

**Chelsea E. Manning**  
89289  
1300 North Warehouse Road  
Fort Leavenworth, Kansas 66027

2015.10.13

**Memorandum for**

All Members of the U.S. Senate  
All Members of the U.S. House of Representatives

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

**A Proposed Bill**

An Act to abolish the Foreign Intelligence Surveillance Court and improve Information Network Security through sharing while protecting privacy.

**Section 1.** Short title; table of contents.

(a) **Short title.** This Act may be cited as the “Foreign Intelligence Surveillance Reform Act of 2015.”

(b) **Table of contents.** The table of contents for this Act is as follows:

**Sec 1.** Short title; table of contents.

**Sec. 2.** Amendments to the Foreign Intelligence Surveillance Act.

**Sec. 3.** Preservation and access to the Foreign Intelligence Surveillance Court rulings.

**Sec. 4.** Improvements to information network security.

**Sec. 5.** Effective date.

**Sec. 6.** Rule of construction.

**Sec. 7.** No additional funds authorized.

**Sec. 2.** Amendments to the Foreign Intelligence Surveillance Act.

**(a) Amendments for electronic surveillance.**

(1) Section 1801 of title 50, United States Code, is amended—

(A) in subsection (h)(4) by striking “a threat of death or serious bodily harm” and inserting “an imminent threat of death or serious bodily harm”; and

(B) by adding at the end the following:

“(q) “Judge of the United States means any judge of the United States district courts or United States courts of appeal, the judges of which are entitled to hold office during good behavior”;

(2) Section 1802 of title 50, United States Code, is amended—

(A) in subsection (a) by striking “court established under section 103(a)” and inserting “a judge of the United States”;

(B) in subsection (b) by striking “court having jurisdiction under section 103” and inserting “a district court”;

(3) Section 1803 of title 50, United States Code, is amended by striking the section heading, subsections (a) through (h), and inserting the following:

“§ 1803. Jurisdiction.”

“(a) District courts to hear applications and grant orders; record of trial; transmittal to the courts of appeal.

“(1) District courts of the United States 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 subchapter.

“(2) No judge of the United States shall hear the same application for electronic surveillance under this subchapter which has already been denied previously by another judge of the United States.

“(3) If any judge of the United States denies an application for an order authorizing electronic surveillance under this chapter—

“(A) such judge of the United States shall provide immediately for the record a written statement of each reason for the decision; and

“(B) on motion of the United States, the record shall be transmitted under seal, to the respective court of appeals under subsection (b).

“(b) Courts of appeal; record; transmittal to Supreme Court.—

“(A) The courts of appeal of the United States shall have jurisdiction to review the denial of any application made under this subchapter.

“(B) If that court of appeals determines that the application was properly denied—

“(i) that court of appeals shall immediately provide for the record a written statement of each reason for its decision; and

“(ii) 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) Expeditious conduct of proceedings; security measures for maintenance of records.—

“(A) Proceedings under this subchapter shall be conducted as expeditiously as possible.

“(B) The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the district courts and courts of appeal in consultation with the Attorney General and the Director of National Intelligence.

“(d) Jurisdiction and procedures for review of petitions.—District courts shall have jurisdiction to review petitions filed pursuant to section 1861(f)(1) and 1881(h)(4) of this chapter.

“(e) Stay of order.—

“(1) A judge of the United States, or a district court, or a court of appeals, 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 district court or the court of appeals entered under any subchapter of this chapter, while—

“(A) the district court conducts a rehearing;

“(B) an appeal is pending to the court of appeals; or

“(C) 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 chapter.

“(f) Establishment and transmittal of rules and procedures.—

“(1) The district courts and courts of appeal may establish such rules and procedures, and take such actions as are reasonably necessary to administer their responsibilities under this chapter.

“(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 in the district courts.

“(B) All of the judges ,in the courts of appeal.

“(C) All of the justices of the Supreme Court 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 in the House of Representatives.

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

“(g) Compliance with orders, rules, and procedures.—Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the district courts, the courts of appeal, or the Supreme Court of the United States to determine or enforce compliance with an order or rule of such courts or with a procedure approved by such courts.”;

(4) Section 1804 of title 50,United States Code, is amended—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1) by striking “judge having Jurisdiction under section 103” and inserting “judge of the United States”; and

(ii) in paragraph (8) by striking “judge under this title” and inserting “judge of the United States”;

(5) Section 1805 of title 50,United States Code,is amended—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(A) in subsection (b), by striking “judge” and inserting “judge— of the United States”;

(B) in subsection (d)(3), by striking “judge” and inserting “judge of the United States”;

(C) In subsection (e)—

(i) ,in paragraph (1)—

(I) in subparagraph (C), by striking “a judge having jurisdiction under section 103” and inserting “a judge of the United States”; and

(II) in subparagraph (D), by striking “a judge having jurisdiction under section 103” and inserting “a judge of the United States”; and

(ii) in paragraph (5), by striking “a threat of death or serious bodily harm” and inserting “an immediate threat of death or serious bodily harm”;

(D) in subsection (f)—

(i) in paragraph (2)(E), by striking “threat of death or serious bodily harm” and inserting “immediate threat of serious bodily harm”; and

(ii) in paragraph (4), by striking “a threat of death or serious bodily harm” and inserting “an immediate threat of death or serious bodily harm”;

(E) in subsection (j)

(i) by striking “district court” and inserting “a judge of the United States”; and

(ii) by striking “United States district court” and inserting “judge of the United States”; and

(F) in subsection (g), by striking “the United States district court” and inserting “the judge of the United States”;

(G) in subsection (h), by striking “the United States district court” and inserting “the judge of the United States”; and

(6) Section 1806 of title 50, United States Code, is amended—

(A) by striking subsection (f) and inserting the following;

“(f) In camera and ex parte review by a judge of the United States. —

“(1) In matters whenever —

“(A) A court or other authority is notified pursuant to subsection (c) or

(d);

“(B) a motion is made pursuant to subsection (e);

“(C) any motion or request is made by

“(i) an aggrieved person pursuant to any other statute or rule of the United States or any state before any court or other authority of the United States or any State to—

“(I) discover or obtain applications or orders or other materials relating to electronic surveillance authorized by this subchapter; or

“(II) discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this subchapter;

“(2) the judge of the United States from the district court which issued the order, or where the motion is made before another authority, a judge of the United States in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the electronic surveillance as may be

necessary to determine whether the electronic surveillance of the aggrieved person was lawfully conducted; and

“(3) in making such determination, that the judge of the United States may disclose to the aggrieved person, under appropriate procedures and protective orders, portions of the application, order, or other materials relating to the electronic surveillance, only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.”; and

(B) in subsection (j)—

(i) in paragraph (1)—

(I) by striking “the judge shall cause” and inserting “the judge of the United States shall cause”; and

(II) by striking “the judge may determine in his discretion” and inserting “the judge of the United States may determine, at the discretion of that judge of the United States, that”; and

(ii) in paragraph (2)—

(I) by striking “judge the serving” and inserting “judge of the United States, the serving”; and

(II) by striking “the court shall forego” and inserting “the judge of the United States shall forgo;

**(b) Amendments for physical searches.**

(1) Section 1821 of title 50, United States Code, is amended by striking paragraph (3) and inserting the following:



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

“(3) ‘Judge of the United States’ means any judge of the United States district courts or United States courts of appeal, the judges of which are entitled to hold office during good behavior.’;

(2) Section 1822 of title 50, United States Code, is amended—

(A) in subsection (a)(3)—

(i) by striking “the Foreign Intelligence Surveillance Court” and inserting “a district court”; and

(ii) by striking “Chief Justice of the United States” and inserting “district courts and courts of appeal”; and

(B) by striking subsections (c) through (e) and inserting the following:

“(c) Jurisdiction for the District Courts.—

“(1) District courts of the United States shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence anywhere within the United States under the procedures set forth in this subchapter.

“(2) If any judge of the United States denies an application for an order authorizing a physical search under this subchapter—

“(A) such judge of the United States shall provide immediately for the record a written statement of each reason for the decision; and

“(B) on motion of the United States, the record shall be transmitted under seal to the respective court of appeals.

“(d) Courts of appeal; record, transmittal to Supreme Court.—

“(A) The courts of appeal shall have jurisdiction to review the denial of any application made under this subchapter.

“(B) If a court of appeals determines that the application was properly denied—

“(i) the court of appeals shall immediately provide for the record a written statement of each reason for its decision; and

“(ii) 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) Expeditious conduct of proceedings; security measures for maintenance of records.—

“(A) Proceedings under this chapter shall be conducted as expeditiously as possible.

“(B) The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the district courts and courts of appeal in consultation with the Attorney General and the Director of National intelligence.”;

(3) Section 1823 of title 50, United States Code, is amended—

(A) in subsection (a) by striking “judge of the Foreign Intelligence Surveillance Court” and inserting “judge of the United States”;

(B) in subsection (c) by striking “judge” and inserting “judge of the United States”;

(4) Section 1824 of title 50, United States Code is amended—

(A) in subsection (a)—

(i) by striking “judge shall enter” and inserting “the judge of the United States shall enter”; and

(ii) by striking “judge finds that” and inserting “judge of the United States finds that”;

(B) in subsection (c) by striking “judge” and inserting “judge of the United States”;

(C) in subsection (c)(2)(E) by striking “the court” and inserting “the issuing judge of the United States”;

(D) in subsection (d)—

(i) in paragraph (2) by striking "the judge" and inserting "the issuing judge of the United States"; and

(ii) in paragraph (3) by striking “judge” and inserting "judge of the United States"; and

(E) in subsection (e)—

(i) in paragraph (1)—

(I) in subparagraph (C) by striking "a judge of the Foreign Intelligence Surveillance Court” and inserting "a judge of the United States”;

(II) in subparagraph (D) by striking "a judge of the Foreign Intelligence Surveillance Court" and inserting "a judge of the United States”;

(ii) in paragraph (5), by striking "a threat of death or serious bodily harm" and inserting "an immediate threat of death or serious bodily harm";

(5) Section 1825 of title 50, United States Code, is amended—

(A) by striking subsection (g) and inserting the following:

(g) In camera and ex parte review by a judge of the United States. —

"(1) In matters whenever. —

"(A) a court or other authority is notified pursuant to subsection (d) or (e);

"(B) a motion is made pursuant to subsection (f); or

"(C) any motion or request is made by—

"(i) an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States of any State to—

