To amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. ROCKEFELLER from the Select Committee on Intelligence reported the following original bill; which was read twice and placed on the calendar

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,

3 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

4 (a) Short Title.—This Act may be cited as the
5 “Foreign Intelligence Surveillance Act of 1978 Amend-
6 ments Act of 2007” or the “FISA Amendments Act of
7 2007”.


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

Sec. 1. Short title; table of contents.

**TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE**

Sec. 101. Targeting the communications of certain persons outside the United States.

Sec. 102. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted.

Sec. 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978.

Sec. 104. Applications for court orders.

Sec. 105. Issuance of an order.

Sec. 106. Use of information.

Sec. 107. Amendments for physical searches.

Sec. 108. Amendments for emergency pen registers and trap and trace devices.

Sec. 109. Foreign Intelligence Surveillance Court.

Sec. 110. Technical and conforming amendments.

**TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS**

Sec. 201. Definitions.

Sec. 202. Limitations on civil actions for electronic communication service providers.

Sec. 203. Procedures for implementing statutory defenses under the Foreign Intelligence Surveillance Act of 1978.

Sec. 204. Preemption of State investigations.

Sec. 205. Technical amendments.

**TITLE III—OTHER PROVISIONS**

Sec. 301. Severability.

Sec. 302. Effective date; repeal; transition procedures.

**TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE**

**SEC. 101. TARGETING THE COMMUNICATIONS OF CERTAIN PERSONS OUTSIDE THE UNITED STATES.**

(a) **IN GENERAL.**—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by striking title VII; and

(2) by adding after title VI the following new title:
“TITLE VII—ADDITIONAL PROCEDURES FOR TARGETING COMMUNICATIONS OF CERTAIN PERSONS OUTSIDE THE UNITED STATES

“SEC. 701. LIMITATION ON DEFINITION OF ELECTRONIC SURVEILLANCE.

“Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States.

“SEC. 702. DEFINITIONS.


“(b) Additional Definitions.—

“(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 es-
established by 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 by
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 communications
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) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term ‘element of the intelligence community’ means an element of the intelligence community specified in or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

“SEC. 703. PROCEDURES FOR ACQUIRING THE COMMUNICATIONS OF CERTAIN PERSONS OUTSIDE THE UNITED STATES.

“(a) AUTHORIZATION.—Notwithstanding any other law, the Attorney General and the Director of National Intelligence may authorize jointly, for periods of up to 1 year, 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 outside the United States if the purpose of such acquisition is to target for surveillance a particular, known person reasonably believed to be in the United States, except in accordance with title I; and

“(3) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

“(c) United States Persons Located Outside the United States.—

“(1) Acquisition inside the United States of United States Persons Outside the United States.—An acquisition authorized by subsection (a) that occurs inside the United States may not target a United States person except in accordance with the provisions of title I.

“(2) Acquisition outside the United States of United States Persons Outside the United States.—An acquisition by an electronic, mechanical, or other surveillance device outside the United States may not intentionally target a United
States person reasonably believed to be outside the United States to acquire the contents of a wire or radio communication sent by or intended to be received by 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 if the technique were used inside the United States unless—

“(A) the Attorney General or the Attorney General’s designee submits an application to the Foreign Intelligence Surveillance Court that includes a statement of the facts and circumstances relied upon by the applicant to justify the Attorney General’s belief that the target of the acquisition is a foreign power or an agent of a foreign power; and

“(B) the Foreign Intelligence Surveillance Court—

“(i) finds on the basis of the facts submitted by the applicant there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
“(ii) issues an ex parte order as requested or as modified approving the targeting of that United States person.

“(3) PROCEDURES.—

“(A) SUBMITTAL TO FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Not later than 30 days after the date of the enactment of this title, the Attorney General shall submit to the Foreign Intelligence Surveillance Court the procedures to be utilized in determining whether a target reasonably believed to be outside the United States is a United States person.

“(B) APPROVAL BY FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The procedures submitted under subparagraph (A) shall be utilized as described in that subparagraph only upon the approval of the Foreign Intelligence Surveillance Court.

