information obtained or derived from electronic surveillance, physical search, or the use of a pen register or trap and trace device. The briefing shall focus on how the Department interprets the phrase "obtained or derived from" in such sections.

TITLE III—EXTENSION OF AUTHORITIES, INCREASED PENALTIES, REPORTS, AND OTHER MATTERS

SEC. 301. EXTENSION OF TITLE VII OF FISA; EFFECTIVE DATES.

(a) EXTENSION.—Section 403(b) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2474) is amended—

(1) in paragraph (1)—

(A) by striking "December 31, 2017" and inserting "December 31, 2021"; and

(B) by inserting "and by the FISA Amendments Reauthorization Act of 2017" after "section 101(a)"; and

(2) in paragraph (2) in the matter preceding subparagraph (A), by striking "December 31, 2017" and inserting "December 31, 2021".

(b) CONFORMING AMENDMENTS.—Section 404(b) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2476), as amended by section 201, is further amended—

(1) in paragraph (1)—

(A) in the heading, by striking "DECEMBER 31, 2017" and inserting "DECEMBER 31, 2021"; and

(B) by inserting "and by the FISA Amendments Reauthorization Act of 2017" after "section 101(a)";

(2) in paragraph (2), by inserting "and by the FISA Amendments Reauthorization Act of 2017" after "section 101(a)"; and

(3) in paragraph (4)—

(A) by inserting "and amended by the FISA Amendments Reauthorization Act of 2017" after "as added by section 101(a)" both places it appears; and

(B) by inserting "and by the FISA Amendments Reauthorization Act of 2017" after "as amended by section 101(a)" both places it appears.

(c) EFFECTIVE DATE OF AMENDMENTS TO FAA.—The amendments made to the FISA Amendments Act of 2008 (Public Law 110–261) by this section shall take effect on the earlier of the date of the enactment of this Act or December 31, 2017.

SEC. 302. INCREASED PENALTY FOR UNAUTHORIZED REMOVAL AND RETENTION OF CLASSIFIED DOCUMENTS OR MATERIAL.

Section 1924(a) of title 18, United States Code, is amended by striking "one year" and inserting "five years".

SEC. 303. REPORT ON CHALLENGES TO THE EFFECTIVENESS OF FOREIGN INTELLIGENCE SURVEILLANCE.

(a) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Attorney General, in coordination with the Director of National Intelligence, 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 on current and future challenges to the effectiveness of the foreign intelligence surveillance activities of the United States authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) MATTERS INCLUDED.—The report under subsection (a) shall include, at a minimum, the following:

(1) A discussion of any trends that currently challenge the effectiveness of the foreign intelligence surveillance activities of the United States, or could foreseeably challenge such activities during the decade following the date of the report, including with respect to—

(A) the extraordinary and surging volume of data occurring worldwide;

(B) the use of encryption;

(C) changes to worldwide telecommunications patterns or infrastructure;

(D) technical obstacles in determining the location of data or persons;

(E) the increasing complexity of the legal regime, including regarding requests for data in the custody of foreign governments;

(F) the current and future ability of the United States to obtain, on a compulsory or voluntary basis, assistance from telecommunications providers or other entities; and

(G) any other matters the Attorney General and the Director of National Intelligence determine appropriate.

(2) Recommendations for changes, including, as appropriate, fundamental changes, to the foreign intelligence surveillance activities of the United States to address the challenges identified under paragraph (1) and to ensure the long-term effectiveness of such activities.

(3) Recommendations for any changes to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) that the Attorney General and the Director of National determine necessary to address the challenges identified under paragraph (1).

(c) FORM.—The report under subsection (a) may be submitted in classified or unclassified form.

SEC. 304. COMPTROLLER GENERAL STUDY ON THE CLASSIFICATION SYSTEM AND PROTECTION OF CLASSIFIED INFORMATION.

(a) STUDY.—The Comptroller General of the United States shall conduct a study of the classification system of the United States and the methods by which the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) protects classified information.

(b) MATTERS INCLUDED.—The study under subsection (a) shall address the following:

(1) Whether sensitive information is properly classified.

(2) The effect of modern technology on the storage and protection of classified information, including with respect to—

(A) using cloud storage for classified information; and

(B) any technological means to prevent or detect unauthorized access to such information.

(3) Any ways to improve the classification system of the United States, including with respect to changing the levels of classification used in such system and to reduce overclassification.

(4) How to improve the authorized sharing of classified information, including with respect to sensitive compartmented information.

(5) The value of polygraph tests in determining who is authorized to access classified information and in investigating unauthorized disclosures of classified information.

(6) Whether each element of the intelligence community—

(A) applies uniform standards in determining who is authorized to access classified information; and

(B) provides proper training with respect to the handling of classified information and the avoidance of overclassification.

(c) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General 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 study under subsection (a).

(d) FORM.—The report under subsection (c) shall be submitted in unclassified form, but may include a classified annex.

SEC. 305. TECHNICAL AMENDMENTS AND AMENDMENTS TO IMPROVE PROCEDURES OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.

(a) TECHNICAL AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended as follows:

(1) In section 103(b) (50 U.S.C. 1803(b)), by striking "designate as the" and inserting "designated as the".

(2) In section 302(a)(1)(A)(iii) (50 U.S.C. 1822(a)(1)(A)(iii)), by striking "paragraphs (1) through (4)" and inserting "subparagraphs (A) through (D)".

(3) In section 406(b) (50 U.S.C. 1846(b)), by striking "and to the Committees on the Judiciary of the House of Representatives and the Senate".

(4) In section 604(a) (50 U.S.C. 1874(a))—

(A) in paragraph (1)(D), by striking "contents" and inserting "contents,"; and

(B) in paragraph (3), by striking "comply in the into" and inserting "comply into".

(5) In section 701 (50 U.S.C. 1881)—

(A) in subsection (a), by striking "The terms" and inserting "In this title, the terms"; and

(B) in subsection (b)—

(i) by inserting "In this title:" after the subsection heading; and

(ii) in paragraph (5), by striking "(50 U.S.C. 401a(4))" and inserting "(50 U.S.C. 3003(4))".

(6) In section 702(h)(2)(A)(i) (50 U.S.C. 1881a(h)(2)(A)(i)), as redesignated by section 201, by inserting "targeting" before "procedures in place".

(7) In section 801(7) (50 U.S.C. 1885(7)), by striking "(50 U.S.C. 401a(4))" and inserting "(50 U.S.C. 3003(4))".

(b) COURT-RELATED AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended as follows:

(1) In section 103 (50 U.S.C. 1803)—

(A) in subsection (b), by striking "immediately"; and

(B) in subsection (h), by striking "the court established under subsection (a)" and inserting "a court established under this section".

(2) In section 105(d) (50 U.S.C. 1805(d)), by adding at the end the following new paragraph:

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

(3) In section 302(d) (50 U.S.C. 1822(d)), by striking "immediately".

(4) In section 402(d) (50 U.S.C. 1842(d)), by adding at the end the following new paragraph:

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

(5) In section 403(c) (50 U.S.C. 1843(c)), by adding at the end the following new paragraph:

"(3) A denial of the application made under subsection (a)(2) may be reviewed as provided in section 103.".

(6) In section 501(c) (50 U.S.C. 1861(c)), by adding at the end the following new paragraph:

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

SEC. 306. SEVERABILITY.

If any provision of this Act, any amendment made by this Act, or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the Act, of any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

PURPOSES

The purposes of H.R. 4478 are to reauthorize title VII of the Foreign Intelligence Surveillance Act (FISA) for four years, to enhance surveillance authorities, and to provide additional transparency

and reporting requirements and privacy safeguards. Title VII of FISA is imperative to the national security of the United States, assists the armed forces of the United States, and supports the President in the execution of the foreign policy of the United States, particularly as it relates to counterterrorism matters.

SCOPE OF COMMITTEE REVIEW

The bill reauthorizes title VII of FISA, which includes FISA Section 702. FISA Section 702 provides a framework for the Government to target non-U.S. people located overseas to obtain foreign intelligence information, with the assistance of electronic communication service providers. The bill also makes critical amendments to other provisions of FISA, increases the effectiveness of the Privacy and Civil Liberties Oversight Board, amends the National Security Act of 1947 to add new procedures related to the dissemination of U.S. person identities that were previously redacted in intelligence community reporting, enhances penalties for the unauthorized removal of classified information, codifies privacy and civil liberties officers at specified Intelligence Community elements, and enhances whistleblower protections for contractors. The Committee has legislative and oversight jurisdiction over activities conducted pursuant to title VII of FISA.

COMMITTEE STATEMENT AND VIEWS

In the thirty years following FISA's enactment, in 1978, changes in communications technology came to strain, and in some cases even to thwart, some U.S. surveillance activities directed at foreigners overseas. Because foreign terrorists' communications were sometimes conveyed by electronic communication service providers located in the United States, the Government was forced to obtain individual, probable cause-based orders to conduct electronic surveillance against them—despite the U.S. Supreme Court's view that the Fourth Amendment does not protect foreign persons, overseas, from U.S. searches or seizures. The FISA Amendments Acts ("FAA") of 2008 updated FISA to address these issues.

The FAA of 2008 added title VII to FISA, which includes, among other things, FISA Section 702. Section 702 grants the Government the authority to target foreigners reasonably believed to be located outside the United States, with the directed assistance of electronic communication service providers, to obtain foreign intelligence information. Section 702 is a critical national security tool that provides invaluable assistance to the United States and its allies regarding counterterrorism efforts worldwide. H.R. 4478 not only reauthorizes title VII of FISA for four years, but also makes critical improvements to privacy and civil liberties while resulting in no negative operational impact to United States' surveillance authorities. The Committee believes that H.R. 4478 strikes the appropriate balance between privacy and national security.

Section 705 emergency provision

FISA Section 705(b) permits the government to obtain the Attorney General's approval, rather than seeking a separate FISA Court (FISC) order under FISA Sections 703 or 704, to conduct certain types of collection overseas against a United States person located

outside the United States who is already subject to a FISC order under Title I or Title III of FISA. Under the current statutory framework, there is no comparable concurrent authority in emergency situations. As a result, in emergency situations where the government wants to target a United States person located outside the United States under Titles I or III and Sections 703 or 704 of FISA, the Government must obtain two emergency authorization from the Attorney General, and then file two court applications with the FISC within seven days of the Attorney General granting the emergency authorizations.