"(I) discover or obtain application or orders or other materials relating to a physical search authorized by this subchapter; or

"(II) discover, obtain, or suppress evidence or Information obtained or derived from a physical search authorized by this subchapter; then

"(2) the judge of the United States from the district court which issued the order, or where the motion is made before another authority, a judge of the United States in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted; and

"(3) in making such determinations, that judge of the United States may—

"(A) disclose to the aggrieved person, under appropriate security procedures and protective order, portions of the application, order, or other materials relating to the physical search; or

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(B) require the Attorney General to provide the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.";

(B) in subsection (j)—

(i) in paragraph (1)—

(I) by striking "the judge shall cause" and inserting "the judge of the United States shall cause"; and

(II) by striking "the judge may determine in his discretion" and inserting "the judge of the United States may determine, at that judge of the United States' discretion, that"; and

(C) in subsection (g), by striking "judge" and inserting "judge of the United States";

**(c) Amendments for pen registers and trap and trace devices for foreign intelligence purposes.—**

(1) Section 1842 of title 50, United States Code, is amended—

(A) in subsection (b) by striking paragraphs (1) and (2), and inserting the following:

"(1) a judge of the United States for the respective district court.";

"(2) a United States magistrate judge under chapter 43 of title 28, United States Code, for the respective district court.";

(B) in subsection (d)—

(A) in paragraph (1)—

(i) by striking "the judge shall enter" and inserting "that judge of the United States shall enter";

(ii) by striking "the judge finds that" and inserting "that judge finds that";

(C) in subsection (g) by striking "the judge" and inserting "that judge of the United States";

(D) in subsection (h)(2) by striking "the court established under section 103(a)" and inserting "any district court";

(2) Section 1843 of title 50, United States Code, is amended—

(A) In subsection (a)—

(i) in paragraph (1) by striking "a judge referred to in section 402(b) of this Act" and inserting "a judge of the United States"; and

(ii) in paragraph (2) by striking "judge" and inserting "a judge of the United States";

(B) in subsection (c)(2) by striking "a threat of death or serious bodily harm to any person" and inserting "an immediate threat of death or serious bodily harm to any person"; and

(C) in subsection (h)(2) by striking "the court established under section 103(a)" and inserting "any judge of the United States"; and

(3) Section 1845 of title 50, United States Code, is amended—

(A) by striking "subsection (f) and inserting the following:

"(f) In camera and ex parte review by a judge of the United States.— “

(1) in matters whenever.—

"(A) a court or other authority is notified pursuant to subsection (d) or (e);

"(B) a motion is made pursuant to subsection (f); or

"(C) any motion or request is made by—

"(i) an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States of any State to—

"(I) discover or obtain applications or orders or other materials relating to the use of a pen register or trap and trace device authorized by this subchapter; or

"(II) discover obtain, or suppress evidence or information obtained or derived from the use of a pen register or trap and trace device authorized by this subchapter; then

"(2) the judge of the United States from the district court which issued the order, or where the motion is made before another authority, a judge of the United States in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the use of a pen register or trap and trace was lawfully authorized and conducted; and

"(3) In making such determinations, that judge of the United States may—

"(A) disclose to the aggrieved person, under appropriate security procedures and protective order, portions of the application, order, or other material relating to the physical search.; or

"(B) require the Attorney General to provide the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search."; and

(B) in subsection (g)—

(i) in paragraph (1)—

(I) by striking "the United States district court" and inserting "a review of foreign intelligence surveillance orders."

(II) by striking "the court" and inserting "that judge of the United States"; and

(ii) in paragraph (2) by striking "the court" and inserting "that judge of the. United States";

**(d) Amendments for access to certain business records for foreign Intelligence purposes.—**

(1) Section 1861 of title 50, United States, is amended—

(A) in subsection (b)—

(i) in paragraph (1) by striking subparagraphs (A) and (B) and inserting the following:

"(A) a judge of the United States for the respective district court.";

"(B) a United States magistrate judge under chapter 43 of title 28.

United States Code, for the respective district court.";

(B) in subsection (c)—

(i) in paragraph (1)—

(I) by striking "the judge shall enter" and inserting "that judge of the United States shall enter";



(ii) by striking "the judge finds that" and inserting "that judge finds that";

(C) in subsection (f)—

(i) by striking "Judicial review of FISA orders" and inserting "Judicial review of foreign intelligence orders."

(ii) in paragraph (2)—

(I) in subparagraph (A) by striking clauses (i) through (iii) and inserting the following:

"(i) A person receiving a production order may challenge the legality of that order by filing a petition with a judge of the United States. Not less than one year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with a judge of the United States.

"(ii) Not later than 72 hours after the assignment of such petition, that judge of the United States shall conduct an initial review of the petition. If that judge of the United States determines that the petition is frivolous, that judge of the United States shall promptly consider the petition.

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

(II) by striking paragraphs (B) and (C) and inserting the following:

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

"(C)(i) A judge of the United States considering a petition to modify or set aside a nondisclosure order may grant such petition only if that judge of the United States 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 immediately endanger the life or physical, safety of any person.

"(ii) If that judge of the United States denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of one year from filing another such petition with respect to such nondisclosure order. unless the recipient of such order can justify, with good cause, that a reconsideration is warranted.

(iii) in paragraph (3)—

(I) by striking "the court of review established under section 103(b)" and inserting "the respective court of appeals for that district court"; and

(II) by striking "The court of review" and inserting "That court of appeals";

(iv) in paragraph (4) by striking "the Chief Justice of the United States" and inserting "the district courts and courts of appeal";

(D) in subsection (g)(3) by striking "the court established under section 103(a)" and inserting "any judge of the United States";

(E) in subsection (i)(4) by striking "section 103" and inserting "section 1803 (d) of this chapter";

(2) Section 1862 of title 50, United States Code, is amended in subsection (c)(1)(E) by striking "the court established under section 103" and inserting "the district courts"; and

(3) Section 1863 of title 50, United States Code, is amended in subsection (a)(1) by striking subparagraphs (E) and (F);

**(e) Amendments for oversight.—**

(1) Section 1871 of title 50, United States Code, is amended—

(A) in subsection (a) by striking paragraphs (4) and (5) and inserting the following:

"(4) a summary of significant legal interpretations of this chapter involving matters before the district courts or the courts of appeal, including interpretations presented in applications or pleadings filed with the district courts or the courts of appeal by the Department of Justice; and

"(5) copies of all decisions, order, or opinions of the district courts or courts of appeal that include significant construction or interpretation of the provisions of this chapter.

(B) in subsection (c) by striking paragraph (1) and inserting the following

"(1) not later than 45 days after the date on which a district court or court of appeals issues—

"(A) a decision, order or opinion, that includes

"(i) any denial or modification of any provision of law;

"(ii) any result in a change of application of any provision of this chapter; or

"(iii) any nuanced, reinterpreted, or novel application of any provision of this chapter; then

"(B) a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and";

(C) by striking subsection (e); and

(2) Section 1872 of title 50, United States Code, is amended—

(A) in subsection (a) by striking "Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(E))" and inserting "the district courts and courts of appeal"; and

(B) in subsection (c)(2)(B) by striking "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review" and inserting "the district courts and courts of appeal";

**(f) Amendments for additional procedures regarding certain persons outside the United States. —**

(1) Section 1881 of title 50, United States Code, is amended in subsection (b)—

(A) by striking paragraphs (2) and (3); and

(B) by redesignating paragraphs (4) and (5) as paragraphs (2) and (3);

(2) Section 1881a of title 50, United States Code, is amended—

(A) in subsection (g)—

(i) in paragraph (1)—

(I) in subparagraph (A) by striking "the Foreign Intelligence Surveillance Court" and inserting "the district courts";

(II) in subparagraph (B) by striking “the court” and inserting “the district courts”;

(ii) in paragraph (2)(A)—

(I) in clause (i) by striking “the Foreign Intelligence Surveillance Court” and inserting “the district courts”;

(II) in clause (ii)(II) by striking “the Foreign Intelligence Surveillance Court” and inserting “the district courts”;

(iii) in paragraph (3) by striking “the Foreign Intelligence Surveillance Court” and inserting “the district courts”;

(C) in subsection (h) by striking paragraphs (4) through (6) and inserting the following:

“(4) Challenging of directives.—

“(A) Authority to challenge.—An electronic service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the issuing judge of the United States, who shall have jurisdiction to review such petition.

“(B) Standards for review.—A judge of the United States considering a petition filed under paragraph (A) may grant such a petition only if that judge of the United States finds that the directive does not meet the requirements of this section or is otherwise unlawful.

“(C) Procedures for initial review.—

“(i) A judge of the United States shall conduct an initial review of a petition filed under subparagraph (A) not later than five days after being assigned such petition.

"(ii) If that judge of the United States determines—

"(I) 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 establishing new law; then

"(II) that judge of the United States shall immediately deny such petitions and affirm the directive or any part of the directive that is the subject of such petitions 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.

"(iii) Upon making a determination under this subparagraph or promptly thereafter, that judge of the United States shall provide a written statement for the record of the reasons for such determination.

"(D) Procedures for plenary review.—

"(i) if a judge of the United States determines that a petition filed under subparagraph (A) requires plenary review, then that judge of the United States 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.

"(ii) If that judge of the United States does not set aside the directive, then that judge of the United States shall immediately affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified.

" (iii) That judge of the United States shall provide a written statement for the record of the reasons for a determination under this subparagraph.

"(E) Continued effect—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

"(F) Contempt of court—Failure to obey an order issued under this paragraph may be punished by the judge of the United States or the district 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 issuing judge of the United States, who shall have jurisdiction to review such petition.

"(B) Procedures for review.—

"(i) A judge of the United States considering a petition filed under subparagraph (A) shall, not later than 30 days after receiving 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 that judge of the United States shall provide a written statement for the record of the reasons for a determination under this paragraph.

"(ii) That judge of the United States shall provide a written statement for the record of the reasons for a determination under this paragraph.

"(C) Contempt of court—Failure to obey an order issued under this paragraph may be punished by a judge of the United States or a district court as contempt of court.

"(D) Process.— Any process under this paragraph may be served before any judge of the United States for any district court in which the electronic communication service provider may be found.

"(6) Appeal. —

"(A) Appeal to the courts of appeal. —

"(i) The United States or an electronic service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the respective court of appeals for review of a decision issued pursuant to paragraph (4) or (5) by a district court.