“(C) UTILIZATION IN TARGETING.—Any targeting of persons authorized by subsection (a) shall utilize the procedures submitted under subparagraph (A) as approved by the Foreign Intelligence Surveillance Court under subparagraph (B).
“(d) CONDUCT OF ACQUISITION.—An acquisition authorized under subsection (a) may be conducted only in accordance with—

“(1) a certification made by the Attorney General and the Director of National Intelligence pursuant to subsection (g); and

“(2) the targeting and minimization procedures required pursuant to subsections (e) and (f).

“(e) 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 ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States.

“(2) JUDICIAL REVIEW.—The procedures referred to in paragraph (1) shall be subject to judicial review pursuant to subsection (i).

“(f) MINIMIZATION PROCEDURES.—

“(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt, consistent with the requirements of section 101(h), minimization proce-
dures for acquisitions authorized under subsection (a).

“(2) JUDICIAL REVIEW.—The minimization procedures required by this subsection shall be subject to judicial review pursuant to subsection (i).

“(g) CERTIFICATION.—

“(1) IN GENERAL.—

“(A) REQUIREMENT.—Subject to subparagraph (B), prior to the initiation of an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence shall provide, under oath, a written certification, as described in this subsection.

“(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence determine that immediate action by the Government is required and time does not permit the preparation of a certification under this subsection prior to the initiation of an acquisition, the Attorney General and the Director of National Intelligence shall prepare such certification, including such determination, as soon as possible but in no event more than 168 hours after such determination is made.
“(2) REQUIREMENTS.—A certification made under this subsection shall—

“(A) attest that—

“(i) there are reasonable procedures in place for determining that the acquisition authorized under subsection (a) is targeted at persons reasonably believed to be located outside the United States and that such procedures have been approved by, or will promptly be submitted for approval by, the Foreign Intelligence Surveillance Court pursuant to subsection (i);

“(ii) the procedures referred to in clause (i) are consistent with the requirements of the fourth amendment to the Constitution of the United States and do not permit the intentional targeting of any person who is known at the time of acquisition to be located in the United States;

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

“(iv) the minimization procedures to be used with respect to such acquisition—
“(I) meet the definition of minimization procedures under section 101(h); and

“(II) have been approved by, or will promptly be submitted for approval by, the Foreign Intelligence Surveillance Court pursuant to subsection (i);

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

“(vi) the acquisition does not constitute electronic surveillance, as limited by section 701; and

“(B) 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 consent of the Senate; or

“(ii) the head of any element of the intelligence community.

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

“(4) Submission to the Court.—The Attorney General shall transmit a copy of a certification made under this subsection, and any supporting affidavit, under seal to the Foreign Intelligence Surveillance Court as soon as possible, but in no event more than 5 days after such certification is made. Such certification shall be maintained under security measures adopted by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence.

“(5) Review.—The certification required by this subsection shall be subject to judicial review pursuant to subsection (i).

“(h) 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 ac-
quisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target; 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 pursuant to paragraph (1).

“(3) RELEASE FROM LIABILITY.—Notwithstanding any other law, 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 challenge the directive by filing a petition with the Foreign Intelligence Surveillance Court.

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

“(C) STANDARDS FOR REVIEW.—A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that the directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply with the directive. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

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

“(5) ENFORCEMENT OF DIRECTIVES.—
“(A) ORDER TO COMPEL.—In the case of a failure to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel compliance with the directive with the Foreign Intelligence Surveillance Court.

“(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 by section 103(e)(1) not later than 24 hours after the filing of the petition.

“(C) STANDARDS FOR REVIEW.—A judge considering a petition shall issue an order requiring the electronic communication service provider to comply with the directive if the judge finds that the directive was issued in accordance with paragraph (1), 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 of the Court 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 the decision issued pursuant to paragraph (4) or (5) not later than 7 days after the issuance of such decision. The Court of Review shall have jurisdiction to consider such a petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

“(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 the decision of the Court of Review issued under
subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(i) JUDICIAL REVIEW.—

“(1) IN GENERAL.—

“(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review any certification required by subsection (d) or targeting and minimization procedures adopted pursuant to subsections (e) and (f).

“(B) SUBMISSION TO THE COURT.—The Attorney General shall submit to the Court any such certification or procedure, or amendment thereto, not later than 5 days after making or amending the certification or adopting or amending the procedures.

“(2) CERTIFICATIONS.—The Court shall review a certification provided under subsection (g) to determine whether the certification contains all the required elements.