Revising Section 705 to include an emergency provision will remove unnecessary resource costs and provide a more streamlined process in emergency situations, which is both consistent with the design and purpose of Section 705, as originally crafted in 2008.

Modification to definitions of foreign power and agent of a foreign power

Over the past several years, the number of cyber-related incidents impacting the United States has grown exponentially. With respect to activities under FISA, one obstacle to addressing that problem is that, unless the government can attribute malicious cyber activities to a foreign power, as currently defined in FISA, the government also cannot obtain a probable cause order to conduct electronic surveillance on the particular malicious cyber actor. Therefore, H.R. 4478 modifies FISA's definitions of "foreign power" and "agent of a foreign power" in order to make clear that certain non-state actors engaged in international malicious cyber activity, or activities in preparation therefor, that threaten the national defense or security of the United States, may be subject to a probable cause order for electronic surveillance under FISA.

It is not possible to anticipate all technologies and its potential uses, whether beneficial or malicious. The Committee wishes to note, therefore, its intention that the amended definitions be interpreted as broadly as possible, consistent with the U.S. Constitution, in order to enable collection targeting individuals and entities that use cyber tools and systems with the intention or actual effect of harming the national defense or security of the United States.

Querying procedures required

The Committee understands that certain lawmakers and privacy advocates worry about the ability of the Intelligence Community to query lawfully acquired data using query terms belonging to United States persons. This concern has been addressed, as the FISC and other federal courts have found that the incidental collection of non-target communications during authorized surveillance is lawful and consistent with the Fourth Amendment to the U.S. Constitution. Additionally, the courts have also determined the act of querying lawfully acquired FISA Section 702 data is lawful and permitted under the Fourth Amendment.

The Committee is dedicated to providing assurances to the American public that the procedures and processes currently in place satisfy the Fourth Amendment, and do not impede on United States person privacy. Therefore, the Committee believes that the Intelligence Community should have separate procedures documenting their current policies and practices related to the querying

of lawfully acquired FISA Section 702 data. Such procedures must be reviewed annually by the FISC.

This section requires that the Attorney General, in consultation with the Director of National Intelligence, adopt procedures that govern United States person queries of unminimized FISA Section 702 collection by any Intelligence Community element with access to such information. Although Section 201 of this bill requires the adoption of querying procedures, query refers only to retrievals "of or concerning United States persons," and therefore, the new querying procedures requirement does not apply to queries that are not specifically intended to return communications "of or concerning United States persons."

Regarding whether a query retrieval is "of or concerning United States persons," this section is not intended to and does not require that Intelligence Community personnel investigate or determine whether every query term pertains to a United States person before or after conducting a query. Congress understands that, for many queries, personnel will have no reason to think the query will or will not bring back information "of or concerning United States persons" and in those instances does not intend for the procedures to apply.

The Attorney General has the discretion to adopt either a single set of procedures, which would be applicable to all Intelligence Community elements that receive unminimized FISA Section 702 collection, or discrete sets of procedures for each such element that are designed to account for the differing missions of those elements. Regardless of the approach taken by the Attorney General, any procedures ultimately adopted must be submitted to the FISC for judicial review to ensure that such procedures are consistent with the requirements of the Fourth Amendment to the U.S. Constitution.

Section 201 further mandates that all querying procedures include a provision requiring that a record is kept for each United States person query term used for a query of FISA Section 702 data. With respect to the retention of such records, Congress intends that the privacy interests of United States persons be protected by requiring the Government to apply a reasonable retention period consistent with each agency's mission and the desire to ensure such records are retained for appropriate oversight purposes. This section is not intended to, and does not impose a requirement that an Intelligence Community element maintain records of United States person query terms in any particular manner, so long as appropriate records are retained and thus available for subsequent oversight. This section ensures that the manner in which the element retains records of United States person query terms is within the discretion of the Attorney General, in consultation with the Director of National Intelligence and subject to the approval of the FISC.

Restrictions on the Use of Incidentally Collected U.S. Person Information in Criminal Matters

Section 201 provides the Federal Bureau of Investigation (FBI) with discretion to apply for an order from the FISC *prior to* initially accessing the contents of communications that were retrieved using a United States person query term that was not designed by

FBI, in whole or in part, to find and extract foreign intelligence information. Section 201 does not require that the FBI obtain an order before either conducting a query, or accessing the results of that query. Accordingly, the section does not interfere with the FBI's ability to find, identify, and act upon information within the Section 702 collection concerning threats to national security.

At the same time, together with Section 202, Section 201 furnishes an incentive for FBI criminal investigators to seek court approval, should they seek to review U.S. person communications obtained pursuant to Section 702 for the specific purpose of finding evidence of, and later prosecuting, the commission by U.S. persons of "garden variety" crimes like bank robbery or tax fraud. The Committee does not believe that the FBI currently uses Section 702 in this fashion, or intends to. Nevertheless, during debate over Section 702's reauthorization, the concern was raised that FBI might do so at some stage in the future.

To address that concern, Sections 201 and 202 employ an exclusionary rule, in criminal prosecutions of U.S. persons. As noted above, before FBI initially accesses the contents of communications retrieved using a query subject to Section 201, the FBI must decide whether to seek a court order authorizing such access. Should the FBI opt *not* to apply for an order, or if the FISC denies such an application, prosecutors thereafter will be precluded from using the query results in evidence against the United States person in any criminal proceeding, subject to exceptions set out in the statute.

Specifically: Absent a court order, information concerning a U.S. person acquired under Section 702 may be introduced into evidence against the U.S. person in question, only if the Attorney General has determined that the criminal proceeding affects, involves, or is related to U.S. national security; or involves extremely serious conduct or offenses outside the national security context.

Sections 201 and 202 do not reflect the Committee's disagreement with past court opinions, or a view that lawfully collected FISA Section 702 data should be subject to a different Fourth Amendment analysis than other lawfully collected data. Instead, language in Section 201 and 202 regarding court orders and criminal prosecutions is intended to provide a safeguard against the potential use of U.S. person information incidentally collected pursuant to Section 702, for inappropriate criminal purposes.

Congressional review and oversight of abouts collection

Under FISA Section 702, the National Security Agency (NSA) has the ability to collect internet communications in its so-called "upstream" collection (i.e. collection with the assistance of providers that control the telecommunications backbone). Because of the way communications are packaged and traverse the telecommunications backbone, the NSA was not only able to retrieve the communications "to" or "from" a FISA Section 702 target, but also "about" a FISA Section 702 target, subject to procedures annually approved by the FISC. This Committee does not believe that "abouts" collection is outside the scope of FISA Section 702. However, due to a compliance incident of a technical nature that was reported to the FISC last year, the NSA proactively and temporarily halted its "abouts" communication collection in order to make necessary tech-

nical changes. The NSA has kept Congress fully and currently informed of this issue.

Section 203 adds a new limitation concerning "abouts" collection. Specifically, Section 203 prohibits the intentional acquisition of "abouts" communications unless Congress is provided with notice of, and an opportunity to review such collection before it begins. The Committee understands that the targeting procedures currently used by the NSA to conduct acquisitions pursuant to FISA Section 702 prohibit the acquisition of communications that are not "to" or "from" a FISA Section 702 target. The new limitation established by Section 203 is intended to codify only current procedures and is not intended to affect acquisitions currently being conducted under FISA Section 702.

Compensation of amici curiae and technical experts

Section 205 of H.R. 4478 authorizes the FISC to compensate court-appointed amici curiae and technical experts, in the same fashion and to the same extent as other federal courts. The authority is important, given the increasingly complicated technological issues which the FISC regularly confronts.

The authority to appoint amici—including for the purpose of "providing technical expertise" to the FISC—is forth at 50 U.S.C. 1803(i)(2). Appointed amici may be required, moreover, to furnish to the FISC "information related to intelligence collection or communications technology." *Id.* at 1803(i)(4)(B).

The Committee fully expects and encourages the appointment and compensation of technical experts, in order to ensure that in relevant cases, the FISC has the fullest possible understanding of complex technical matters.

COMMITTEE CONSIDERATION AND ROLL CALL VOTES

On December 1, 2017, the committee met in open session and ordered the bill H.R. 4478 favorably reported.

In open session, the committee considered the text of the bill H.R. 4478. Chairman Nunes offered an Amendment in the Nature of a Substitute (ANS), making technical edits to H.R. 4478, as well as adding three new sections of the bill: increased whistleblower protections for IC contractors, a briefing on the Government's interpretation and implement of "derived from" in the FISA context, and a report on any future implementation challenges associated with FISA collection. Chairman Nunes' ANS passed by a voice vote.

Ranking Member Schiff offered an amendment to the ANS which would seek to strike Section 207 of the bill related to procedures associated with the dissemination of U.S. person information in disseminated intelligence community reporting. The amendment was voted down by voice vote.

Chairman Nunes then moved for final consideration of H.R. 4478, as amended. The motion was agreed to by a record vote of 13 ayes and 8 noes:

> Voting aye: Chairman Nunes, Mr. Conaway, Mr. King, Mr. LoBiondo, Ms. Ros-Lehtinen, Mr. Rooney, Mr. Turner, Mr. Wenstrup, Mr. Stewart, Mr. Crawford, Mr. Gowdy, Ms. Stefanik, and Mr. Hurd.
>
> Vote no: Ranking Member Schiff, Mr. Himes, Ms. Sewell, Mr. Carson, Ms. Speier, Mr. Swalwell, Mr. Castro, and Mr. Heck.

The Committee then agreed to a motion by the Chairman to favorably report the bill H.R. 4478 to the House, as amended. The motion was agreed to by a voice vote.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF AMENDMENT

Section 1—Short title; table of contents

Section 1 lists the short title and table of contents of the FISA Amendments Reauthorization Act of 2017 (the Act).