"(ii) The court of appeals of the issuing district court shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

"(B) Certiorari to the Supreme Court. —

"(i) The United States or an electronic communication service provider receiving a directive pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision by the court appeals issued under subparagraph (A).

"(ii) The record of for such review shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.";

(D) by striking subsection (i) and U) and inserting the following:

"(i) Judicial review of certifications and procedures. — “

(1) In general. —

"(A) Review by a judge of the United States. — A judge of the United States shall have jurisdiction to review a certification —

"(i) submitted in accordance with subsection (g);

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

“(iii) amendments to such certification or procedures.



"(B) Time period for review. —

"(i) That judge of the United States shall review —

"(I) a certification submitted in accordance with subsection (g); and

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

"(ii) that judge of the United States shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and procedures are submitted.

"(C) Amendments. —

"(i) The Attorney General and the Director of National Intelligence —

"(I) may, as necessary at any time, amend a certification submitted in accordance with subsection (g); or the targeting and minimization procedures adopted in accordance with subsections (d) and (e);

"(II) may make such amendments even if that judge of the United States is conducting or has completed the review of such certification or such procedures; and

"(III) shall submit the amended certification or amended procedures to that judge of the United States not later than seven days after amending such certification or such procedures.

"(ii) That judge of the United States shall review any amendment under this subparagraph under the procedures set forth in this subsection.

"(iii) The Attorney General and the Director of National Intelligence may authorize the use of such an amended certification or amended procedures by that judge of the United States.

"(2) Review.—That judge of the United States shall review the following:

"(A) Certification.—A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements. “

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

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

"(ii) prevent the intentional acquisition of any communications 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 1801(h) or section 1821(4) of this chapter, as appropriate.

“(3) Orders.—

"(A) Approval.—

"(i) If a judge of the United States finds that a certification submitted in accordance with subsection (g)—

“(I) contains all of the required elements; and

“(II) that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States; then

“(ii) that judge of the United States 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. —

“(i) If that judge of the United States finds—

“(I) that a certification submitted in accordance with subsection (g) does not contain all the required elements; or

“(II) that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the Fourth Amendment to the Constitution of the United States; then

“(ii) that judge of the United States shall issue an order directing the United States to, at the election of the United States and to the extent required by the order of that judge of the United States—

“(I) correct any deficiency identified by the order of that judge of the United States not later than 30 days after the date on which that judge of the United States 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, that judge of the United States shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

"(D) Limitations on use of information.—

"(i) In general.—Except as provided in clause (ii), if that judge of the United States 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 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, except with the approval of the Attorney General if the information indicates an imminent threat of death or serious bodily harm to any person.

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

"(4) Appeal.—

"(A) Appeal to the courts of appeal.—

"(i) The United States may file a petition with the respective court of appeals for review of an order made under this subsection.

"(ii) That court of appeals shall have jurisdiction to consider such petition.

"(iii) For any decision under this subparagraph affirming, reversing, or modifying an order of a judge of the United States, then that court of appeals 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 if the United States files a petition for review of an order under this section, until that court of appeals enters an order under subparagraph (c).

"(C) Implementation pending approval.— 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 appeals shall determine, and enter a corresponding order regarding, whether all or part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

"(D) Certiorari to the Supreme Court.—

"(i) The United States may file a petition for a writ of certiorari for review of a decision of the court of appeals under subparagraph (A).

"(ii) 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 that judge of the United States—

"(i) the certification prepared in accordance with subsection (g); and

"(ii) the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

"(B) Reauthorization of orders, authorizations, and directives.— If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directive issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until that judge of the United States 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 of such certifications.

"(j) Judicial proceedings.—

"(1) Expedited judicial proceedings.— Judicial proceedings under this section shall be conducted as expeditiously as possible.

"(2) Time limits.— A time limit for a judicial decision in this section shall apply unless the district, the courts of appeal, or any judge of the United States, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.";

(E) in subsection (k)(1)—

(i) by striking "The Foreign Intelligence Surveillance Court" and inserting "the district courts"; and

(ii) by striking "The Chief Justice of the United States" and inserting "the district courts and courts of appeal";

(F) in subsection (1)—

(i) in paragraph (1) by striking subparagraph (A) and inserting the following:

"(A) the district courts; and";

(ii) in paragraph (3)(C) by striking clause (i) and inserting the following:

"(i) the district courts;";

(3) Section 1881b of title 50, United States Code, is amended by striking the section heading and subsections (a) through (g) and inserting the following;

"§ 1881b. Certain acquisitions inside the United States targeting United States persons outside the United States.

"(a) Jurisdiction of the district courts.—

"(1) In general.—A judge of the United States shall have jurisdiction to review an application and to enter an order—

"(A) approving the targeting of a United States person reasonably believed to be outside the United States to acquire foreign intelligence information;

"(B) if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this chapter; and

"(C) such acquisition is conducted within the United States.

"(2) Limitation.—

"(A) Limiting on targeting.— If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States

person is again reasonably believed to be located in the United States while an order issued pursuant to subsection (c) is in effect.

"(B) Rule of Construction. — Nothing in this section shall be construed to limit the authority of the United States to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.

"(b) Application. —

"(1) In general. — Each application for an order under this section shall be made by a federal officer in writing upon oath or affirmation to a judge of the United States having jurisdiction under subsection (a)(1), and require the approval of the Attorney General based upon the finding of the Attorney General that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include —

"(A) the identity of the Federal officer making the application;

"(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

"(C) as statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is —

"(i) a person reasonably believed to be located outside the United States; and

"(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

"(D) a statement of proposed minimization procedures that meet the definition of minimization proposed under section 1801(h) or 1821(4) of this chapter, as appropriate;



"(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;

"(F) a certification made by the Attorney General or an official specified in section 1804(a)(6) of this chapter that—

"(i) the certifying official deems the information sought to be foreign intelligence information;

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

"(iii) such information cannot reasonably be obtained by normal investigative techniques;

"(iv) designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this chapter; and

"(v) includes a statement of the basis for the certification that—

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

"(II) such information cannot reasonably be obtained by normal investigative techniques;

"(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;

"(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;

"(I) a statement of the facts concerning any previous applications that have been made to any judge of the United States involving the United States person specified in the application and the action taken on each previous application; and

"(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

"(2) Other requirements of the Attorney General.—The Attorney General may require that any affidavit or certification from any other officer in connection with the application.

"(3) Other requirements of the judge of the United States.—That judge of the United States may require the applicant to furnish other such information as may be necessary to make the findings required by subsection (c)(1).

"(c) Order.—

"(1) Findings.—Upon an application made pursuant to subsection (b), the judge of the United States shall enter an ex parte order as requested or modified by that judge of the United States approving the acquisition if that judge of the United States finds that—

"(A) the application has been made by a federal officer and approved by the Attorney General;

"(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

"(i) a person reasonably believed to be located outside the United States; and

"(ii) a foreign power, an agent of a foreign power or an officer or employee of a foreign power;

"(C) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate; and

"(D) the filed application contains all statements and certifications required by subsection(b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(i)(F)(v) and any other information furnished under subsection (b)(3).

"(2) Probable cause.—

"(A) In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge of the United States having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target.

"(B) No United States person may be consider a foreign power, agent of a foreign power, or officer or employee of a foreign power solely on the basis of activities protected by the First Amendment of the Constitution of the United States.

"(3) Review.—

"(A) Limitation on review.—A review by a judge of the United States having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

"(B) Review of probable cause.—If that judge of the United States determines that the facts submitted under subsection (b) are insufficient to establish

probable cause under paragraph (1)(B), then that judge of the United States shall enter an order so stating.

"(C) Review of minimization procedures. — If that judge of the United States determines that the proposed minimization procedures referred to in paragraph (1)(C) do not meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate, then that judge of the United States shall enter an order so stating.

"(D) Review of certification. — If that judge of the United States determines that an application pursuant to subsection (b) does not contain all of the required elements, or that certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), then that judge of the United States shall enter an order so stating.

"(E) Appeal of review. — The United States may appeal an order under subparagraphs (B) through (D) pursuant to subsection (f).

"(F) Record. — For any determination made under subparagraphs (B) through (D), that judge of the United States shall provide a written statement for the record of the reasons for the determination.

"(4) Specifications. — An order approving an acquisition under this subsection shall specify —

“(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

"(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition shall be directed;

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

"(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

"(E) the period of time during which the acquisition is approved.

"(5) Directives.—An order approving an acquisition under this subsection shall direct—

"(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by a judge of the United States, be followed;

"(B) if applicable, an electronic communication service provider to provide to the United States forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

"(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

"(D) if applicable, that the United States compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities or assistance.'

"(6) Duration.—An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90—day periods Upon submission of renewal applications meeting the requirements of subsection (b).

"(7) Compliance.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge of the United States may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained or disseminated.

"(d) Emergency authorization.—

"(1) Authority for emergency authorization.—Notwithstanding any other provision of this section, the Attorney General may authorize an emergency acquisition if—

“(A) a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition;

“(B) an application in accordance with this section is made to a judge of the United States as soon as practicable, but not more than seven days after the Attorney General authorizes such acquisition; and

“(C) the Attorney General reasonably determines that—

“(i) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained; and

“(ii) that the factual basis for the issuance of an order under this section exists;

"(2) Minimization procedures. — If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

"(3) Termination of emergency authorization. — In the absence of a judicial order approving an acquisition under paragraph (1) such acquisition shall, at the earliest of the following, terminate—

"(A) when the information sought is obtained;

"(B) when the application for the order is denied; or

"(C) after the expiration of seven days from the time of authorization by the Attorney General.

"(4) Use of information. — If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information reasonably indicates an imminent threat of death or serious bodily harm to any person.

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(e) Release from liability.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

"(f) Appeal.—

"(1) Appeals to the courts of appeal.—

"(A) The United States may file a petition with the respective court of appeals for review of an order issued pursuant to subsection (c).

"(B) That court of appeals shall—

"(i) have jurisdiction to consider such petition; and

"(ii) provide a written statement for the record of a decision under this paragraph.

"(2) Certiorari to the Supreme Court.—

"(A) The United States may file a petition for a writ of certiorari for a review of decision by the courts of appeal issued under subparagraph (1).

"(B) 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.

(4) Section 1881c of title 50, United States Code, is amended by striking the section heading and subsection (a) through (e) and inserting the following:

"§ 1881c. Other acquisitions targeting United States persons outside the United States.

"(a) Jurisdiction and scope.—

"(1) Jurisdiction.—A judge of the United States shall have jurisdiction to enter an order pursuant to subsection (c).