“(3) TARGETING PROCEDURES.—The Court shall review the targeting procedures required by
subsection (e) to assess whether the procedures are reasonably designed to ensure that the acquisition authorized under subsection (a) is limited to the targeting of persons reasonably believed to be located outside the United States.

"(4) MINIMIZATION PROCEDURES.—The Court shall review the minimization procedures required by subsection (f) to assess whether such procedures meet the definition of minimization procedures under section 101(h).

"(5) ORDERS.—

“(A) APPROVAL.—If the Court finds that a certification required by subsection (g) contains all of the required elements and that the targeting and minimization procedures required by subsections (e) and (f) 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 continued use of the procedures for the acquisition authorized under subsection (a).

“(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification required by subsection (g) does not contain all of the re-
required elements, or that the procedures required by subsections (e) and (f) 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 the Court issues the order; or

“(ii) cease the acquisition authorized under subsection (a).

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

“(6) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government may appeal any order under this section to the Foreign Intelligence Surveillance Court of Review, which shall have jurisdiction to review such order. For any deci-
sion 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 its reasons.

“(B) CONTINUATION OF ACQUISITION
PENDING REHEARING OR APPEAL.—Any acqui-
sitions affected by an order under paragraph
(5)(B) may continue—

“(i) during the pending of any rehear-
ing of the order by the Court en banc; and

“(ii) during the pendency of any ap-
peal of the order to the Foreign Intel-
ligence Surveillance Court of Review.

“(C) 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 subpara-
graph (A). The record for such review shall be
transmitted under seal to the Supreme Court of
the United States, which shall have jurisdiction
to review such decision.

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

“(k) MAINTENANCE OF RECORDS.—
“(1) **STANDARDS.**—A record of a proceeding under this section, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained 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.**—A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.

“(1) **OVERSIGHT.**—

“(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 minimiza-
tion procedures required by subsections (e) and (f) and shall submit each such assessment to—

“(A) the Foreign Intelligence Surveillance Court; and

“(B) the congressional intelligence committees.

“(2) AGENCY ASSESSMENT.—The Inspectors General of the Department of Justice and of any element of the intelligence community authorized to acquire foreign intelligence information under subsection (a)—

“(A) are authorized to review the compliance of their agency or element with the targeting and minimization procedures required by subsections (e) and (f);

“(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States person identity and the number of United States person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;
“(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and the number of persons located in the United States whose communications were reviewed; and

“(D) shall provide each such review to—

“(i) the Attorney General;

“(ii) the Director of National Intelligence; and

“(iii) the congressional intelligence committees.

“(3) ANNUAL REVIEW.—

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

“(i) an accounting of the number of disseminated intelligence reports con-
taining 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; and

“(iii) the number of targets that were later determined to be located in the United States and the number of persons located in the United States whose communications were reviewed.

“(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 or the application of the minimization procedures to a particular acquisition authorized under subsection (a).

“(C) PROVISION OF REVIEW TO FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The head of each element of the intelligence community that conducts an annual review under sub-
paragraph (A) shall provide such review to the
Foreign Intelligence Surveillance Court.

“(4) Reports to congress.—

“(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, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning the implementation of this Act.

“(B) Content.—Each report made under subparagraph (A) shall include—

“(i) any certifications made under subsection (g) during the reporting period;

“(ii) any directives issued under subsection (h) during the reporting period;

“(iii) the judicial review during the reporting period of any such certifications and targeting and minimization procedures utilized with respect to such acquisition, including a copy of any order or pleading in connection with such review that contains a significant legal interpretation of the provisions of this Act;
“(iv) any actions taken to challenge or enforce a directive under paragraphs (4) or (5) of subsections (h);

“(v) any compliance reviews conducted by the Department of Justice or the Office of the Director of National Intelligence of acquisitions authorized under subsection (a);

“(vi) a description of any incidents of noncompliance with a directive issued by the Attorney General and the Director of National Intelligence under subsection (h), including—

“(I) incidents of noncompliance by an element of the intelligence community with procedures adopted pursuant to subsections (e) and (f); and

“(II) incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under subsection (h);

“(vii) any procedures implementing this section; and
“(viii) any annual review conducted pursuant to paragraph (3).

“SEC. 704. USE OF 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, except for the purposes of subsection (j) of such section.”.