Section 2—Amendments to the Foreign Intelligence Surveillance Act of 1978

Section 2 provides clarity that any amendment or repeal shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (FISA), unless otherwise specified.

TITLE I—ENHANCEMENTS TO FOREIGN INTELLIGENCE COLLECTION

Section 101—Section 705 emergency fix

Section 101 adds an emergency authorization provision to FISA Section 705, which governs joint applications and concurrent authorizations.

Section 102—Modification to definitions of foreign power and agent of a foreign power

Section 102 amends the FISA definitions of "foreign power" and "agent of a foreign power" to account for foreign entities engaged in international malicious cyber activity that threatens the national defense or security of the United States.

TITLE II—SAFEGUARDS, ACCOUNTABILITY, AND OVERSIGHT

Section 201—Querying procedures required

Section 201 requires that the Intelligence Community develop separate procedures related to the querying of lawfully acquired FISA Section 702 information. These procedures will be reviewed by the Foreign Intelligence Surveillance Court (FISC) every year.

Furthermore, Section 201 institutes an optional order requirement, which states that the FBI may obtain an order to initially view the content of FISA Section 702 communications that were responsive to U.S. person queries that were not designed to return foreign intelligence information. As provided in Section 202 of the Act, if the FBI decides to obtain an order to initially view the content, they may use the communication in a criminal case. If the FBI decides to forego an order, the responsive FISA Section 702 communication may only be used in prosecutions pursuant to the "use" restrictions identified in Section 202 of the Act.

Section 202—Use and disclosure provisions

Section 202 sets restrictions on the Government's use of FISA Section 702 communications of a U.S. person as evidence against that U.S. person in any criminal proceeding unless the FBI obtains an order as described in Section 201 of the Act, or the Attorney

General authorizes such use in a criminal proceeding that falls into one of the serious crimes designated in the section. The section also provides for increased transparency by adding new reporting requirements related to various FISA provisions.

Section 203—Congressional review and oversight of abouts collection

Section 203 limits the collection of communications that contain a reference to, but are not to or from (i.e. "abouts" collection), a FISA Section 702 foreign intelligence surveillance target. The section provides that the Government may initiate this collection only after obtaining approval from the FISC and submitting all supporting documents to the congressional intelligence and judiciary committees for review no less than 30 days prior to recommencing this type of collection. This section also requires additional incident compliance notification related to "abouts" collection.

Section 203 also presumes the appointment of amici curiae during the FISC's review of the first FISA Section 702 certification that reconstitutes collection of communications that contain a reference to, but are not to or from, a FISA Section 702 foreign intelligence surveillance target.

Section 204—Publication of minimization procedures under Section 702

Section 204 requires that the Director of National Intelligence and the Attorney General conduct a declassification review and publicly release the FISA Section 702 minimization procedures every year.

Section 205—Compensation of amici curiae and technical experts

Section 205 grants the FISC the authority to compensate any appointed amicus curiae.

Section 206—Additional reporting requirements

Section 206 requires additional reporting requirements related to how the Intelligence Community (IC) utilizes other sections of FISA.

Section 207—Procedures regarding dissemination of nonpublicly available information concerning United States persons

Section 207 adds a new section to the National Security Act of 1947 that requires certain procedures governing the handling of requests for nonpublicly available U.S. person identities that were originally redacted in intelligence community reporting. These procedures must include, but are not limited to, the requirement that an individual requesting a U.S. person identity include a fact-based, individualized justification as to why that individual needs the U.S. person identity, new congressional reporting requirements, and an elevated review for U.S. person identity requests that pertain to members of the president or vice-president's transition teams during times of presidential transition.

Section 208—Improvements to Privacy and Civil Liberties Oversight Board

Section 208 reforms the Privacy and Civil Liberties Oversight Board (the Board) such that the Board no longer falls under the requirement for open meetings pursuant to Section 552b(a)(1) of title 5, United States Code. Section 208 also amends the Intelligence Reform and Terrorism Prevention Act of 2004 such that the Board now has the ability to exercise the authority of the Chairman of the Board if such position is vacant or a quorum is absent, so long as such authority is exercised by a unanimous vote of the serving members of the Board.

Section 209—Privacy and civil liberties officers

Section 209 codifies the requirement that certain elements of the Intelligence Community maintain privacy and civil liberties officers.

Section 210—Whistleblower protections for contractors of the intelligence community

Section 210 increases whistleblower protections for IC contractors by providing protection from reprisals made in response to IC contractors exercising their right to report fraud, waste, or abuse.

Section 211—Briefing on notification requirements

Section 211 requires the Attorney General and Director of National Intelligence to brief the congressional intelligence and judiciary committees on their interpretation of the "derived from" standard in FISA, as well as how the Government interprets certain notification requirements in FISA related to aggrieved persons.

TITLE III—EXTENSION OF FISA AUTHORITIES, INCREASED PENALTIES, REPORTS, AND OTHER MATTERS

Section 301—Extension of title VII of FISA; effective dates

Section 301 reauthorizes title VII of FISA, which includes FISA Section 702, for four years.

Section 302—Increased penalty for unauthorized removal and retention of classified documents or material

Section 302 increases the penalties for the unauthorized removal and retention of classified documents or material from one year to five years.

Section 303—Report on challenges to the effectiveness of foreign intelligence surveillance

Section 303 requires the Attorney General and Director of National Intelligence to submit to the congressional intelligence and judiciary committees a report on current and future challenges to the effectiveness of FISA surveillance authorities.

Section 304—Comptroller General study on the classification system and protection of classified information

Section 304 requires the Comptroller General to conduct a study and report on the U.S. classification system and how the IC protects classified information.

Section 305—Technical amendments and amendments to improve procedures of the Foreign Intelligence Surveillance Court of Review

Section 305 makes several technical amendments to FISA and amendments to clarify procedures related to the Foreign Intelligence Surveillance Court of Review.

Section 306—Severability

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, over the past two years, the Committee held multiple hearings and hosted various Member and staff-level education sessions related to the authorities reauthorized in H.R. 4478. The bill, as reported by the Committee, is the product of these various oversight sessions.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goals and objectives of H.R. 4478 are to reauthorize title VII of FISA for four years, as well as enhance surveillance authorities and provide additional transparency and reporting requirements. Title VII of FISA is imperative to the national security of the United States, supports and assists the armed forces of the United States, and supports the President in the execution of the foreign policy of the United States, particularly as it relates to counterterrorism matters.

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104–4) requires a statement of whether the provision of the reported bill include unfunded mandates. In compliance with this requirement, the Committee has received a letter from the Congressional Budget Office included herein.

STATEMENT ON CONGRESSIONAL EARMARKS

Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits.

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".

* * * * * * *

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**[**.**]***; or*

(8) an entity not substantially composed of United States persons that is engaged in international malicious cyber activity, or activities in preparation therefor, that threatens the national defense or security of the United States.

(b) "Agent of a foreign power" means—

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

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

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

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

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

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or

knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(F) engages in international malicious cyber activity that threatens the national defense or security of the United States, 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 international malicious cyber activity or activities in preparation therefor, or knowingly conspires with any person to engage in such international malicious cyber activity 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 Attor-

ney 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.

(q)(1) The term "international malicious cyber activity" means activity on or through an information system—

(A) originating from, or directed by, persons located, in whole or in substantial part, outside the United States;

(B) that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information systems or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon; and

(C) that is not authorized by the United States Government or otherwise carried out in accordance with Federal law.

(2) In paragraph (1), the term "information system" has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501), and includes national security systems (as defined in section 11103 of title 40, United States Code).

* * * * * * *

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)] *section 702(i)*, hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

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

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

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

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

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

section (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)**]** *a court established under this section* to determine or enforce

compliance with an order or a rule of such court or with a procedure approved by such court.

(i) AMICUS CURIAE.—

(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after the enactment of this subsection, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

(2) AUTHORIZATION.—A court established 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), the amicus curiae—

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

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

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

(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or 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 designated to serve as amicus curiae under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

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

(11) COMPENSATION.—Notwithstanding any other provision of law, a court established under subsection (a) or (b) may compensate an amicus curiae appointed under paragraph (2) for as-

sistance provided under such paragraph as the court considers appropriate and at such rate as the court considers appropriate.

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

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

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

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

* * * * * * *

ISSUANCE OF AN ORDER

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

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

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

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

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

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

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

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

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

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

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

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

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

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

(2) 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.

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

(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 prac-

ticable, but not later than 7 days after the Attorney General authorizes such surveillance.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(A) it is not reasonable to—

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

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

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

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

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

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

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

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

* * * * * * *

[REPORT OF ELECTRONIC SURVEILLANCE

[SEC. 107. In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—

[(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and

[(b) the total number of such orders and extensions either granted, modified, or denied.]

SEC. 107. REPORT OF ELECTRONIC SURVEILLANCE.

(a) ANNUAL REPORT.—In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding calendar year—

(1) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title;

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

(3) the total number of persons who were subject to electronic surveillance conducted under an order or emergency authorization under this title, rounded to the nearest 500, including the number of such individuals who are United States persons, reported to the nearest band of 500, starting with 0–499.

(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits each such report, the Attorney General shall make the report publicly available, or, if the Attorney General determines that the report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.

* * * * * * *

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

* * * * * * *

AUTHORIZATION OF PHYSICAL SEARCHES FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 302. (a)(1) Notwithstanding any other provision of law, the President, acting through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information for periods of up to one year if—

(A) the Attorney General certifies in writing under oath that—

(i) the physical search is solely directed at premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers (as defined in section 101(a) (1), (2), or (3));

(ii) there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States person; and

(iii) the proposed minimization procedures with respect to such physical search meet the definition of minimization procedures under ⟦paragraphs (1) through (4)⟧ *subparagraphs (A) through (D)* of section 301(4); and

(B) the Attorney General reports such minimization procedures and any changes thereto to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate at least 30 days before their effective date, unless the Attorney General determines that immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) A physical search authorized by this subsection may be conducted only in accordance with the certification and minimization

procedures adopted by the Attorney General. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under the provisions of section 306.