"(2) Scope.—

“(A) Limitation on targeting United States persons.—No element of the intelligence community, for the purpose of acquiring foreign intelligence information, may—

“(i) intentionally target a United States person reasonably believed to be outside the United States; and

“(ii) under circumstances in which that targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes;

“(B) Exceptions.—Elements of the intelligence community, for the purpose of acquiring foreign intelligence information, may target a United States person under the limitations of subparagraph (A) if—

“(i) a judge of the United States has entered an order with respect to such targeted United States person; or

“(ii) the Attorney General has authorized an emergency acquisition pursuant to subsection (c) and (d), respectively, or any other provision of this chapter.

"(3) Limitations.—

“(A) Moving or misidentified targets.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

"(B) Applicability.—If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 1881b of this chapter, the acquisition may only be conducted if authorized under section 188b of this chapter, or in accordance with another provision of this chapter other than this section.

"(C) Rule of construction.—Nothing in this paragraph shall be construed to limit the authority of the United States to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.

"(b) Application.—

"(1) In general— Each application for an order under this section shall be made by a federal officer in writing upon oath or affirmation to a judge of the United States having jurisdiction under subsection (a)(1), and require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section and shall include—

"(A) the identity of the Federal officer making the application;

"(B) the identity, if known, or a description of the specific United States person who is the target of the acquisition;

"(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target is—

"(i) a person reasonably believed to be located outside the United States; and

"(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

"(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate;

"(E) a certification made by the Attorney General, an official specified in section 1804(a)(6) of this chapter, or the head of an element of the intelligence community that—

"(i) the certifying official deems the information sought to be foreign intelligence information; and

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

"(F) a statement of the facts concerning any previous applications that have been made to any judge of the United States involving the United States person specified in the application and the action taken on each previous application; and

"(G) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

"(2) Other requirements of the Attorney General—The Attorney General may require that any affidavit or certification from any other officer in connection with the application.

"(3) Other requirements of the judge of the United States.—That judge of the United States may require the applicant to furnish other such information as may be necessary to make the findings required by subsection (c)(1).

"(c) Order.—

"(1) Findings.— Upon an application made pursuant to subsection (b), that judge of the United States shall enter an ex parte order as requested or as modified by that judge of the United States if that judge of the United States finds that—

"(A) the application has been made a federal officer and approved by the Attorney General;

"(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

"(i) a person reasonably believed to be located outside the United States; and

"(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

"(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate; and

"(D) the filed application contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

"(2) Probable cause.—

"(A) In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge of the United States having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target.

"(B) No United States person may be considered a foreign power, agent of a foreign power, or officer or employee protected by the First Amendment of the Constitution of the United States.

"(3) Review.—

"(A) Limitations on review.—

"(i) A review by a judge of the United States having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

"(ii) That judge of the United States shall not have jurisdiction to review, if requested by that judge of the United States, more than a summary of the means by which an acquisition under this section may be conducted.

"(B) Review of probable cause.—If that judge of the United States determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, then that judge of the United States shall enter an order so stating.

"(C) Review of minimization procedures.—If that judge of the United States determines that the proposed minimization procedures applicable to the dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate, then that judge of the United States shall enter an order so stating.

"(D) Review of certification.—If that judge of the United States determines that an application pursuant to subsection (b) does not contain all of the required elements, or that certification or certifications are clearly erroneous on the basis of

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), then that judge of the United States shall enter an order so stating.

"(E) Scope of review of certification. —

"(i) If that judge of the United States determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), then that judge of the United States shall enter an order so stating.

"(F) Appeal of review. — The United States may appeal an order under subparagraphs (B) through (E) pursuant to subsection (e).

"(G) Record. — For any determination made under subparagraphs (B) through (D), that judge of the United States shall provide a written statement for the record of the reasons for the determination.

"(4) Duration. — An order under this paragraph shall be effective for a period of not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

"(5) Compliance. — At or prior to the end of the period of time for which an order or extension is granted under this section, that judge of the United States may —

"(A) assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated; and

"(B) not inquire into the circumstances relating to the conduct of the acquisition without any reason to believe that those procedures have not been followed.

"(d) Emergency authorization. —

"(1) Authority for emergency authorization. — Notwithstanding any other provision of this section, the Attorney General may authorize an emergency acquisition if—

"(A) a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition;

"(B) an application in accordance with this section is made to a judge of the United States as soon as practicable, but not more than seven days after the Attorney General authorizes such acquisition; and

"(C) the Attorney General reasonably determines that—

"(i) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained; and

"(ii) that the factual basis for the issuance of an order under this section exists;

"(2) Minimization procedures. — If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

"(3) Termination of emergency authorization. — In the absence of a judicial order under subsection (c), an emergency acquisition shall, at the earliest of the following, terminate—

"(i) when the information sought is obtained;

"(ii) when the application for the order is denied; or

“(iii) after the expiration of seven days from the time of authorization by the Attorney General.

“(4) Use of information.—If an application for approval submitted to that judge of the United States pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order issued approving the acquisition is issued under subsection (c), no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information reasonably indicates an imminent threat of death or serious bodily harm to any person.

“(e) Appeal.—

“(1) Appeals to the courts of appeal.—

“(A) The United States may file a petition with the respective court of appeals for review of an order issued pursuant to subsection (c).

“(B) That court of appeals shall—

“(i) have jurisdiction to consider such petition; and

“(ii) provide a written statement for the record of a decision under this paragraph.

“(2) Certiorari to the Supreme Court.—



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(A) The United States may file a petition for a writ of certiorari for a review of decision by the courts of appeal issued under subparagraph (1).

"(B) 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) Section 1881d of title 50, United States Code, is amended in subsection (a) by striking "judge having jurisdiction under section 703(a)(1) or 704(a)(1)" and inserting "a judge of the United States having jurisdiction under 1881a(a)(1) or 1881c(a)(1) of this chapter";

(g) **Amendments for protection of persons assisting the government.**—Section 1885a of title 50, United States Code, is amended in subsection (a)(1) by striking "the court established under section 103(a)" and inserting "a judge of the United States";

(h) **Numbering of subchapters.**

(1) Title 50, United States Code, is amended in the heading—

(A) by striking "ELECTRONIC SURVEILLANCE" and inserting "SUBCHAPTER I - ELECTRONIC SURVEILLANCE";

(B) by striking "PHYSICAL SEARCHES" and inserting "SUBCHAPTER II - PHYSICAL SEARCHES";

(C) by striking "ACCESS TO CERTAIN BUSINESSES RECORDS FOR FOREIGN INTELLIGENCE PURPOSES" and inserting "SUBCHAPTER III - ACCESS TO CERTAIN BUSINESS RECORDS";

(D) by striking "OVERSIGHT" and inserting "SUBCHAPTER IV - OVERSIGHT";

(E) by striking "ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES" and inserting "SUBCHAPTER V -

ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES";

(F) by striking "PROTECTION OF PERSONS ASSISTING THE GOVERNMENT" and inserting "SUBCHAPTER VI - PROTECTION OF PERSONS ASSISTING THE UNITED STATES";

**(i) Table of contents amendments.—**

(1) by striking the item relating to section 1803 of title 50, United States code, and inserting the following item:

"§ 1803. Jurisdiction"; and

(2) by striking "ELECTRONIC SURVEILLANCE" and inserting "SUBCHAPTER I - ELECTRONIC SURVEILLANCE";

(3) by striking "PHYSICAL SEARCHES" and inserting "SUBCHAPTER II - PHYSICAL SEARCHES";

(4) by striking "ACCESS TO CERTAIN BUSINESSES RECORDS FOR FOREIGN INTELLIGENCE PURPOSES" and inserting "SUBCHAPTER III - ACCESS TO CERTAIN BUSINESS RECORDS";

(5) by striking "OVERSIGHT" and inserting "SUBCHAPTER IV - OVERSIGHT";

(6) by striking "ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES" and inserting "SUBCHAPTER V - ADDITIONAL PROCEDURE REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES";

(7) by striking "PROTECTION OF PERSONS ASSISTING THE GOVERNMENT" and inserting "SUBCHAPTER VI - PROTECTION OF PERSONS ASSISTING THE UNITED STATES";

**(j) Miscellaneous amendments.—**

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(1) Section 1801 of title 50, United States Code, as amended in subsection (a)(1), is further amended—

(A) in subsection (a)—

(i) In paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking "title" and inserting "subchapter";

(II) in subparagraph (A)—

(aa) in clause (i) by striking "section 101(a)(1), (2), or (3)" and inserting "section 1801(a)(1), (2), or (3) of this chapter";

(B) in subsection (b)—

(i) by striking "title" and inserting "subchapter"; and

(ii) by striking "section 105" and inserting "section 1805 of this chapter";

(3) Section 1804 of title 50, United States Code, as amended in subsection (a)(4), is further amended—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1)—

(I) by striking "under this title" and inserting "under this subchapter";

(II) by striking "in this title" and inserting "in this subchapter";

(ii) In paragraph (6)(D) by striking "section 101(e)" and inserting "section 1801(e) of this chapter";

(iii) in paragraph (8) by striking "title" and inserting "subchapter"; and

(B) in subsection (c) by striking "section 105" and inserting "section 1805 of this chapter";

(C) in subsection (d)(1)(A) by striking "section 105" and inserting "section 1805 of this chapter";

(4) Section 1805 of title 50, United States Code, as amended in subsection (a)(5) is further amended—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1) by striking "section 104" and inserting "section 1804 of this chapter";

(ii) in paragraph (3) by striking "section 101(h)" and inserting "section 1801(h) of this chapter";

(iii) in paragraph (4)—

(I) by striking "required by section 104" and inserting "required by section 1804 of this chapter";

(II) by striking "section 104(A)(7)(E)" and inserting "section 1804(A)(7)(E) of this chapter";

(III) by striking "section 104(d)" and inserting "section 1804(d) of this chapter";

(B) in subsection (c)(1)(A) by striking "section 104(a)(3)" and inserting "section 1804(a)(3) of this chapter";

(C) in subsection (d)—

(i) in paragraph (1)—

(aa) by striking "section 101(a)(1), (2), or (3)" and inserting "section 1801(a)(1), (2), or (3) of this chapter"; and

(bb) by striking "Act" and inserting "chapter";

(ii) in paragraph (2)—

(I) in the matter preceding subparagraph (A), by striking "title" and inserting "subchapter";