(b) 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—

(1) by striking the item relating to title VII;

(2) by striking the item relating to section 701;

and

(3) by adding at the end the following:

“TITLE VII—ADDITIONAL PROCEDURES FOR TARGETING COMMUNICATIONS OF CERTAIN PERSONS OUTSIDE THE UNITED STATES

“Sec. 701. Limitation on definition of electronic surveillance.

“Sec. 702. Definitions.

“Sec. 703. Procedures for acquiring the communications of certain persons outside the United States.

“Sec. 704. Use of information acquired under section 703.”.

(e) SUNSET.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendments made by subsections (a)(2) and (b) shall cease to have effect on December 31, 2013.
(2) CONTINUING APPLICABILITY.—Section 703(h)(3) of the Foreign Intelligence Surveillance Act of 1978 (as amended by subsection (a)) shall remain in effect with respect to any directive issued pursuant to section 703(h) of that Act (as so amended) during the period such directive was in effect. The use of information acquired by an acquisition conducted under section 703 of that Act (as so amended) shall continue to be governed by the provisions of section 704 of that Act (as so amended).

SEC. 102. STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF DOMESTIC COMMUNICATIONS MAY BE CONDUCTED.

(a) STATEMENT OF EXCLUSIVE MEANS.—Title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end of the following new section:

“STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF DOMESTIC COMMUNICATIONS MAY BE CONDUCTED

“Sec. 112. Chapters 119 and 121 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) and the inter-
ception of domestic wire, oral, or electronic communications may be conducted.”.

(b) 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 adding after the item relating to section 111, the following:

“Sec. 112. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted.”.

SEC. 103. SUBMITTAL TO CONGRESS OF CERTAIN COURT ORDERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) INCLUSION OF CERTAIN ORDERS IN SEMI-ANNUAL REPORTS OF ATTORNEY GENERAL.—Subsection (a)(5) of section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended by striking “(not including orders)” and inserting “, orders,”.

(b) REPORTS BY ATTORNEY GENERAL ON CERTAIN OTHER ORDERS.—Such section 601 is further amended by adding at the end the following new subsection:

“(c) The Attorney General shall submit to the committees of Congress referred to in subsection (a) a copy of any decision, order, or opinion issued by the court established under section 103(a) or the court of review established under section 103(b) that includes significant construction or interpretation of any provision of this Act
not later than 45 days after such decision, order, or opinion is issued.”.

SEC. 104. APPLICATIONS FOR COURT ORDERS.

Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended—

(1) in subsection (a)—

(A) by striking paragraphs (2) and (11);

(B) by redesignating paragraphs (3) through (10) as paragraphs (2) through (9), respectively;

(C) in paragraph (5), as redesignated by subparagraph (B) of this paragraph, by striking “detailed”;

(D) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—

(i) by striking “Affairs or” and inserting “Affairs,”; and

(ii) by striking “Senate—” and inserting “Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—”;

(E) in paragraph (7), as redesignated by subparagraph (B) of this paragraph, by striking
“statement of” and inserting “summary statement of”;

(F) in paragraph (8), as redesignated by subparagraph (B) of this paragraph, by adding “and” at the end; and

(G) in paragraph (9), as redesignated by subparagraph (B) of this paragraph, by striking “; and” and inserting a period;

(2) by striking subsection (b);

(3) by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and

(4) in paragraph (1)(A) of subsection (d), as redesignated by paragraph (3) of this subsection, by striking “or the Director of National Intelligence” and inserting “the Director of National Intelligence, or the Director of the Central Intelligence Agency”.

SEC. 105. ISSUANCE OF AN ORDER.

Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended—

(1) in subsection (a)—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively;
(2) in subsection (b), by striking “(a)(3)” and inserting “(a)(2)”;

(3) in subsection (c)(1)—

(A) in subparagraph (D), by adding “and” at the end;

(B) in subparagraph (E), by striking “; and” and inserting a period; and

(C) by striking subparagraph (F);

(4) by striking subsection (d);

(5) by redesignating subsections (e) through (i) as subsections (d) through (h), respectively;

(6) by amending subsection (e), as redesignated by paragraph (5) of this section, to read as follows:

“(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) 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) determines that the factual basis for issuance of an order under this title to approve such electronic surveillance exists;
“(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

“(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 168 hours 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 168 hours 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 surveil-
lance 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 oth-
erwise 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 sub-
division 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).”; and

(7) by adding at the end the following:

“(i) 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).”.