(3) The Attorney General shall immediately transmit under seal to the Foreign Intelligence Surveillance Court a copy of the certification. Such certification shall be maintained under security measures established by the Chief Justice of the United States with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the physical search is made under section 301(4) and section 303; or

(B) the certification is necessary to determine the legality of the physical search under section 305(g).

(4)(A) With respect to physical searches authorized by this subsection, the Attorney General may direct a specified landlord, custodian, or other specified person to—

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

(ii) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the search or the aid furnished that such person wishes to retain.

(B) The Government shall compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the Foreign Intelligence Surveillance Court. Notwithstanding any other provision of law, a judge of the court to whom application is made may grant an order in accordance with section 304 approving a physical search in the United States of the premises, property, information, or material of a foreign power or an agent of a foreign power for the purpose of collecting foreign intelligence information.

(c) The Foreign Intelligence Surveillance Court shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence information anywhere within the United States under the procedures set forth in this title, except that no judge (except when sitting en banc) shall hear the same application which has been denied previously by another judge designated under section 103(a) of this Act. If any judge so designated denies an application for an order authorizing a physical search under this title, such judge shall provide immediately for the record a written statement of each reason for such decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established under section 103(b).

(d) The court of review established under section 103(b) shall have jurisdiction to review the denial of any application made under this title. 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.

(e) Judicial proceedings under this title shall be concluded as expeditiously as possible. The record of proceedings under this title, including applications made and orders granted, 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.

* * * * * * *

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

* * * * * * *

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

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

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

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

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

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

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

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

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation

of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution; and

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

(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.

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

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

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

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

(g) Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable

intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) PRIVACY PROCEDURES.—

(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

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

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.

(3) A denial of the application made under subsection (a)(2) may be reviewed as provided in section 103.

(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;

(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)**[**.**]***; and*

(6) a good faith estimate of the total number of subjects who were targeted by the installation and use of a pen register or trap and trace device under an order or emergency authorization issued under this title, rounded to the nearest 500, including—

(A) the number of such subjects who are United States persons, reported to the nearest band of 500, starting with 0–499; and

(B) of the number of United States persons described in subparagraph (A), the number of persons whose information acquired pursuant to such order was reviewed or accessed by a Federal officer, employee, or agent, reported to the nearest band of 500, starting with 0–499.

(c) Each report under subsection (b) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits such a report, the Attorney General shall make the report publicly available, or, if the Attorney General determines that the report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.

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 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.

(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;

(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;

(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

(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;

(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).

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

(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 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 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 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 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 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)(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 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).

(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 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.—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 proce-

dures 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.

* * * * * * *

TITLE VI—OVERSIGHT

* * * * * * *

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;⟧ *good faith estimate of—*

(A) the number of targets of such orders;

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

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

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

(A) the number of targets of such orders;

⟦(A)⟧ *(B)* 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)⟧ *(C)* 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;

(D) the number of instances in which the Federal Bureau of Investigation has received and reviewed the unminimized contents of electronic communications or wire communications concerning a United States person obtained through acquisitions authorized under such section in response to a search term that was not designed to find and extract foreign intelligence information; and

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

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

(A) the number of targets of such **[**orders; and**]** *orders, including—*

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

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

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

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

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

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

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

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

(A) the number of targets of such orders;

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

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

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

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

(d) EXCEPTIONS.—

(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), **[**(4), or (5)**]** *(5), or (6)* of subsection (b) is fewer than 500, it shall be expressed as a numerical range of "fewer than 500" and shall not be expressed as an individual number.

(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs [(2)(A), (2)(B), and (5)(C)] *(2)(B), (2)(C), and (6)(C)* of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

(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)] *subsection (b)(2)(C)* cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

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

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

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

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

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

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

(e) 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] *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] *comply 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 sub-

section 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. 701. DEFINITIONS.

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

(b) ADDITIONAL DEFINITIONS.—*In this title:*

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

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

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

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

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

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

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

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

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

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

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

(5) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 **[**(50 U.S.C. 401a(4))**]** *(50 U.S.C. 3003(4))*.

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

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

(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; [and]

(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a facility, place, premises, or property at which an acquisition authorized under subsection (a) is directed or conducted, except as provided under section 203(b) of the FISA Amendments Reauthorization Act of 2017; and

[(5)] *(6)* shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) CONDUCT OF ACQUISITION.—

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

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

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

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

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

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

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

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

(d) TARGETING PROCEDURES.—

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

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

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

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

(e) MINIMIZATION PROCEDURES.—

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

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

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

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

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

(f) QUERIES.—

(1) PROCEDURES REQUIRED.—

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

(B) RECORD OF UNITED STATES PERSON QUERY TERMS.—The Attorney General, in consultation with the Director of National Intelligence, shall ensure that the procedures adopted under subparagraph (A) include a technical procedure whereby a record is kept of each United States person query term used for a query.

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

(2) COURT ORDERS FOR ACCESS OF CONTENTS FROM CERTAIN QUERIES.—

(A) DISCRETION FOR FBI TO APPLY FOR COURT ORDER.—Before the Federal Bureau of Investigation accesses the contents of communications acquired under subsection (a) that were retrieved using a United States person query term that was not designed to find and extract foreign intelligence information, the Bureau may apply for an order of the Court under subparagraph (C).

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

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

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

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

(I) criminal activity;

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

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

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

(E) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to prohibit the Federal Bureau of Investigation from querying information acquired under subsection (a), or accessing the results of such a query, regardless of whether the Bureau applies for or receives an order under this paragraph.

(3) QUERY DEFINED.—In this subsection, the term "query" means the use of one or more terms to retrieve the unminimized contents (as defined in section 2510(8) of title 18, United States Code) or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under subsection (a).

[(f)] *(g)* GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

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

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

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

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

(A) the congressional intelligence committees;

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

(C) the Foreign Intelligence Surveillance Court.

[(g)] *(h)* CERTIFICATION.—

(1) IN GENERAL.—

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

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

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

(A) attest that—

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

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

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

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

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

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

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

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

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

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

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

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

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

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

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

(D) include—

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

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

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

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

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

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

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

[(h)] *(i)* DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

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

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

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

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

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

(4) CHALLENGING OF DIRECTIVES.—

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

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

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

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

promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

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

tion 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)**]** *(j)* JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

(1) IN GENERAL.—

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

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

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

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

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

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

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

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

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

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

(3) ORDERS.—

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

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

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

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

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

(D) LIMITATION ON USE OF INFORMATION.—

(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the 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)] *with subsection (h)* and the procedures adopted in accordance [with subsections (d) and (e)] *with subsections (d), (e), and (f)(1)* at least 30 days prior to the expiration of such authorization.

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

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

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

[(k)] *(l)* MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

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

[(l)] *(m)* ASSESMENTS [AND REVIEWS] *REVIEWS, AND REPORTING*.—

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

(A) the Foreign Intelligence Surveillance Court; and

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

(i) the congressional intelligence committees; and

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

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

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

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

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

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

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

(I) the congressional intelligence committees; and

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

(3) ANNUAL REVIEW.—

(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an an-

nual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

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

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

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

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

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

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

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

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

(I) the congressional intelligence committees; and

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

(4) REPORTING OF MATERIAL BREACH.—

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

(B) DEFINITIONS.—In this paragraph:

(i) The term "abouts communication" means a communication that contains reference to, but is not to or from, a facility, a place, premises, or property at which an acquisition authorized under subsection (a) is directed or conducted.

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

* * * * * * *

SEC. 705. JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS.

(a) JOINT APPLICATIONS AND ORDERS.—If an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 703(a)(1) or 704(a)(1) may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 703(b) and 704(b), orders under sections 703(c) and 704(c), as appropriate.

(b) CONCURRENT AUTHORIZATION.—If an order authorizing electronic surveillance or physical search has been obtained under section 105 or 304, the Attorney General may authorize, for the effective period of that order, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

(c) EMERGENCY AUTHORIZATION.—

(1) CONCURRENT AUTHORIZATION.—If the Attorney General authorized the emergency employment of electronic surveillance or a physical search pursuant to section 105 or 304, the Attorney General may authorize, for the effective period of the emergency authorization and subsequent order pursuant to section 105 or 304, without a separate order under section 703 or 704, the targeting of a United States person subject to such emergency employment for the purpose of acquiring foreign intelligence information while such United States person is reasonably believed to be located outside the United States.

(2) USE OF INFORMATION.—If an application submitted to the Court pursuant to section 104 or 304 is denied, or in any other case in which the acquisition pursuant to paragraph (1) is terminated and no order with respect to the target of the acquisition is issued under section 105 or 304, all information obtained or evidence derived from such acquisition shall be handled in accordance with section 704(d)(4).

SEC. 706. USE OF INFORMATION ACQUIRED UNDER TITLE VII.

(a) INFORMATION ACQUIRED UNDER SECTION 702.—[Information acquired]

(1) IN GENERAL.—Information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.

(2) UNITED STATES PERSONS.—

(A) IN GENERAL.—Any information concerning a United States person acquired under section 702 shall not be used in evidence against that United States person pursuant to paragraph (1) in any criminal proceeding unless—

(i) the Federal Bureau of Investigation obtained an order of the Foreign Intelligence Surveillance Court to access such information pursuant to section 702(f)(2); or

(ii) the Attorney General determines that—

(I) the criminal proceeding affects, involves, or is related to the national security of the United States; or

(II) the criminal proceeding involves—

(aa) death;

(bb) kidnapping;

(cc) serious bodily injury, as defined in section 1365 of title 18, United States Code;

(dd) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006 (34 U.S.C. 20911);

(ee) incapacitation or destruction of critical infrastructure, as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e));

(ff) cybersecurity, including conduct described in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) or section 1029, 1030, or 2511 of title 18, United States Code;

(gg) transnational crime, including transnational narcotics trafficking and transnational organized crime; or

(hh) human trafficking.

(B) NO JUDICIAL REVIEW.—A determination by the Attorney General under subparagraph (A)(ii) is not subject to judicial review.

(b) INFORMATION ACQUIRED UNDER SECTION 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

SEC. 707. CONGRESSIONAL OVERSIGHT.