(II) in subparagraph (B)—

(aa) by striking "Act" and inserting "chapter";

(bb) by striking "of section 101(a)" and inserting "of section 1801(a) of this chapter";

(cc) by striking "section 101(a)(4)" and inserting "section 1801(a)(4) of this chapter"; and

(III) in subparagraph (B), by striking "Act" and inserting "chapter";

(D) in subsection (e)—

(i) in paragraph (1)—

(I) in the matter preceding paragraph (A), by striking "title" and inserting "subchapter";

(II) in subparagraph (B) by striking "title" and inserting "subchapter"; and

(III) in subparagraph (D) by striking "title" and inserting "subchapter":

(ii) in paragraph (2) by striking "title" and inserting "subchapter"; and

(iii) in paragraph (4) by striking "section 103" and inserting "section 1803(b) of this chapter";

(E) in subsection (f)—

(i) in the matter preceding paragraph (1), by striking "title" and inserting "subchapter"; and

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(ii) in paragraph (3)(A)(ii) by striking "title" and inserting "subchapter";

(F) in subsection (g)—

(i) by striking "section 102(a)" and inserting "section 1802(a) of this chapter";

(ii) by striking "title" and inserting "subchapter";

(G) in subsection (h) by striking "Act" and inserting "chapter"; and

(H) in subsection (i)—

(i) by striking "Government" and inserting "United States";

(ii) by striking "title" and inserting "subchapter"; and

(iii) by striking "section 402(d)(2)" and inserting "section 1842(d)(2) of this chapter";

(5) Section 1806 of title 50, United States Code, as amended in subsection (a)(6) is further amended—

(A) in subsection (a)—

(i) by striking "this title concerning" and inserting "this subchapter concerning";

(ii) by striking "required by this title" and inserting "required by this subchapter";

(iii) by striking "title shall" and inserting "subchapter shall"; and

(iv) by striking "this title may" and inserting "this subchapter may";

(B) in subsection (b) by striking "title" and inserting "subchapter";

(C) in subsection ©—

(i) by striking "Whenever the Government intends" and inserting "Whenever the United States intends";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(ii) by striking "title" and inserting "subchapter";

(iii) by striking "the Government shall" and inserting "the United States shall"; and

(iv) by striking "that the Government intends" and inserting "that United States intends";

(D) in subsection (d) by striking "title" and inserting "subchapter";

(E) in subsection (j), in the matter preceding subparagraph (A) by striking "section 105(e)" and inserting "Section 1805(e) of this chapter"; and

(F) in subsection (k)—

(i) in paragraph (1), in the matter preceding subparagraph (A) by striking "title" and inserting "subchapter"; and

(ii) in paragraph (2)—

(I) by striking "section 104(a)(7)(B)" and inserting "section 1804(a)(7)(B) of this chapter"; and

(II) by striking "section 105" and inserting "section 1805 of this chapter";

(6) Section 1807 of title 50, United States Code, is amended, in subsection (a) by striking "title" and inserting "subchapter";

(7) Section 1808 of title 50, United States Code, is amended—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by striking "under this title" and inserting "under this subchapter"; and

(II) by striking "in this title" and inserting "in this subchapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(ii) in paragraph (2)—

(I) in subparagraph (A) by striking "subchapter";

(II) in subparagraph (B) by striking "Act" and inserting "chapter";

and

(III) in subparagraph (C) by striking "section 105(e)" and

inserting "section 1805(e) of this chapter";

(B) in subsection (b)—

(i) by striking "date of this Act" and inserting "date of this chapter";

(ii) by striking "implementation of this Act" and inserting

"implementation of this chapter"; and

(iii) by striking "whether this Act" and inserting "whether this chapter";

(8) Section 1809 of title 50, United States Code, is amended, in the matter preceding subsection (a)—

(A) in paragraph (1)—

(i) by striking "Act" and inserting "chapter"; and

(ii) by striking "section 112" and inserting "section 1812 of this chapter";

(B) by striking "section 112" and inserting "section 1812 of this chapter";

(9) Section 1810 of title 50, United States Code, is amended in the matter preceding subsection (a)—

(A) by striking "section 101(a) or (b)(1)(A)" and inserting "section 1801(a) or (b)(1)(A) of this chapter"; and

(B) by striking "section 109" and inserting "section 1809 of this chapter";

(10) Section 1811 of title 50, United States Code, is amended by striking "title" and inserting "subchapter";



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(11) Section 1812 of title 50, United States Code, is amended—

(A) in subsection (a) by striking "Act" and inserting "subchapter"; and

(B) in subsection (b) by striking "Act" and inserting "subchapter";

(12) Section 1813 of title 50, United States Code, is amended—

(A) in subsection (a)(3) by striking "section 101 of the Foreign Intelligence Surveillance Act of 1978" and inserting "section 1801 of this chapter"; and

(B) in subsection (b)—

(i) in paragraph (1) by striking "the date of the enactment of this Act" and inserting "December 19th, 2014"; and

(ii) in paragraph (3)(A) by striking "court established under subsection (a) or (b) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1803)" and inserting "a judge of the United States";

(13) Section 1821 of title 50, United States Code, as amended in subsection (b)(1) is further amended—

(A) in the matter preceding paragraph (1)—

(i) by striking "section 101 of this Act" and inserting "section 1801 of this chapter"; and

(ii) by striking "title" and inserting "subchapter";

(B) in paragraph (4)—

(i) in subparagraph (B) by striking "section 101(e)(1) of this Act" and inserting "section 1801(e)(1) of this chapter";

(ii) in subparagraph (D)—

(l) by striking "section 302(a)" and inserting "section 1822(a) of this chapter"; and

(II) by striking "section 304" and inserting "section 1824 of this chapter";and

(C) in paragraph (5)—

(i) in subparagraph (A)—

(aa) by striking "section 101(f) of this Act" and inserting "section 1801(f) of this chapter"; and

(bb) by striking "Government"; and

(ii) in subparagraph (B) by striking "section 101(f) of this Act" and inserting "section 1801(f) of this chapter";

(14) Section 1822 of title 50, United States Code, as amended in subsection (b)(2) is further amended—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking "title" and inserting "subchapter";and

(II) in subparagraph (A)—

(aa) in clause (i) by striking "section 101(a)(1), (2),or (3)" and inserting "section 1801(a)(1), (2), or (3) of this chapter"; and

(bb) in clause (iii) by striking "section 301(4)" and inserting "Section 1821(4) of this chapter":

(ii) in paragraph (2) by striking "section 306" and inserting "section 1826 of this chapter"; and

(iii) in paragraph (3)—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(I) in subparagraph (A) by striking "section 301(4) and section 303" and inserting "section 1821(4) and section 1823 of this chapter"; and

(II) in subparagraph (B) by striking "section 305(g)" and inserting "Section 1825(g) of this chapter"; and

(iv) in paragraph (4)(B) by striking "Government" and inserting "United States"; and

(B) in subsection (b)—

(i) by striking "title" and inserting "subchapter"; and

(ii) by striking "section 304" and inserting "section 1824 of this chapter";

(15) Section 1823 of title 50, United States Code, as amended in subsection (b)(3) is further amended—

(A) in subsection (a)—

(i) In the matter preceding paragraph (1)—

(I) by striking "under this title" and inserting "under this subchapter"; and

(II) by striking "set forth in this title" and inserting "under this subchapter";

(ii) in paragraph (6)(D) by striking "section 101(e)" and inserting "section 1801(e) of this chapter"; and

(iii) in paragraph (8) by striking "title" and inserting "subchapter";

(B) in subsection (c) by striking "section 304" and inserting "section 1824 of this chapter"; and

(C) In subsection (d)(1)(A) by striking "section 101(b)(2)" and inserting "section 1801(b)(2) of this chapter";

(16) Section 1824 of title 50, United States Code, as amended in subsection (b)(4) is further amended—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1) by striking “section 303” and inserting “section 1823 of this chapter”;

(ii) in paragraph (3) by striking “title” and inserting “subchapter”;and

(iii) in paragraph (4)—

(I) by striking “by section 303” and inserting “by section 1823 of this chapter”;

(II) by striking “section 303(a)(6)(E)” and inserting “section 1823(a)(6)(E) of this chapter”;and

(III) by striking “section 303(c)” and inserting “section 1823(c) of this chapter”;

(B) in subsection (d)—

(i) in paragraph (1) by striking “section 101(a)” and inserting “section 1801(a) of this chapter”;

(ii) in paragraph (2)—

(I) by striking “title” and inserting “subchapter”;

(II) by striking “Act” and inserting “chapter”;

(III) by striking “paragraph (5), (6), or (7) of section 101(a)” and inserting “paragraph (5), (6), or (7) of section 1801of this chapter”;

(IV) by striking “section 101(a)(4)” and inserting “section 1801(a) of this chapter”;

(C) in subsection (e)—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A) by striking "title" and inserting "subchapter";

(II) in subparagraph (B) by striking "title" and inserting "subchapter"; and

(III) in subparagraph (D) by striking "title" and inserting "subchapter";

(ii) in paragraph (2) by striking "title" and inserting "subchapter"; and

(iii) in paragraph (4) by striking "section 103" and inserting "section 1803(b) of this chapter"; and

(D) in subsection (f) by striking "title" and inserting "subchapter"; and

(17) Section 1825 of title 50, United States Code, as amended in subsection (b)(5), is further amended—

(A) in subsection (a)—

(i) by striking "conducted pursuant to this title" and inserting "conducted pursuant to this subchapter";

(ii) by striking "procedures required by this title" and inserting "procedures required by this subchapter"; and

(iii) by striking "search pursuant to this title" and inserting "search pursuant to this subchapter";

(B) in subsection (b)—

(i) by striking "section 304" and inserting "section 1824 of this chapter"; and

(ii) by striking "Act" and inserting "chapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(C) in subsection (c) by striking "title" and inserting "subchapter";

(D) in subsection (d) by striking "title" and inserting "subchapter";

(E) in subsection (e) by striking "title" and inserting "subchapter";

(F) in subsection (j) by striking "section 304(d)" and inserting "section 1824(d) of this chapter"; and

(G) in subsection (k)—

(i) by striking "title" and inserting "subchapter";

(ii) by striking "section 303(a)(6)" and inserting "section 1823(a)(6) of this chapter"; and

(iii) by striking section 304" and inserting "section 1824 of this chapter";

(18) Section 1826 of title 50, United States Code, is amended—

(A) in the matter preceding paragraph (1) by striking "title" and inserting "subchapter";