SEC. 106. USE OF INFORMATION.

Subsection (i) of section 106 of the Foreign Intelligence Surveillance Act of 1978 (8 U.S.C. 1806) is amended by striking “radio communication” and inserting “communication”.

SEC. 107. AMENDMENTS FOR PHYSICAL SEARCHES.

(a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—

(1) in subsection (a)—

(A) by striking paragraph (2);

(B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively;

(C) in paragraph (2), as redesignated by subparagraph (B) of this paragraph, by striking “detailed”;

(D) in paragraph (3)(C), as redesignated by subparagraph (B) of this paragraph, by inserting “or is about to be” before “owned”; and

(E) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—

(i) by striking “Affairs or” and inserting “Affairs,”; and
(ii) by striking “Senate—” and inserting “Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—”; and

(2) in subsection (d)(1)(A), by striking “or the Director of National Intelligence” and inserting “the Director of National Intelligence, or the Director of the Central Intelligence Agency”.

(b) ORDERS.—Section 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824) is amended—

(1) in subsection (a)—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and

(2) by amending subsection (e) to read as follows:

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

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

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

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

“(D) makes an application in accordance with
this title to a judge of the Foreign Intelligence Sur-
veillance Court as soon as practicable, but not more
than 168 hours after the Attorney General author-
izes such physical search.

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

“(3) In the absence of a judicial order approving such
physical search, the physical search shall terminate when
the information sought is obtained, when the application
for the order is denied, or after the expiration of 168
hours 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)(A) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(B) The Attorney General shall assess compliance with the requirements of subparagraph (A).”.

(e) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—
(1) in section 304(a)(4), as redesignated by subsection (b) of this section, by striking “303(a)(7)(E)” and inserting “303(a)(6)(E)”; and

(2) in section 305(k)(2), by striking “303(a)(7)” and inserting “303(a)(6)”.

SEC. 108. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.

Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(1) in subsection (a)(2), by striking “48 hours” and inserting “168 hours”; and

(2) in subsection (c)(1)(C), by striking “48 hours” and inserting “168 hours”.

SEC. 109. FOREIGN INTELLIGENCE SURVEILLANCE COURT.

(a) DESIGNATION OF JUDGES.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by inserting “at least” before “seven of the United States judicial circuits”.

(b) EN BANC AUTHORITY.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978, as amended by subsection (a) of this section, is further amended—

(A) by inserting “(1)” after “(a)”; and
(B) by adding at the end the following new paragraph:

“(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 703(h), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

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

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

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

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

(2) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—
(A) in subsection (a) of section 103, as amended by this subsection, by inserting “(except when sitting en banc under paragraph (2))” after “no judge designated under this subsection”; and

(B) in section 302(c) (50 U.S.C. 1822(c)), by inserting “(except when sitting en banc)” after “except that no judge”.

(e) Stay or Modification During an Appeal.—

Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—

(1) by redesignating subsection (f) as subsection (g); and

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

“(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.”.

SEC. 110. TECHNICAL AND CONFORMING AMENDMENTS.

Section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(1) in paragraph (1), by striking “105B(h) or 501(f)(1)” and inserting “501(f)(1) or 703”; and

(2) in paragraph (2), by striking “105B(h) or 501(f)(1)” and inserting “501(f)(1) or 703”.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

SEC. 201. 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) CONTENTS.—The term “contents” has the meaning given that term in section 101(n) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(n)).

(3) 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.

(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 an 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).

(5) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term “element of the intelligence community” means an element of the intelligence community specified in or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

SEC. 202. LIMITATIONS ON CIVIL ACTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

(a) LIMITATIONS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a covered civil action shall not lie or be maintained in a Federal or State court, and
shall be promptly dismissed, if the Attorney General certifies to the court that—

(A) the assistance alleged to have been provided by the electronic communication service provider was—

(i) in connection with an intelligence activity involving communications that was—

(I) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and

(II) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(ii) described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—

(I) authorized by the President; and

(II) determined to be lawful; or
(B) the electronic communication service provider did not provide the alleged assistance.

(2) REVIEW.—A certification made pursuant to paragraph (1) shall be subject to review by a court for abuse of discretion.