(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, 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, concerning the implementation of this title.

(b) CONTENT.—Each report under subsection (a) shall include—

(1) with respect to section 702—

(A) any certifications submitted in accordance with ⟦section 702(g)⟧ *section 702(h)* during the reporting period;

(B) with respect to each determination under section 702(c)(2), the reasons for exercising the authority under such section;

(C) any directives issued under [section 702(h)] *section 702(i)* during the reporting period;

(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with subsections (d) and (e) of section 702 and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 702;

(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of [section 702(h)] *section 702(i)*;

(F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 702(a);

(G) a description of any incidents of noncompliance—

(i) with a directive issued by the Attorney General and the Director of National Intelligence under [section 702(h)] *section 702(i)*, including incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under [section 702(h)] *section 702(i)*; and

(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with [subsections (d), (e), and (f)] *subsections (d), (e), (f)(1), and (g)* of section 702; and

(H) any procedures implementing section 702;

(2) with respect to section 703—

(A) the total number of applications made for orders under section 703(b);

(B) the total number of such orders—

(i) granted;

(ii) modified; and

(iii) denied; and

(C) the total number of emergency acquisitions authorized by the Attorney General under section 703(d) and the total number of subsequent orders approving or denying such acquisitions; and

(3) with respect to section 704—

(A) the total number of applications made for orders under section 704(b);

(B) the total number of such orders—

(i) granted;

(ii) modified; and

(iii) denied; and

(C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such applications.

* * * * * * *

TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

SEC. 801. DEFINITIONS.

In this title:

(1) ASSISTANCE.—The term "assistance" means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

(2) CIVIL ACTION.—The term "civil action" includes a covered civil action.

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

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

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

(4) CONTENTS.—The term "contents" has the meaning given that term in section 101(n).

(5) COVERED CIVIL ACTION.—The term "covered civil action" means a civil action filed in a Federal or State court that—

(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and

(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

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

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

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

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

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;

(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or

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

(7) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 ~~[~~(50 U.S.C. 401a(4))~~]~~ *(50 U.S.C. 3003(4))*.

(8) PERSON.—The term "person" means—

(A) an electronic communication service provider; or

(B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—

(i) an order of the court established under section 103(a) directing such assistance;

(ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code; or

(iii) a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), or 702(h).

(9) STATE.—The term "State" means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

* * * * * * *

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2008

* * * * * * *

TITLE IV—OTHER PROVISIONS

* * * * * * *

SEC. 404. TRANSITION PROCEDURES.

(a) TRANSITION PROCEDURES FOR PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

(i) the expiration of such order, authorization, or directive; or

(ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) PROTECTION FROM LIABILITY.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

(A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;

(iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and

(iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been in-

cluded in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification [under section 702(i)(3)] *under section 702(j)(3)* of such Act (as so added) at which time the provisions of that section and [of section 702(i)(4)] *of section 702(j)(4)* of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON DECEMBER 31, 2017.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or direc-

tive referred to in paragraph (1), title VII of such Act, as amended by section 101(a), shall continue to apply until the later of—

(A) the expiration of such order, authorization, or directive; or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant [to section 702(h)] *to section 702(i)* of such Act, as added by section 101(a);

(B) [section 702(h)(3) of] *section 702(i)(3) of* such Act (as so added) shall continue to apply with respect to any directive issued pursuant [to section 702(h)] *to section 702(i)* of such Act (as so added);

(C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), [and sections 702(l)] *and sections 702(m)* and 707 of such Act, as added by section 101(a), shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), [or

section 702(l)] *or section 702(m)* or 707 of such Act, as added by section 101(a), relating to any acquisition conducted under title VII of such Act, as amended by section 101(a), has been included in a review, assessment, or report under such section 601, 702(l), or 707.

(5) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

NATIONAL SECURITY ACT OF 1947

SHORT TITLE

That this Act may be cited as the "National Security Act of 1947".

TABLE OF CONTENTS

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

* * * * * * *

SEC. 512. PROCEDURES REGARDING DISSEMINATION OF NONPUBLICLY AVAILABLE INFORMATION CONCERNING UNITED STATES PERSONS.

(a) PROCEDURES.—The head of each element of the intelligence community, in consultation with the Director of National Intelligence, shall develop and maintain procedures for that element to respond to covered requests.

(b) REQUIREMENTS.—The procedures under subsection (a) shall ensure, at a minimum, the following:

(1) The originating element documents in writing each covered request received by the element, including—

(A) the name or title of the individual of the requesting element who is making the request;

(B) the name or title of each individual who will receive the United States person identity information sought by the covered request; and

(C) a fact-based justification describing why such United States person identity information is required by each individual described in subparagraph (B) to carry out the duties of the individual.

(2) A covered request may only be approved by the head of the originating element or by officers or employees of such element to whom the head has specifically delegated such authority.

(3) The originating element retains records on covered requests, including the disposition of such requests, for not less than 5 years.

(4) The records described in paragraph (3) include, with respect to approved covered requests, the name or title of the individual of the originating element who approved such request.

(5) The procedures include an exception that—

(A) allows for the immediate disclosure of United States person identity information in the event of exigent circumstances or where a delay could result in the loss of intelligence; and

(B) requires that promptly after such disclosure the requesting element makes a covered request with respect to such information.

(6) If a covered request is made during a period beginning on the date of a general election for President and ending on the date on which such President is inaugurated—

(A) the documentation under paragraph (1) includes whether—

(i) the individual of a requesting element who is making the request knows or believes that any United States person identity sought by the request is of an individual who is a member of the transition team of the President-elect and Vice-President-elect; or

(ii) based on the intelligence community report to which the request pertains, the originating element knows or reasonably believes that any United States person identity sought by the request is of an individual who is a member of the transition team of the President-elect and Vice-President-elect;

(B) the approval made pursuant to paragraph (2) of a covered request that contains a United States person identity described in subparagraph (A) is subject to the concurrence of the general counsel of the originating element (or, in the absence of the general counsel, the first assistant general counsel) that the dissemination of such identity information is in accordance with the procedures under subsection (a); and

(C) consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the head of the originating element notifies the chairmen and ranking minority members of the congressional intelligence committees of any approval described in subparagraph (B) by not later than 14 days after the date of such approval.

(c) ANNUAL REPORTS.—Not later than April 30 of each year, the head of each element of the intelligence community shall submit to

the congressional intelligence committees a report documenting, with respect to the year covered by the report—

(1) the total number of covered requests received by that element;

(2) of such total number, the number of requests approved;

(3) of such total number, the number of requests denied; and

(4) for each number calculated under paragraphs (1) through (3), the number listed by each requesting element.

(d) CERTAIN PROCEDURES REGARDING CONGRESSIONAL IDENTITY INFORMATION.—

(1) REQUIREMENTS.—With respect to the dissemination of congressional identity information, the head of each element of the intelligence community shall carry out this section in accordance with annex A of Intelligence Community Directive 112, or successor annex or directive.

(2) NOTIFICATION.—The Director of National Intelligence may not modify or supersede annex A of Intelligence Community Directive 112, or successor annex or directive, unless—

(A) the Director notifies the congressional intelligence committees of the proposed modifications or new annex or directive; and

(B) a period of 30 days elapses following such notification.

(e) EFFECT ON MINIMIZATION PROCEDURES.—The requirements of this section are in addition to any minimization procedures established pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), Executive Order No. 12333 (50 U.S.C. 3001 note), or successor order, or other relevant provision of law or executive order.

(f) DEFINITIONS.—In this section:

(1) The term "covered request" means a request by a requesting element to an originating element for nonpublic identifying information with respect to a known unconsenting United States person that was omitted from an intelligence community report disseminated by the originating element.

(2) The term "originating element" means an element of the intelligence community that disseminates an intelligence community report that contains a reference to a known unconsenting United States person but omits nonpublic identifying information with respect to such person.

(3) The term "requesting element" means an element of the United States Government that receives an intelligence community report from an originating element and makes a covered request with respect to such report.

(4) The term "United States person" has the meaning given the term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

* * * * * * *

TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

* * * * * * *

SEC. 1104. PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term "agency" means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, United States Code, that contains an intelligence community element, except the Federal Bureau of Investigation.

(2) COVERED INTELLIGENCE COMMUNITY ELEMENT.—The term "covered intelligence community element"—

(A) means—

(i) the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office; and

(ii) any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities; and

(B) does not include the Federal Bureau of Investigation.

(3) PERSONNEL ACTION.—The term "personnel action" means, with respect to an employee in a position in a covered intelligence community element (other than a position excepted from the competitive service due to its confidential, policy-determining, policymaking, or policy-advocating character) *or a contractor employee*—

(A) an appointment;

(B) a promotion;

(C) a disciplinary or corrective action;

(D) a detail, transfer, or reassignment;

(E) a demotion, suspension, or termination;

(F) a reinstatement or restoration;

(G) a performance evaluation;

(H) a decision concerning pay, benefits, or awards;

(I) a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation; or

(J) any other significant change in duties, responsibilities, or working conditions.

(4) CONTRACTOR EMPLOYEE.—The term "contractor employee" means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element.

(b) [IN GENERAL.—] *AGENCY EMPLOYEES.*—Any employee of an agency who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take a personnel action with respect to any employee of a covered intelligence community element as a reprisal for a lawful disclosure of information by the employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, the head of the employing agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the employing agency, a congressional intelligence committee, or a

member of a congressional intelligence committee, which the employee reasonably believes evidences—

(1) a violation of any Federal law, rule, or regulation; or

(2) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(c) CONTRACTOR EMPLOYEES.—(1) Any employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take a personnel action with respect to any contractor employee as a reprisal for a lawful disclosure of information by the contractor employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, the head of the contracting agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the contracting agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the contractor employee reasonably believes evidences—

(A) a violation of any Federal law, rule, or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or

(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(2) A personnel action under paragraph (1) is prohibited even if the action is undertaken at the request of an agency official, unless the request takes the form of a nondiscretionary directive and is within the authority of the agency official making the request.

[(c)**]** *(d)* ENFORCEMENT.—The President shall provide for the enforcement of this section.