(B) in paragraph (1) by striking "title" and inserting "subchapter";

(C) in paragraph (3) by striking section 305(b)" and inserting "section 1825(b) of this chapter"; and

(D) in paragraph (4) by striking "section 304(e)" and inserting "section 1824(e) of this chapter"; and

(19) Section 1828 of title 50, United States Code, is amended in the matter preceding paragraph (1)—

(A) by striking "section 101(a) or (b)(1)(A)" and inserting "section 1801(a) or (b)(1)(A) of this chapter";

(B) by striking "Act" and inserting "chapter"; and

(C) by striking "section 307" and inserting "section 1827 of this chapter"

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(20) Section 1829 of title 50, United States Code, is amended by striking "title" and inserting "subchapter";

(21) Section 1841 of title 50, United States Code, is amended—

(A) in the matter preceding paragraph (1) by striking "title" and inserting "subchapter";

(B) In paragraph (1) by striking "section 101 of this Act" and inserting "section 1801 of this chapter";

(C) in paragraph (3)—

(i) in subparagraph (A) by striking "title" and inserting "subchapter"; and

(ii) in subparagraph (B) by striking "title" and inserting "subchapter";

and

(D) in paragraph (4)(B)(i) by striking "section 701" and inserting "section 1881 of this chapter";

(22) Section 1842 of title 50, United States Code, as amended in subsection (c)(1), is further amended—

(A) in subsection (a)—

(i) in paragraph (1) by striking "Government" and inserting "United States";

(ii) in paragraph (2) by striking "title I of this Act" and inserting "subchapter I of this chapter";

(B) in the matter preceding subsection (c)(1) by striking "Government" and inserting "United States";

(C) in subsection (d)(2)(B)(ii)(II) by striking "section 105(b)(2)(C) of this Act" and inserting "section 1805(b)(2)(C) of this chapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(D) in subsection (g) by striking "Government" and inserting "United States";

and

(23) Section 1843 of title 50, United States Code, as amended in subsection (c)(2), is further amended—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1) by striking "title" and inserting "subchapter";

(ii) in paragraph (1) by striking "section 402(b) of this Act" and inserting "section 1842(b) of this subchapter"; and

(iii) in paragraph (2) by striking "section 402 of this Act" and inserting "section 1842 of this chapter"; and

(B) in subsection (b)—

(i) In paragraph (1) by striking "section 402 of this Act" and inserting "section 1842 of this subchapter"; and

(ii) in paragraph (2) by striking "section 402" and inserting "section 1842 of this chapter";

(C) In subsection (c)—

(i) in paragraph (1) by striking "section 402 of this Act" and inserting "section 1842 of this chapter"; and

(ii) in paragraph (2) by striking "section 402 of this Act" and inserting "section 1842 of this chapter"; and

(D) in subsection (d) by striking "section 402h" and inserting "1842(h) of this chapter";



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(24) Section 1844 of title 50, United States Code, is amended by striking "title" and inserting "subchapter";

(25) Section 1845 of title 50, United States Code, as amended in subsection (c)(3), is further amended—

(A) in subsection (a)—

(i) in paragraph (1) by striking "title" and inserting "subchapter";

(ii) in paragraph (2) by striking "title" and inserting "subchapter";

(B) in subsection (b) by striking "title" and inserting "subchapter";

(C) in subsection (c) by striking "title" and inserting "subchapter";

(D) in subsection (d) by striking "title" and inserting "subchapter"; and

(E) in subsection (e)(1)(B) by striking "title" and inserting "subchapter";

(26) Section 1846 of title 50, United States Code, is amended—

(A) in subsection (a) by striking "title" and inserting "subchapter"; and

(B) in subsection (b)—

(i) in paragraph (1) by striking "title" and inserting "subchapter"; and

(ii) in paragraph (3) by striking "section 403" and inserting "section

1843 of this chapter";

(27) Section 1861 of title 50, United States Code, as amended in subsection (d)(1), is further amended—

(A) in subsection (c)(2)(F)—

(i) in clause (iv) by striking "Government" and inserting "United States";

(ii) in clause (vi)—

(I) by striking "Government directs" and inserting "United States directs";

(II) by striking "Government forthwith" and inserting "United States forthwith"; and

(iii) in the matter preceding clause (vii)(I) by striking "Government" and inserting "United States";

(B) in subsection (f)—

(i) In paragraph (3)—

(I) by striking "order by the Government" and inserting "order by the United States"; and

(II) by striking "petition by the Government" and inserting "petition by the United States"; and

(ii) in paragraph (5)—

(I) by striking "the Government" and inserting "the United States";

(II) by striking "any Government" and inserting "any United States";

(C) in subsection (g)—

(i) in paragraph (1) by striking "title" and inserting "subchapter"; and

(ii) in paragraph (2)(B) by striking "section 101(e)(1)" and inserting "section 1801(e)(1) of this chapter";

(D) in subsection (h)—

(i) by striking "order under this title concerning" and inserting "order under this subchapter concerning";

(ii) by striking "provisions of this title" and inserting "provisions of this subchapter"; and

(iii) by striking "order under this title may" and inserting "order under this subchapter may";

(E) in subsection (i)(4) by striking "section 103" and inserting "section 1803(b) of this chapter"; and

(F) in subsection (j)—

(i) in the matter preceding paragraph (1) by striking "Government" and inserting "United States";

(ii) in paragraph (2) by striking "Government" and inserting "United States";

(G) in subsection (k)(1) by striking "section 101" and inserting "section 1801 of this chapter";

(28) Section 1862 of title 50, United States Code, as amended in subparagraph (d) (2), is further amended—

(A) in subsection (a) by striking "section 501" and inserting "section 1861 of this chapter";

(B) in subsection (b)—

(i) in paragraph (1) by striking "section 501" and inserting "section 1861 of this chapter";

(ii) in paragraph (2) by striking "section 501(b)(2)(C)" and inserting "section 1861(b)(2)(C) of this chapter";

(iii) in paragraph (4) by striking "section 601(b)(2)(C)" and inserting "section 1861(b)(2)(C) of this chapter"; and

(iv) in paragraph (6) by striking "section 501" and inserting "section 1861 of this chapter";

(C) in subsection (c)(1)—

(i) in subparagraph (A) by striking "section 501" and inserting "section 1861 of this chapter";

(ii) in subparagraph (C) by striking "section 501" and inserting "section 1861 of this chapter";

(iii) in subparagraph (E) by striking "section 501(g)" and inserting "section 1861(g) of this chapter";

(29) Section 1863 of title 50, United States Code, as amended in subparagraph (d) (3), is further amended—

(A) in subsection (a)(1)(A) by striking "sections 105, 305, 402, 501, 702, 703, and 704" and inserting "sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this chapter"; and

(B) in subsection (b)—

(i) in paragraph (1) by striking "sections 703 and 704" and inserting "section 1881b, and 1881c of this chapter";

(ii) in the matter preceding paragraph (2)(A) by striking "section 702" and inserting "section 1881a of this chapter"

(iii) in paragraph (4), in the matter preceding subparagraph (A) by striking "section 501(b)(2)(B)" and inserting "section 1861(b)(2)(B) of this chapter"; and

(iv) in paragraph (5), in the matter preceding subparagraph (A) by striking "section 501(b)(2)(C)" and inserting "section 1861(b)(2)(C) of this chapter";

(30) Section 1864 of title 50, United States Code, is amended—

(A) in subsection (a)—

(i) in paragraph (1)—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(I) in subparagraph (C) by striking "Act" and inserting "chapter";

(II) in subparagraph (E) by striking "Act" and inserting "chapter":

and

(III) by striking "subparagraph (F)" and inserting the following:

"(i) subchapter IV of this chapter.

"(ii) subchapter V of this chapter with respect to applications described in section 1861(b)(2)(B).

"(iii) subchapter V of this chapter with respect to applications described in section 1861(b)(2)(C).";

(ii) in paragraph (2)—

(I) in subparagraph (C) by striking "Act" and inserting "chapter";

(II) in subparagraph (E) by striking "Act" and inserting "chapter";

and

(III) in subparagraph (F) by striking "Act" and inserting "chapter";

(iii) in paragraph (3)—

(I) in subparagraph (A) by striking "Act" and inserting "chapter";

and

(II) in subparagraph (B) by striking "Act" and inserting "chapter";

(iv) in paragraph (4)—

(I) in subparagraph (A) by striking "Act" and inserting "chapter";

(II) in subparagraph (B) by striking "Act" and inserting "chapter";

(B) in subsection (b)(1) by striking "Act" and inserting "chapter";

(31) Section 1871 of title 50, United States Code, as amended in subsection (e)(1), is further amended in subsection (a)—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(A) in paragraph (1)—

(i) in subparagraph (A) by striking "section 105" and inserting "section 1805 of this chapter";

(ii) In subparagraph (B) by striking "section 304" and inserting "section 1825 of this chapter";

(iii) in subparagraph (C) by striking "section 402" and inserting "section 1842 of this chapter";

(iv) in subparagraph (D) by striking "section 501" and inserting "section 1861 of this chapter";

(v) in subparagraph (E) by striking "section 703" and inserting "section 1881b of this chapter"; and

(vi) in subparagraph (F) by striking "section 704" and inserting "section 1881c of this chapter"; and

(B) in paragraph (2) by striking "section 101(b)(1)(C)" and inserting "section 1801(b)(1)(C) of this chapter"; and

(C) in paragraph (3) by striking "Act" and inserting "chapter";

(32) Section 1873 of title 50, United States Code, is amended—

(A) in subsection (a)(1)—

(i) in subparagraph (A) by striking "sections 105, 304, 402, 501, 702, 703, and 704" and inserting "sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this chapter"; and

(ii) by striking subparagraphs (E) and (F);

(B) in subsection (b)—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(i) in paragraph (1) by striking "sections 703 and 704" and inserting "sections 1881b, and 1881c of this chapter";

(ii) in paragraph (2), in the matter preceding subparagraph (A) by striking "section 702" and inserting "section 1881a of this chapter";

(iii) in paragraph (4), in the matter preceding subparagraph (A) by striking "section 501(b)(2)(B)" and inserting "section 1861(b)(2)(B) of this chapter"; and

(iv) in paragraph (5), in the matter preceding subparagraph (A) by striking "section 501(b)(2)(C)" and inserting "section 1861(b)(2)(C)";

(33) Section 1881 of title 50, United States Code, as amended in subsection (f)(1), is further amended in subsection (A)—