(b) REVIEW OF CERTIFICATIONS.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) would harm the national security of the United States, the court shall—

(1) review such certification in camera and ex parte; and

(2) limit any public disclosure concerning such certification, including any public order following such an ex parte review, to a statement that the conditions of subsection (a) have been met, without disclosing the subparagraph of subsection (a)(1) that is the basis for the certification.

(c) NONDELEGATION.—The authority and duties of the Attorney General under this section shall be performed by the Attorney General (or Acting Attorney General) or a designee in a position not lower than the Deputy Attorney General.

(d) CIVIL ACTIONS IN STATE COURT.—A covered civil action that is brought in a State court shall be
deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

(e) Rule of Construction.—Nothing in this section may be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.

(f) Effective Date and Application.—This section shall apply to any covered civil action that is pending on or filed after the date of enactment of this Act.

SEC. 203. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101, is further amended by adding after title VII the following new title:

“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 relat-
ing to a customer or communication), facilities, or
another form of assistance.

“(2) ATTORNEY GENERAL.—The term ‘Attor-
ney General’ has the meaning give that term in sec-
tion 101(g).

“(3) CONTENTS.—The term ‘contents’ has the
meaning given that term in section 101(n).

“(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 Communica-
tions Act of 1934 (47 U.S.C. 153);

“(B) a provider of electronic communica-
tions 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 pro-
vider who has access to wire or electronic com-
munications 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).

“(5) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term ‘element of the intelligence community’ means an element of the intelligence community as specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

“(6) 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 in effect on the day before the date of the enactment of the FISA Amendments Act of 2007 or 703(h).

“(7) 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.

“SEC. 802. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES.

“(a) REQUIREMENT FOR CERTIFICATION.—

“(1) IN GENERAL.—Notwithstanding any other provision of law, no civil action may lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the court that—

“(A) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;
“(B) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;

“(C) any assistance by that person was provided pursuant to a directive under sections 102(a)(4), 105B(e), as in effect on the day before the date of the enactment of the FISA Amendments Act of 2007, or 703(h) directing such assistance; or

“(D) the person did not provide the alleged assistance.

“(2) Review.—A certification made pursuant to paragraph (1) shall be subject to review by a court for abuse of discretion.

“(b) Limitations on Disclosure.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) would harm the national security of the United States, the court shall—

“(1) review such certification in camera and ex parte; and

“(2) limit any public disclosure concerning such certification, including any public order following such an ex parte review, to a statement that the con-
ditions of subsection (a) have been met, without dis-
closing the subparagraph of subsection (a)(1) that is
the basis for the certification.

“(c) REMOVAL.—A civil action against a person for
providing assistance to an element of the intelligence com-
munity that is brought in a State court shall be deemed
to arise under the Constitution and laws of the United
States and shall be removable under section 1441 of title
28, United States Code.

“(d) RELATIONSHIP TO OTHER LAWS.—Nothing in
this section may be construed to limit any otherwise avail-
able immunity, privilege, or defense under any other provi-
sion of law.

“(e) APPLICABILITY.—This section shall apply to a
civil action pending on or filed after the date of enactment
of the FISA Amendments Act of 2007.”.

SEC. 204. PREEMPTION OF STATE INVESTIGATIONS.

Title VIII of the Foreign Intelligence Surveillance
Act (50 U.S.C. 1801 et seq.), as added by section 203
of this Act, is amended by adding at the end the following
new section:

“SEC. 803. PREEMPTION.

“(a) IN GENERAL.—No State shall have authority
to—
“(1) conduct an investigation into an electronic communication service provider’s alleged assistance to an element of the intelligence community;

“(2) require through regulation or any other means the disclosure of information about an electronic communication service provider’s alleged assistance to an element of the intelligence community;

“(3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or

“(4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.

“(b) SUITS BY THE UNITED STATES.—The United States may bring suit to enforce the provisions of this section.

“(c) JURISDICTION.—The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this section.

“(d) APPLICATION.—This section shall apply to any investigation, action, or proceeding that is pending on or
filed after the date of enactment of the FISA Amendments Act of 2007.”

SEC. 205. TECHNICAL AMENDMENTS.

The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101(b), is further amended by adding at the end the following:

“TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

“Sec. 801. Definitions.
“Sec. 802. Procedures for implementing statutory defenses.
“Sec. 803. Preemption.”