[(d)**]** *(e)* EXISTING RIGHTS PRESERVED.—Nothing in this section shall be construed to—

(1) preempt or preclude any employee, *contractor employee,* or applicant for employment, at the Federal Bureau of Investigation from exercising rights provided under any other law, rule, or regulation, including section 2303 of title 5, United States Code; or

(2) repeal section 2303 of title 5, United States Code.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * * * *

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

* * * * * * *

Subtitle F—Privacy and Civil Liberties

SEC. 1061. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.

(a) IN GENERAL.—There is established as an independent agency within the executive branch a Privacy and Civil Liberties Oversight Board (referred to in this section as the "Board").

(b) FINDINGS.—Consistent with the report of the National Commission on Terrorist Attacks Upon the United States, Congress makes the following findings:

(1) In conducting the war on terrorism, the Government may need additional powers and may need to enhance the use of its existing powers.

(2) This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given.

(3) The National Commission on Terrorist Attacks Upon the United States correctly concluded that "The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.".

(c) PURPOSE.—The Board shall—

(1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and

(2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

(d) FUNCTIONS.—

(1) ADVICE AND COUNSEL ON POLICY DEVELOPMENT AND IMPLEMENTATION.—The Board shall—

(A) review proposed legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the development and adoption of information sharing guidelines under subsections (d) and (f) of section 1016;

(B) review the implementation of new and existing legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the implementation of information sharing guidelines under subsections (d) and (f) of section 1016;

(C) advise the President and the departments, agencies, and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of such legislation, regulations, policies, and guidelines; and

(D) in providing advice on proposals to retain or enhance a particular governmental power, consider whether the department, agency, or element of the executive branch has established—

(i) that the need for the power is balanced with the need to protect privacy and civil liberties;

(ii) that there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and

(iii) that there are adequate guidelines and oversight to properly confine its use.

(2) OVERSIGHT.—The Board shall continually review—

(A) the regulations, policies, and procedures, and the implementation of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected;

(B) the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they appropriately protect privacy and civil liberties and adhere to the information sharing guidelines issued or developed under subsections (d) and (f) of section 1016 and to other governing laws, regulations, and policies regarding privacy and civil liberties; and

(C) other actions by the executive branch relating to efforts to protect the Nation from terrorism to determine whether such actions—

(i) appropriately protect privacy and civil liberties; and

(ii) are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.

(3) RELATIONSHIP WITH PRIVACY AND CIVIL LIBERTIES OFFICERS.—The Board shall—

(A) receive and review reports and other information from privacy officers and civil liberties officers under section 1062;

(B) when appropriate, make recommendations to such privacy officers and civil liberties officers regarding their activities; and

(C) when appropriate, coordinate the activities of such privacy officers and civil liberties officers on relevant interagency matters.

(4) TESTIMONY.—The members of the Board shall appear and testify before Congress upon request.

(e) REPORTS.—

(1) IN GENERAL.—The Board shall—

(A) receive and review reports from privacy officers and civil liberties officers under section 1062; and

(B) periodically submit, not less than semiannually, reports—

(i)(I) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Oversight and Govern-

ment Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(II) to the President; and

(ii) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) CONTENTS.—Not less than 2 reports submitted each year under paragraph (1)(B) shall include—

(A) a description of the major activities of the Board during the preceding period;

(B) information on the findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);

(C) the minority views on any findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);

(D) each proposal reviewed by the Board under subsection (d)(1) that—

(i) the Board advised against implementation; and

(ii) notwithstanding such advice, actions were taken to implement; and

(E) for the preceding period, any requests submitted under subsection (g)(1)(D) for the issuance of subpoenas that were modified or denied by the Attorney General.

(f) INFORMING THE PUBLIC.—**[**The Board shall**]** *The Board—*

(1) **[**make its**]** *shall make its* reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and

(2) **[**hold public**]** *shall hold public* hearings and otherwise inform the public of its activities, as appropriate and in a manner consistent with the protection of classified information and applicable law*, but may, notwithstanding section 552b of title 5, United States Code, meet or otherwise communicate in any number to confer or deliberate in a manner that is closed to the public*.

(g) ACCESS TO INFORMATION.—

(1) AUTHORIZATION.—If determined by the Board to be necessary to carry out its responsibilities under this section, the Board is authorized to—

(A) have access from any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element, to all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law;

(B) interview, take statements from, or take public testimony from personnel of any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element;

(C) request information or assistance from any State, tribal, or local government; and

(D) at the direction of a majority of the members of the Board, submit a written request to the Attorney General of the United States that the Attorney General require, by subpoena, persons (other than departments, agencies, and elements of the executive branch) to produce any relevant information, documents, reports, answers, records, accounts, papers, and other documentary or testimonial evidence.

(2) REVIEW OF SUBPOENA REQUEST.—

(A) IN GENERAL.—Not later than 30 days after the date of receipt of a request by the Board under paragraph (1)(D), the Attorney General shall—

(i) issue the subpoena as requested; or

(ii) provide the Board, in writing, with an explanation of the grounds on which the subpoena request has been modified or denied.

(B) NOTIFICATION.—If a subpoena request is modified or denied under subparagraph (A)(ii), the Attorney General shall, not later than 30 days after the date of that modification or denial, notify the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(3) ENFORCEMENT OF SUBPOENA.—In the case of contumacy or failure to obey a subpoena issued pursuant to paragraph (1)(D), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found may issue an order requiring such person to produce the evidence required by such subpoena.

(4) AGENCY COOPERATION.—Whenever information or assistance requested under subparagraph (A) or (B) of paragraph (1) is, in the judgment of the Board, unreasonably refused or not provided, the Board shall report the circumstances to the head of the department, agency, or element concerned without delay. The head of the department, agency, or element concerned shall ensure that the Board is given access to the information, assistance, material, or personnel the Board determines to be necessary to carry out its functions.

(5) ACCESS.—Nothing in this section shall be construed to authorize the Board, or any agent thereof, to gain access to information regarding an activity covered by section 503(a) of the National Security Act of 1947 (50 U.S.C. 3093(a)).

(h) MEMBERSHIP.—

(1) MEMBERS.—The Board shall be composed of a full-time chairman and 4 additional members, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—Members of the Board shall be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation, but in no event shall more than 3 members of the Board be members of the same political party. The President shall, before appointing an individual who is not a member of the same political party as the President, consult with the leader-

ship of that party, if any, in the Senate and House of Representatives.

(3) INCOMPATIBLE OFFICE.—An individual appointed to the Board may not, while serving on the Board, be an elected official, officer, or employee of the Federal Government, other than in the capacity as a member of the Board.

(4) TERM.—Each member of the Board shall serve a term of 6 years, except that—

(A) a member appointed to a term of office after the commencement of such term may serve under such appointment only for the remainder of such term; and

(B) upon the expiration of the term of office of a member, the member shall continue to serve until the member's successor has been appointed and qualified, except that no member may serve under this subparagraph—

(i) for more than 60 days when Congress is in session unless a nomination to fill the vacancy shall have been submitted to the Senate; or

(ii) after the adjournment sine die of the session of the Senate in which such nomination is submitted.

(5) QUORUM AND MEETINGS.—The Board shall meet upon the call of the chairman or a majority of its members. Three members of the Board shall constitute a quorum.

(i) COMPENSATION AND TRAVEL EXPENSES.—

(1) COMPENSATION.—

(A) CHAIRMAN.—The chairman of the Board shall be compensated at the rate of pay payable for a position at level III of the Executive Schedule under section 5314 of title 5, United States Code.

(B) MEMBERS.—Each member of the Board shall be compensated at a rate of pay payable for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Board.

(2) TRAVEL EXPENSES.—Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for persons employed intermittently by the Government under section 5703(b) of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Board.

(j) STAFF.—

(1) APPOINTMENT AND COMPENSATION.—The chairman of the Board, in accordance with rules agreed upon by the Board, shall appoint and fix the compensation of a full-time executive director and such other personnel as may be necessary to enable the Board to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) APPOINTMENT IN ABSENCE OF CHAIRMAN.—If the position of chairman of the Board is vacant, during the period of the vacancy, the Board, at the direction of the unanimous vote of the serving members of the Board, may exercise the authority of the chairman under paragraph (1).

[(2)**]** *(3)* DETAILEES.—Any Federal employee may be detailed to the Board without reimbursement from the Board, and such detailee shall retain the rights, status, and privileges of the detailee's regular employment without interruption.

[(3)**]** *(4)* CONSULTANT SERVICES.—The Board may procure the temporary or intermittent services of experts and consultants in accordance with section 3109 of title 5, United States Code, at rates that do not exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of such title.

(k) SECURITY CLEARANCES.—

(1) IN GENERAL.—The appropriate departments, agencies, and elements of the executive branch shall cooperate with the Board to expeditiously provide the Board members and staff with appropriate security clearances to the extent possible under existing procedures and requirements.

(2) RULES AND PROCEDURES.—After consultation with the Secretary of Defense, the Attorney General, and the Director of National Intelligence, the Board shall adopt rules and procedures of the Board for physical, communications, computer, document, personnel, and other security relating to carrying out the functions of the Board.

(l) TREATMENT AS AGENCY, NOT AS ADVISORY COMMITTEE.—The Board—

(1) is an agency (as defined in section 551(1) of title 5, United States Code); and

(2) is not an advisory committee (as defined in section 3(2) of the Federal Advisory Committee Act (5 U.S.C. App.)).

(m) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section amounts as follows:

(1) For fiscal year 2008, $5,000,000.

(2) For fiscal year 2009, $6,650,000.

(3) For fiscal year 2010, $8,300,000.

(4) For fiscal year 2011, $10,000,000.

(5) For fiscal year 2012 and each subsequent fiscal year, such sums as may be necessary.

SEC. 1062. PRIVACY AND CIVIL LIBERTIES OFFICERS.