(A) by striking "section 101" and inserting "section 1801 of this chapter"; and

(B) by striking "title" and inserting "subchapter";

(34) Section 1881a of title 50, United States Code, as amended in subsection (f)(2), is further amended—

(A) in subsection (c)(4)—

(i) by striking "title" and inserting "subchapter"; and

(ii) by striking "title" and inserting "subchapter";

(B) in subsection (e)(1) by striking "section 101(h) or 301(4)" and inserting "section 1801(h) or 1821(4) of this chapter";

(C) in subsection (f)(1)(b) by striking "Act" and inserting "subchapter";

(D) in subsection (g)(2)(A)—

(i) in clause (ii)(I) by striking "section 101(h) or 301(4) and inserting "section 1801(h) or 1821(4) of this chapter"; and

(ii) in clause (iii) by striking "Act" and inserting "subchapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(E) in subsection (h)—

(i) in paragraph (1)(A) by striking "Government" and inserting "United States"; and

(ii) in paragraph (2) by striking "Government" and inserting "United States";

(F) in subsection (i)—

(i) in paragraph (2)(C) by striking "section 101(h) or section 301(4)" and inserting "section 1801(h) or 1821(4) of this chapter"; and

(ii) in paragraph (3)(B), in the matter preceding clause (i) by striking "Government to, at the Government's election" and inserting "United States to, at the election of the United States"; and

(G) in subsection (k)(2)—

(i) by striking "the Government" and inserting "the United States"; and

(ii) by striking "any Government" and inserting "any United States";

(35) Section 1881d of title 50, United States Code, is amended—

(A) in subsection (a)—

(i) by striking "under section 703 or 704" and inserting "section 1881b or 188c of this chapter";

(ii) by striking "Government" and inserting "United States";

(B) in subsection (b)—

(i) by striking "section 105 or 304" and inserting "section 1805 or 1824 of this chapter";

(ii) by striking "section 703 or 704" and inserting "section 1881b or 1881c of this chapter";



(36) Section 1881e of title 50, United States Code, is amended by striking subsections (a) and (b) and inserting the following:

"(a) Information acquired under section 1881a of this chapter. Information acquired from an acquisition conducted under section 1881a of this chapter shall be deemed to be information acquired from an electronic surveillance order pursuant to subchapter I for purposes of section 1805 of this chapter, except for the purposed of subsection U) of such section.

"(b) Information acquired under section 1881b of this chapter. Information acquired from an acquisition conducted under section 1881b of this chapter shall be deemed to be information acquired from an electronic surveillance order pursuant to subchapter I for purposes of section 1806 of this chapter.";

(37) Section 1881f of title 50, United States Code, is amended—

(A) in subsection (a) by striking "title" and inserting "subchapter"; and

(B) in subsection (b)—

(i) in paragraph (1)—

(I) in subparagraph (A) by striking "section 702(g)" and inserting "section 1881a(g) of this chapter";

(II) in subparagraph (B) by striking "section 702(c)(2)" and inserting "section 1881a(c)(2) of this chapter";

(III) in subparagraph (C) by striking "section 702(h)" and inserting "section 1881a(h) of this chapter";

(IV) in subparagraph (D)

(aa) by striking "subsections (d) and (e) of section 702" and inserting "section 1881a(d) and (e) of this chapter";

(bb) by striking "provisions of section 702" and inserting "section 1881a of this chapter";

(V) in subparagraph (E) by striking "paragraph (4) or (5) of section 702(h)" and inserting "section 1881a(h)(4) or (5) of this chapter";

(VI) in subparagraph (F) by striking "section 702(a)" and inserting "section 1881a(a) of this chapter"; and

(VII) in subparagraph (G) by striking clauses (i) and (ii), and inserting the following:

"(i) with a directive issued by the Attorney General and the Director of National Intelligence under section 1881a(h) of this chapter, including Incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under section 1881a(h) of this chapter; and

"(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with section 1881a(d), (e), and (f) of this chapter; and";

(ii) in paragraph (2)—

(I) in the matter preceding subparagraph (A) by striking "section 702" and inserting "section 1881a"

(II) in subparagraph (A) by striking "section 703(b)" and inserting "section 1881b(b) of this chapter"; and

(III) in subparagraph (C) by striking "section 703(d)" and inserting "section 1881b(d) of this chapter"; and

(iii) in paragraph (3)—

(I) in the matter preceding subparagraph (A) by striking “section 704” and inserting “section 1881c of this chapter”;

(II) in subparagraph (A) by striking “section 704(b)” and inserting “section 1881c(b) of this chapter”; and

(III) in subparagraph (C) by striking “section 704(d)” and inserting “section 1881c(d) of this chapter”;

(38) section 1881g of title 50, United States Code, is amended—

(A) in subsection (a) by striking “title” and inserting “subchapter”;

(B) in subsection (b)—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A) by striking “section 702” and inserting “section 1881a of this chapter”;

(II) in subparagraph (A) by striking “section 702(g)” and inserting “section 1881a(g) of this chapter”;

(III) in subparagraph (B) by striking “section 702(c)(2)” and inserting “section 1881a(c)(2) of this chapter”;

(IV) in subparagraph (C) by striking “section 702(h)” and inserting “section 1881a(h) of this chapter”;

(V) in subparagraph (D)—

(aa) by striking “subsections (d) and (e) of section 702” and inserting “section 1881a(d) and (e) of this chapter”; and

(bb) by striking “provisions of section 702” and inserting “provisions of section 702(h)” and inserting “section 1881a(h) of this chapter”:

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(VI) in subparagraph (E) by striking "paragraph (4) or (5) of section 702(h)" and inserting "section 1881a(h)(4) or (5) of this chapter";

(VII) in subparagraph (F) by striking "section 702(a)" and inserting "section 1881a(a) of this chapter";

(VIII) in subparagraph (G) by striking clauses (i) and (ii) and inserting the following:

"(i) with directive issued by the Attorney General and the Director of National Intelligence under section 1881a(h) of this chapter, including incidents of noncompliance by a specified person to whom the Attorney General and the Director of National Intelligence issued a directive under section 1881.a(h) of this chapter; and

"(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with section 1881a(d), (e), and (f) of this chapter; and"; and

(IX) in subparagraph (H) by striking "section 702" and inserting "section 1881a of this chapter";

(ii) in paragraph (2)—

(I) in the matter preceding subparagraph (A) by striking "section 703" and inserting "section 1881b of this chapter"; and

(II) in subparagraph (A) by striking "section 703(b)" and inserting "section 1881b(b) of this chapter";

(iii) in paragraph (3)—

(I) in the matter preceding subparagraph (A) by striking "section 704" and inserting "section 1881c of this chapter";

(II) in subparagraph (A) by striking "section 704(b)" and inserting "section 1881c(b) of this chapter"; and

(III) in subparagraph (C) by striking "section 704(d)" and inserting "section 1881c(d) of this chapter";

(39) Section 1881g of title 50, United States Code is amended—

(A) by striking "title" and inserting "chapter";

(B) by striking "Government" and inserting "United States";

(C) by striking "title of this Act" and inserting "subchapter of this chapter";

(40) Section 1885 of title 50, United States Code, is amended—

(A) In the matter preceding paragraph (1) by striking "title" and inserting "subchapter";

(B) in paragraph (4) by striking "section 101(n)" and inserting "section 1801(n)"; and

(C) in paragraph (8)(B)—

(i) in clause (i) by striking "section 103(a)" and inserting "section 1803(a) of this chapter"; and

(ii) in clause (ii) by striking "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)." and inserting "section 1802(a)(4), 1805B(e), or 1881a(h).";

(41) Section 1885a of title 50, United States Code, is amended in subsection (a)—

(A) in paragraph (1) by striking "section 103(a)" and inserting "section 1803(a) of this chapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(B) in paragraph (3) by striking "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))" and inserting "section 1802(a)(4), 1805(e), or 1881a(h) of this chapter";

(42) Section 1885c of title 50, United States Code, is amended—

(A) in subsection (a) by striking "title" and inserting "subchapter";

(B) in subsection (b)—

(i) in paragraph (1) by striking "section 802" and inserting "section 1885a of this chapter";

(ii) in paragraph (2) by striking "section 802" and inserting "section 1885a of this chapter"; and

(iii) in paragraph (3) by striking "section 803" and inserting "section 1885b of this chapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

**Sec. 3.** Preservation and access to the Foreign Intelligence Surveillance Court rulings.

(1) All rulings, orders, rules, memoranda of law, supporting documents, or other pleadings or evidence produced by and for the former Foreign Intelligence Surveillance Court judges or panels, or by and for any former Foreign Intelligence Surveillance Court of Review judges or panels shall be preserved by the Attorney General and the Director of National Intelligence in a manner consistent with—

(A) national security; and

(B) ease of access by the district courts and courts of appeal.

(2) All such pleadings and documentation in paragraph (1) shall be made available to the judges of the district courts, the judges of the courts of appeal, in a manner consistent with national security.

**Sec. 4.** Improvements to information network security.

**(a) Provisions for commercial and government information network security.—**

(1) Title 50, United States Code is amended by inserting after section 3045 to the following:

"§ 3046. Definitions for information network security sharing.

"As used in this chapter—

"(1) Agency.—The term 'agency' has the meaning given the term in section 3502 of title 44, United States Code.

"(2) Antitrust laws.— The term 'antitrust laws'—

"(A) has the meaning given the term in section 12 of title 15, United States Code (section 1 of the Clayton Act);

"(B) includes section 45 of title 15, United States Code (section 45 of the Federal Trade Commission Act) to the extent that section applies to unfair methods of competition; and

"(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

"(3) Defensive measure.—The term 'defensive measure' means an action, device, procedure, technique, or other measure executed on an information system that prevents or mitigates a known or suspected information network security threat or security vulnerability.

"(4) Information network command and control.— The term 'information network command and control' means a method that may reasonably be determined to be used for remote identification of, access to, or use of, and information system or information that is stored on, processed by, or transiting an information system.



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(5) Information network security purpose.—The term 'information network security purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from an information network security threat or security vulnerability or identifying the source of an information network security threat or using a defensive measure.

"(6) Information network security threat.—

"(A) In general.—The term 'information network security threat' means an action—

"(i) not protected by the First Amendment of the Constitution; “

(ii) on or through a specific information system or information systems;

"(iii) that will deliberately or intentionally result in an unauthorized effort to impact—

"(I) the security and protection;

"(II) the confidentiality of any person;

“(III) the physical or electronic integrity; or

"(IV) the access and availability; and

"(iv) affecting—

"(I) a specific information system or information systems;

or

"(II) Information that is stored on, processed by, or transiting an information system.