TITLE III—OTHER PROVISIONS

SEC. 301. 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, any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

SEC. 302. EFFECTIVE DATE; REPEAL; TRANSITION PROCEDURES.

(a) In General.—Except as provided in subsection (c), the amendments made by this Act shall take effect on the date of the enactment of this Act.

(b) Repeal.—
(1) IN GENERAL.—Except as provided in subsection (c), sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(2) 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.

(c) TRANSITIONS PROCEDURES.—

(1) PROTECTION FROM LIABILITY.—Notwithstanding subsection (b)(1), subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978 shall remain in effect with respect to any directives issued pursuant to such section 105B for information, facilities, or assistance provided during the period such directive was or is in effect.

(2) ORDERS IN EFFECT.—

(A) ORDERS IN EFFECT ON DATE OF ENACTMENT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978—

(i) any order in effect on the date of enactment of this Act issued pursuant to the Foreign Intelligence Surveillance Act of
1978 or section 6(b) of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 556) shall remain in effect until the date of expiration of such order; and

(ii) at the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) shall reauthorize such order if the facts and circumstances continue to justify issuance of such order under the provisions of such Act, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, and 109 of this Act.

(B) ORDERS IN EFFECT ON DECEMBER 31, 2013.—Any order issued under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act, in effect on December 31, 2013, shall continue in effect until the date of the expiration of such order. Any such order shall be governed by the applicable provisions of the Foreign Intelligence Surveillance Act of 1978, as so amended.
(3) Authorizations and Directives in Effect.—

(A) Authorizations and Directives in Effect on Date of Enactment.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978, any authorization or directive in effect on the date of the enactment of this Act issued pursuant to the Protect America Act of 2007, or any amendment made by that Act, shall remain in effect until the date of expiration of such authorization or directive. Any such authorization or directive shall be governed by the applicable provisions of the Protect America Act of 2007 (121 Stat. 552), and the amendment made by that Act, and, except as provided in paragraph (4) of this subsection, any acquisition pursuant to such authorization or directive shall be deemed not to constitute electronic surveillance (as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(f)), as construed in accordance with section 105A of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a)).
(B) Authorization and directives in effect on December 31, 2013.—Any authorization or directive issued under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act, in effect on December 31, 2013, shall continue in effect until the date of the expiration of such authorization or directive. Any such authorization or directive shall be governed by the applicable provisions of the Foreign Intelligence Surveillance Act of 1978, as so amended, and, except as provided in section 704 of the Foreign Intelligence Surveillance Act of 1978, as so amended, any acquisition pursuant to such authorization or directive shall be deemed not to constitute electronic surveillance (as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978, to the extent that such section 101(f) is limited by section 701 of the Foreign Intelligence Surveillance Act of 1978, as so amended).

(4) Use of information acquired under Protect America Act.—Information acquired from an acquisition conducted under the Protect America Act of 2007, and the amendments made by that Act,
shall be deemed to be information acquired from an
electronic surveillance pursuant to title I of the For-

eign Intelligence Surveillance Act of 1978 (50
U.S.C. 1801 et seq.) for purposes of section 106 of
that Act (50 U.S.C. 1806), except for purposes of
subsection (j) of such section.

(5) **NEW ORDERS.**—Notwithstanding any other
provision of this Act or of the Foreign Intelligence
Surveillance Act of 1978—

(A) the government may file an application
for an order under the Foreign Intelligence
Surveillance Act of 1978, as in effect on the
day before the date of the enactment of the
Protect America Act of 2007, except as amend-
ed by sections 102, 103, 104, 105, 106, 107,
108, and 109 of this Act; and

(B) the court established under section
103(a) of the Foreign Intelligence Surveillance
Act of 1978 shall enter an order granting such
an application if the application meets the re-
quirements of such Act, as in effect on the day
before the date of the enactment of the Protect
America Act of 2007, except as amended by
sections 102, 103, 104, 105, 106, 107, 108,
and 109 of this Act.
(6) EXTANT AUTHORIZATIONS.—At the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 shall extinguish any extant authorization to conduct electronic surveillance or physical search entered pursuant to such Act.

(7) APPLICABLE PROVISIONS.—Any surveillance conducted pursuant to an order entered pursuant to this subsection shall be subject to the provisions of the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, and 109 of this Act.