(a) DESIGNATION AND FUNCTIONS.—The Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency*, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation*, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board under section 1061 to be appropriate for coverage under this section shall designate not less than 1 senior officer to serve as the principal advisor to—

(1) assist the head of such department, agency, or element and other officials of such department, agency, or element in

appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;

(2) periodically investigate and review department, agency, or element actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department, agency, or element is adequately considering privacy and civil liberties in its actions;

(3) ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties; and

(4) in providing advice on proposals to retain or enhance a particular governmental power the officer shall consider whether such department, agency, or element has established—

(A) that the need for the power is balanced with the need to protect privacy and civil liberties;

(B) that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and

(C) that there are adequate guidelines and oversight to properly confine its use.

(b) EXCEPTION TO DESIGNATION AUTHORITY.—

(1) PRIVACY OFFICERS.—In any department, agency, or element referred to in subsection (a) or designated by the Privacy and Civil Liberties Oversight Board, which has a statutorily created privacy officer, such officer shall perform the functions specified in subsection (a) with respect to privacy.

(2) CIVIL LIBERTIES OFFICERS.—In any department, agency, or element referred to in subsection (a) or designated by the Board, which has a statutorily created civil liberties officer, such officer shall perform the functions specified in subsection (a) with respect to civil liberties.

(c) SUPERVISION AND COORDINATION.—Each privacy officer or civil liberties officer described in subsection (a) or (b) shall—

(1) report directly to the head of the department, agency, or element concerned; and

(2) coordinate their activities with the Inspector General of such department, agency, or element to avoid duplication of effort.

(d) AGENCY COOPERATION.—The head of each department, agency, or element shall ensure that each privacy officer and civil liberties officer—

(1) has the information, material, and resources necessary to fulfill the functions of such officer;

(2) is advised of proposed policy changes;

(3) is consulted by decision makers; and

(4) is given access to material and personnel the officer determines to be necessary to carry out the functions of such officer.

(e) REPRISAL FOR MAKING COMPLAINT.—No action constituting a reprisal, or threat of reprisal, for making a complaint or for dis-

closing information to a privacy officer or civil liberties officer described in subsection (a) or (b), or to the Privacy and Civil Liberties Oversight Board, that indicates a possible violation of privacy protections or civil liberties in the administration of the programs and operations of the Federal Government relating to efforts to protect the Nation from terrorism shall be taken by any Federal employee in a position to take such action, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(f) PERIODIC REPORTS.—

(1) IN GENERAL.—The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

(g) INFORMING THE PUBLIC.—Each privacy officer and civil liberties officer shall—

(1) make the reports of such officer, including reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and

(2) otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law.

(h) SAVINGS CLAUSE.—Nothing in this section shall be construed to limit or otherwise supplant any other authorities or responsibilities provided by law to privacy officers or civil liberties officers.

* * * * * * *

TITLE III—SECURITY CLEARANCES

SEC. 3001. SECURITY CLEARANCES.

(a) DEFINITIONS.—In this section:

(1) The term "agency" means—

(A) an executive agency (as that term is defined in section 105 of title 5, United States Code);

(B) a military department (as that term is defined in section 102 of title 5, United States Code); and

(C) an element of the intelligence community.

(2) The term "authorized investigative agency" means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term "authorized adjudicative agency" means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term "highly sensitive program" means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)); or

(ii) other information commonly referred to as "sensitive compartmented information".

(5) The term "current investigation file" means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term "personnel security investigation" means any investigation required for the purpose of determining the eligi-

bility of any military, civilian, or government contractor personnel to access classified information.

(7) The term "periodic reinvestigations" means investigations conducted for the purpose of updating a previously completed background investigation—

(A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;

(B) every 10 years in the case of a secret clearance; or

(C) every 15 years in the case of a Confidential Clearance.

(8) The term "appropriate committees of Congress" means—

(A) the Permanent Select Committee on Intelligence and the Committees on Armed Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.

(9) ACCESS DETERMINATION.—The term "access determination" means the determination regarding whether an employee—

(A) is eligible for access to classified information in accordance with Executive Order 12968 (60 Fed. Reg. 40245; relating to access to classified information), or any successor thereto, and Executive Order 10865 (25 Fed. Reg. 1583; relating to safeguarding classified information with industry), or any successor thereto; and

(B) possesses a need to know under such an Order.

(b) SELECTION OF ENTITY.—Except as otherwise provided, not later than 90 days after the date of the enactment of this Act, the President shall select a single department, agency, or element of the executive branch to be responsible for—

(1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

(2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;

(3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;

(4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);

(5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals;

(6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances; and

(7) not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2014, and consistent with subsection (j)—

(A) developing policies and procedures that permit, to the extent practicable, individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee's access to classified information and to retain their government employment status while such challenge is pending; and

(B) developing and implementing uniform and consistent policies and procedures to ensure proper protections during the process for denying, suspending, or revoking a security clearance or access to classified information following a protected disclosure, including the ability to appeal such a denial, suspension, or revocation, except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts no longer than 1 year or the head of the agency or a designee of the head of the agency certifies that a longer suspension is needed before a final decision on denial or revocation to prevent imminent harm to the national security.

(c) PERFORMANCE OF SECURITY CLEARANCE INVESTIGATIONS.—(1) Notwithstanding any other provision of law, not later than 180 days after the date of the enactment of this Act, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investigations if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before the date of the enactment of this Act;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) RECIPROCITY OF SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) DATABASE ON SECURITY CLEARANCES.—(1) Not later than 12 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting informa-

tion to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) EVALUATION OF USE OF AVAILABLE TECHNOLOGY IN CLEARANCE INVESTIGATIONS AND ADJUDICATIONS.—(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after the date of the enactment of this Act, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(g) REDUCTION IN LENGTH OF PERSONNEL SECURITY CLEARANCE PROCESS.—(1) The head of the entity selected pursuant to subsection (b) shall, within 90 days of selection under that subsection, develop, in consultation with the appropriate committees of Congress and each authorized adjudicative agency, a plan to reduce the length of the personnel security clearance process.

(2)(A) To the extent practical the plan under paragraph (1) shall require that each authorized adjudicative agency make a determination on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application for a security clearance by an

authorized investigative agency. Such 60-day average period shall include—

(i) a period of not longer than 40 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 20 days to complete the adjudicative phase of the clearance review.

(B) Determinations on clearances not made within 60 days shall be made without delay.

(3)(A) The plan under paragraph (1) shall take effect 5 years after the date of the enactment of this Act.

(B) During the period beginning on a date not later than 2 years after the date after the enactment of this Act and ending on the date on which the plan under paragraph (1) takes effect, each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance pursuant to this section within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-day average period shall include—

(i) a period of not longer than 90 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 30 days to complete the adjudicative phase of the clearance review.

(h) REPORTS.—(1) Not later than February 15, 2006, and annually thereafter through 2011, the head of the entity selected pursuant to subsection (b) shall submit to the appropriate committees of Congress a report on the progress made during the preceding year toward meeting the requirements of this section.

(2) Each report shall include, for the period covered by such report—

(A) the periods of time required by the authorized investigative agencies and authorized adjudicative agencies for conducting investigations, adjudicating cases, and granting clearances, from date of submission to ultimate disposition and notification to the subject and the subject's employer;

(B) a discussion of any impediments to the smooth and timely functioning of the requirements of this section; and

(C) such other information or recommendations as the head of the entity selected pursuant to subsection (b) considers appropriate.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).

(j) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) IN GENERAL.—Agency personnel with authority over personnel security clearance or access determinations shall not take or fail to take, or threaten to take or fail to take, any action with respect to any employee's security clearance or access determination in retaliation for—

(A) any lawful disclosure of information to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose) or the head of the employing agency (or employee designated by

the head of that agency for such purpose) by an employee that the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(B) any lawful disclosure to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(C) any lawful disclosure that complies with—

(i) subsections (a)(1), (d), and (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)); and

(D) if the actions do not result in the employee or applicant unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(2) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in paragraph (1) shall be construed to authorize the withholding of information from Congress or the taking of any personnel action against an employee who lawfully discloses information to Congress.

(3) DISCLOSURES.—

(A) IN GENERAL.—A disclosure shall not be excluded from paragraph (1) because—

(i) the disclosure was made to a person, including a supervisor, who participated in an activity that the employee reasonably believed to be covered by paragraph (1)(A)(ii);

(ii) the disclosure revealed information that had been previously disclosed;

(iii) the disclosure was not made in writing;

(iv) the disclosure was made while the employee was off duty; or

(v) of the amount of time which has passed since the occurrence of the events described in the disclosure.

(B) REPRISALS.—If a disclosure is made during the normal course of duties of an employee, the disclosure shall not be excluded from paragraph (1) if any employee who has authority to take, direct others to take, recommend, or approve any personnel action with respect to the employee making the disclosure, took, failed to take, or threatened to take or fail to take a personnel action with respect to that employee in reprisal for the disclosure.

(4) AGENCY ADJUDICATION.—

(A) REMEDIAL PROCEDURE.—An employee or former employee who believes that he or she has been subjected to a reprisal prohibited by paragraph (1) may, within 90 days after the issuance of notice of such decision, appeal that decision within the agency of that employee or former employee through proceedings authorized by subsection (b)(7), except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts not longer than 1 year (or a longer period in accordance with a certification made under subsection (b)(7)).

(B) CORRECTIVE ACTION.—If, in the course of proceedings authorized under subparagraph (A), it is determined that the adverse security clearance or access determination violated paragraph (1), the agency shall take specific corrective action to return the employee or former employee, as nearly as practicable and reasonable, to the position such employee or former employee would have held had the violation not occurred. Such corrective action may include back pay and related benefits, travel expenses, and compensatory damages not to exceed $300,000.

(C) CONTRIBUTING FACTOR.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual, unless the agency demonstrates by a preponderance of the evidence that it would have taken the same action in the absence of such disclosure, giving the utmost deference to the agency's assessment of the particular threat to the national security interests of the United States in the instant matter.

(5) APPELLATE REVIEW OF SECURITY CLEARANCE ACCESS DETERMINATIONS BY DIRECTOR OF NATIONAL INTELLIGENCE.—

(A) APPEAL.—Within 60 days after receiving notice of an adverse final agency determination under a proceeding under paragraph (4), an employee or former employee may appeal that determination in accordance with the procedures established under subparagraph (B).

(B) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Attorney Gen-

eral and the Secretary of Defense, shall develop and implement policies and procedures for adjudicating the appeals authorized by subparagraph (A).

(C) CONGRESSIONAL NOTIFICATION.—Consistent with the protection of sources and methods, at the time the Director of National Intelligence issues an order regarding an appeal pursuant to the policies and procedures established by this paragraph, the Director of National Intelligence shall notify the congressional intelligence committees.

(6) JUDICIAL REVIEW.—Nothing in this section shall be construed to permit or require judicial review of any—

(A) agency action under this section; or

(B) action of the appellate review procedures established under paragraph (5).

(7) PRIVATE CAUSE OF ACTION.—Nothing in this section shall be construed to permit, authorize, or require a private cause of action to challenge the merits of a security clearance determination.

(8) INCLUSION OF CONTRACTOR EMPLOYEES.—In this subsection, the term "employee" includes an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of an agency. With respect to such employees, the term "employing agency" shall be deemed to be the contracting agency.

* * * * * * *

FISA AMENDMENTS ACT OF 2008

* * * * * * *

TITLE IV—OTHER PROVISIONS

* * * * * * *

SEC. 403. REPEALS.

(a) REPEAL OF PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) AMENDMENTS TO FISA.—

(A) IN GENERAL.—Except as provided in section 404, sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(B) TECHNICAL AND CONFORMING AMENDMENTS.—

(i) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C.

(ii) CONFORMING AMENDMENTS.—Except as provided in section 404, section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(I) in paragraph (1), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)"; and

(II) in paragraph (2), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)".

(2) REPORTING REQUIREMENTS.—Except as provided in section 404, section 4 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 555) is repealed.

(3) TRANSITION PROCEDURES.—Except as provided in section 404, subsection (b) of section 6 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556) is repealed.

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective [December 31, 2017] *December 31, 2021*, title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) *and by the FISA Amendments Reauthorization Act of 2017*, is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective [December 31, 2017] *December 31, 2021*—

(A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;

(B) except as provided in section 404, section 601(a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and

(C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978".

SEC. 404. TRANSITION PROCEDURES.

(a) TRANSITION PROCEDURES FOR PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

(i) the expiration of such order, authorization, or directive; or

(ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) PROTECTION FROM LIABILITY.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

(A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;

(iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and

(iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(i)(3) of such Act (as so added) at which time the provisions of that section and of section 702(i)(4) of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON [DECEMBER 31, 2017] *DECEMBER 31, 2021*.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) *and by the FISA Amendments Reauthorization Act of 2017*, shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act, as amended by section 101(a) *and by the FISA Amendments Reau-*

thorization Act of 2017, shall continue to apply until the later of—

(A) the expiration of such order, authorization, or directive; or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act, as added by section 101(a);

(B) section 702(h)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act (as so added);

(C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), and sections 702(l) and 707 of such Act, as added by section 101(a) *and amended by the FISA Amendments Reauthorization Act of 2017*, shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a) *and by the FISA Amendments Reauthorization Act of 2017*, after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under sec-

tion 601 of such Act, as amended by section 101(c), or section 702(l) or 707 of such Act, as added by section 101(a) *and amended by the FISA Amendments Reauthorization Act of 2017*, relating to any acquisition conducted under title VII of such Act, as amended by section 101(a) *and by the FISA Amendments Reauthorization Act of 2017*, has been included in a review, assessment, or report under such section 601, 702(l), or 707.

(5) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 93—PUBLIC OFFICERS AND EMPLOYEES

* * * * * * *

§ 1924. Unauthorized removal and retention of classified documents or material

(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than **[**one year**]** *five years*, or both.

(b) For purposes of this section, the provision of documents and materials to the Congress shall not constitute an offense under subsection (a).

(c) In this section, the term "classified information of the United States" means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.

* * * * * * *

DISCLOSURE OF DIRECTED RULE MAKING

H.R. 4478 does not specifically direct any rule makings within the meaning of 5 U.S.C. 551.

DUPLICATION OF FEDERAL PROGRAMS

H.R. 4478 does not duplicate or reauthorize an established program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report form 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.

MINORITY VIEWS

Section 702 of the Foreign Intelligence Surveillance Act is a critical Intelligence Community (IC) tool. We will continue to work to reauthorize and reform this authority in a way which will enhance privacy and transparency, while maintaining operational effectiveness.

We regret the Majority's inclusion, in must-pass legislation to reauthorize Section 702, an unnecessary and politicized provision which purports to address deficiencies in the process for "unmasking" U.S. person identity information contained in intelligence reports.

Of greatest concern is the creation of special review and congressional notification procedures for requests made to the IC during a presidential transition. These would be triggered when the sought information, if "unmasked," might identify personnel of a presidential or vice presidential transition team.

This language is intended to bolster the false claim that, during the 2016 presidential transition and before, officials of the last Administration surveilled Trump Tower, and sought identifying information contained in intelligence reports for improper or even illegal purposes, including to leak classified information to journalists.

The Committee has seen no evidence, heard no testimony, and has no grounds for believing that senior officials of the Obama Administration—or any Administration—abused the identity request process. And, although the topics of Section 702 and "unmasking" frequently have been conflated, the Committee also has seen no evidence that U.S. person identity information incidentally collected pursuant to Section 702 has been improperly "unmasked." The Chairman's own inquiry has yielded no evidence that IC professionals who adjudicate identity requests acted inappropriately.

Nonetheless, the IC is taking action to further heighten privacy protection. On the day before Committee markup of the Section 702 reauthorization, the Director of National Intelligence pledged to strengthen existing procedures governing identity requests—including with regard to presidential transitions—and to seek greater harmonization of those procedures across the IC. Given this commitment, there is simply no policy reason to insist on including the presidential transition language in Section 702's reauthorization.

During markup, Minority Members expressed different views about the sorts of additional privacy safeguards that Congress ought to establish as a condition for Section 702's reauthorization. We each believe, however, that legislation so vital to national security cannot include language obviously meant to further a partisan agenda.

In the short time that remains before Section 702's expiration at the end of this month, we will work to remove the offending "unmasking" language, and to add privacy and transparency safeguards without diminishing Section 702's proven capability to protect national security.

ADAM B. SCHIFF.
JAMES A. HIMES.
TERRI A. SEWELL.
ANDRÉ CARSON.
JACKIE SPEIER.
MIKE QUIGLEY.
ERIC SWALWELL.
JOAQUIN CASTRO.

ADDITIONAL VIEWS

Section 702 of the Foreign Intelligence Surveillance Act is an important national security tool, but a balance that must be struck between security and civil liberties. The last time we reviewed and debated these surveillance authorities in 2012, I voted against reauthorization of 702 authorities because of concerns over Americans' most fundamental civil rights.

Since that time, significant numbers of Americans have been improperly swept up in surveillance activities that the law says must not target Americans. This improperly obtained information is retained for years. It has been used in court against Americans charged with crimes that have nothing to do with national security, with no warrants and without the required notifications to the defense. The government selectively publicizes what it calls Section 702 successes, but has defied Congress by refusing share information on how many Americans are impacted by Section 702 failures. The checks and balances built into the system are insufficient: a rotating cast of federal oversight judges are expected to grapple with the highly technical aspects of electronic surveillance, outmatched by an army of expert government lawyers.

Unfortunately, this bill fails to allay my concerns. Specifically, it omits two measures I advocated for during drafting: the appointment of a permanent, expert "special master" to advise the Foreign Intelligence Surveillance Court on technical matters; and, an independent assessment by the Comptroller General of the United States of the government's claims to the efficacy of Section 702 authorities.

My concerns are shared widely on both sides of the aisle, and civil liberties groups have assessed that the so-called fixes in this bill would be worse than no fixes at all. We must instead work together to address these problems. This is far too serious of a matter to ram through a renewal of these authorities with limited debate, particularly given the profound implications for all Americans and for American businesses operating overseas.

I serve in Congress because I love this country, and I am driven to protect it both from external national security threats and from internal weakening of our Constitutional protections. This bill fails to balance those concerns, and so I must oppose it.

JACKIE SPEIER.

ADDITIONAL VIEWS

Like Section 702 of the Foreign Intelligence Surveillance Act (FISA) itself, H.R. 4478, the FISA Amendments Reauthorization Act of 2017, is designed to ensure security. It seeks to accomplish that goal, in my view, at too great a cost to privacy. The tradeoff embodied in this bill is not the only, or even the best, option available. With a little more work, deliberation and debate, we could reform the Section 702 program—which is necessary for security—in a fashion that would more effectively safeguard privacy.

The Committee has not sufficiently considered the serious legal and policy concerns associated with "about collection" by the NSA, pursuant to Section 702. That form of surveillance has been troubled by compliance difficulties and inadvertent collection, and drawn criticism from the Foreign Intelligence Surveillance Court. Compounding the problem, "about collection" was not explicitly authorized by the original text of Section 702 itself. Although the practice has been discontinued by NSA, issues implicated by it remain very real and have not been addressed. I am thus uncomfortable with provisions of H.R. 4478—which contemplate the resumption of "about collection" in the future. The issue deserves fuller discussion here in Congress, before we sign off.

Furthermore, H.R. 4478 does not adequately address law enforcement's practice of querying the Section 702 database, through use of an American's identifying information, without first obtaining judicial approval. Although courts have approved such queries, they nevertheless are, in my view, inconsistent with values we hold dear in the United States. Though H.R. 4478 contains reforms intended to address law enforcement uses of Section 702 data, these may not protect Americans' privacy interests in an adequate way.

Finally, H.R. 4478 newly authorizes surveillance, under provisions of FISA other than Section 702, of persons engaged in international malicious cyber activities against the United States. The bill's definition of "malicious cyber activities" appears to conflict with other legal and policy definitions of the term. That inconsistency could cause confusion and conflicts, both at home and abroad. Additionally, the new language obviously expands the scope of permitted surveillance under FISA; I have not yet been furnished with adequate information to conclude that such an expansion is necessary.

For these reasons, I oppose this bill.

DENNY HECK.

○