“(B) Exclusion.—The term 'information network security threat' does not include any action that solely involves a violation of—

"(i) any terms and conditions;"

(ii) any terms of service;

"(iii) any licensing agreement; or

"(iv) any other contract or agreement.

"(7) Information network threat indicator.—The term 'information network threat indicator' means any specific information or a specific physical object that is necessary to describe or identify—

"(A) malicious reconnaissance, including anomalous patterns of communications that may reasonably be determined to be transmitted for the purpose of gathering technical information related to a specific—

"(i) information network security threat; or

"(ii) security vulnerability.

"(B) a specific method that may reasonably be determined to defeat a security control or exploitation of a security vulnerability;

"(C) a specific security vulnerability, including anomalous activity that may reasonably be determined to indicate the existence of such specific security vulnerability;

"(D) a specific method that may reasonably be determined to cause a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

"(E) a specific information network command and control that may reasonably be determined to be malicious in nature;

"(F) any actual or potential harm caused by a specific incident, including a description of any information that may reasonably be determined to have been exfiltrated as a result of a specific Information network security threat; or

"(G) any other specific attribute or characteristics that may reasonably be determined to identify or describe a specific information network security threat, if such disclosure of that attribute or characteristic is not otherwise prohibited by law.

"(8) Information system.—The term 'information system'—

"(A) has the meaning given the term in section 3502 of title 44, United States Code; and

"(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

"(9) Local government—The term 'local government' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

"(10) Malicious reconnaissance.—The term 'malicious reconnaissance' means a specific method for actively probing or passively monitoring an information system, if such method is associated with a known or suspected information security threat.

"(11) Monitor.—The term 'monitor' means to acquire, identify, scan, or otherwise process information that is stored, processed by, or transiting an information system.

"(12) Non-Federal entity.—

"(A) In general—Except as otherwise provided in this paragraph, the term 'non-Federal entity' means any—

"(i) private entity;

"(ii) non-Federal government department or agency;

"(iii) or State, tribal, or local government (including a political subdivision, department, officer, employee, or agent thereof).

"(13) Private entity.—

"(A) In general.— Except as otherwise provided in this paragraph, the term 'private entity' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

"(B) Inclusion.— The term 'private entity' includes a component of a State, tribal, or local government performing, water, telephony, and electric utility services.

"(C) Exclusion.— The term 'private entity' does not include a foreign power as defined in section 1801 of title 50, United States Code (Foreign Intelligence Surveillance Act of 1978, as amended).

"(14) Security control.— The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information stored or transiting such information system.

"(15) Security vulnerability.— The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

"(16) United States entity.— The term 'United States entity' means a department or agency of the United States or any component or office of such department or agency.

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(17) Tribal. — The term 'tribal' has the meaning given the term 'Indian tribe' in section 450b of title 25, United States Code (section 4 of the Indian Self-Determination and Education Assistance Act).";

(2) Title 50, United States Code is amended after 3046, as inserted in paragraph (1), by inserting the following:

"§ 3046a. Sharing of information network threat indicators or defensive measures between the United States government with non-Federal entities.

"(a) Sharing by the United States government. —

"(1) In general. — Consistent with the protection of national defense information, classified information, intelligence source and methods, and privacy and civil liberties, the Director of National Intelligence, shall —

"(A) consult with the heads of —

"(i) the Department of Defense:

"(ii) the Department of Energy;

"(iii) the Department of Homeland Security;

"(iv) the Department of Justice; and

"(v) and the National Laboratories (as defined in section 15801 of title 42, United States Code (section 2 of the Energy Policy Act of 2005)); and

"(B) develop and promulgate procedures to facilitate and promote —

"(i) the timely sharing of information network threat indicators in the possession of the United States with representatives of relevant non-Federal entities with appropriate security clearances;

"(ii) the timely sharing with relevant non-Federal entities of information network threat indicators or information in the possession of the United States that may be declassified and shared as unclassified information; and

"(iii) the sharing with non-Federal entities, if appropriate, of information in the possession of the United States about imminent or ongoing information network security threats to such entities to prevent or mitigate adverse impacts from such information network security threats.

"(2) Development of procedures.—The procedures developed and promulgated under paragraph (1) shall—

"(A) ensure the United States has and maintains the capability to share information network threat indicators in a reasonable period of time consistent with the protection of classified information;

"(B) incorporate existing and responsibilities of the United States intelligence community and non-Federal entities for information sharing by the United States, including sector-specific information sharing and analysis offices;

"(C) include procedures for notifying non-Federal entities that have received an information network threat indicator from a United States entity that is known or determined to be in error or contravention of this section, the Foreign Intelligence Surveillance Reform Act, or amendments made by such Act, or another provision of United States law or policy of such error or contravention;

"(D) include requirements for United States entities, prior to the sharing of an information network threat indicator, to—

"(E) include procedures that require United States entities, prior to the sharing of an information network threat indicator, to—

"(i) review such information network threat indicator to assess whether such information network threat indicator, in contravention of the requirement under section 3046c(d)(2) of this chapter, contains any information that such departments or agencies can reasonably determine to be personal information of, or personal information identifying, any person not directly related to an information network security threat, and remove and destroy such information in a reasonable period of time;

"(ii) implement a technical capability configured to remove or exclude any personal information of, or information identifying, any person not directly related to a specific information network security threat.

"(b) Policies and procedures for sharing with the United States government.—

"(1) Establishment—The President shall develop policies and procedures relating to the receipt of information network threat indicators and defensive measures by United States entities.

"(2) Requirements concerning policies and procedures.— The policies and procedures required under paragraph (1) shall—

"(A) be developed in accordance with the privacy and civil liberties guidelines required under subsection (c).

"(B) ensure that an information network threat indicator shared by a non-Federal entity with a United States entity, is shared in a reasonable period of time with other United States entities deemed to have a clear interest in such an information network threat indicator.

"(C) ensure there—

"(i) is an audit capability;

"(ii) are appropriate measures in place for the training of officers, employees, or agents of United States entities to prevent any willful or negligent usage an information network threat indicator or defensive measure with the United States government; and

"(iii) are appropriate measures in place for the investigation of officers, employees, or agents of United States entities who knowingly,willfully or negligently use an information network threat indicator or defensive measure with the United States government in violation of an offense under subsection (d) or any other procedure, regulation, or law.

"(3) Public sector notice and access.—The president shall ensure there is public notice of, and access to, the policies and procedures established in paragraph (1) so that—

"(A) any non-Federal entity may share network threat indicators and defensive measures through such process with the United States government; and

"(B) information network threat indicators shared by non-Federal entities with a United States entity are shared in a reasonable period of time with other United States entities that are deemed to have a clear interest in such information network threat indicator.

"(4) Report on development and implementation.—

"(A) in general.—Not later than 60 days after the date of the enactment of this section, the President, or a designee of the President, shall submit a report on the development and implementation of the policies and procedures established in paragraph (1), including a description of such policies and procedures to—



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(i) the Permanent Select Committee on Intelligence of the House of Representatives;

"(ii) the Select Committee on Intelligence of the Senate;  
and

"(iii) the Committee on the Judiciary of the Senate;

"(B) Classified annex.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

"(c) Office of Information Network Security.—

"(1) Establishment.—There is within the Office of the Director of National Intelligence an Office of Information Network Security.

"(2) Director.—There is a Director of Information Network Security, who shall be appointed by the Director of National Intelligence.

"(3) Primary mission.—The Office of Information Network Security shall —  
"(A) serve as the primary organization within the United States government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to information network security threats;

"(B) ensure that appropriate United States entities have reasonable access to and receive all-source intelligence support necessary to execute the information network security threat intelligence activities of such entities and to perform independent, alternative analyses;

"(C) disseminate information network security threat analysis to the President, the relevant head of United States entities, and the relevant committees of Congress.

"(D) coordinate information network security intelligence activities of United States entities; and

"(E) conduct strategic intelligence planning and coordination for the United States government for—

“(i) planning against information network security threats;

“(ii) the implementation of defensive measures;

“(iii) the protection of United States government information systems and information networks.

"(4) Limitations.—The Office of Information Network Security shall—

"(A) have not more than 30 permanent positions;

"(B) in carrying out the primary missions of the Office of Information Network Security described in paragraph (3), may not—

"(i) augment staffing through detailees, assignees, or core contractor personnel; or

"(ii) enter into any personal service contracts to exceed the limitation under paragraph (1);

"(C) not be located in any building owned or operated by an element of the intelligence community.

“(d) Criminal sanctions.—

“(1) Prohibited activities.—Any person is guilty of an offense if that person is an officer, employee, or agent of the United States and—

"(A) knowingly and willfully uses any information network security threat indicator or defensive measure shared with the United States government, or any

personal information of, or information identifying, any person not directly related to a specific information network security threat and, under color of law—

"(i) the prevention, investigation, or criminal prosecution of any acts not directly related to a specific information network threat indicator; “

“(ii) any intelligence collection or analysis;

“(iii) any counterintelligence purposes; or

“(iv) any other surveillance purposes; or

“(B) negligently discloses or uses any information network security threat or defensive measure shared with the United States government knowing, having reason to know, or reasonably believing that the information network security threat indicator or defensive measure was shared with the United States government; or

“(C) knowingly, deliberately, or negligently fails to destroy, discloses, or otherwise misuses any personal information of, or information identifying, any person not directly related to a specific information network threat indicator;

“(2) Defenses.—It is a defense to a prosecution under paragraph (1) that the person was a law enforcement or investigative officer engaged in the course of that person's official duties and any usage of an information network threat Indicator shared with the United States government is authorized by and conducted pursuant to a search warrant or a court order of a court of competent jurisdiction.

“(3) Penalties.—An offense described in this section is punishable by a fine of not more than \$50,000 or imprisonment for not more than five years, or both.

“(4) Jurisdiction.—The United States shall have jurisdiction over an offense under this paragraph if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

"(e) Privacy and civil liberties.—

"(1) Guidelines of the Attorney General.—

"(A) Development and periodic review.—The Attorney General shall develop and periodically review guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of information network threat indicators by a United States entity obtained in accordance with this chapter.

"(B) Consultation requirement—When developing and reviewing the guidelines in subparagraph (A) the Attorney General shall consult with the heads of—

"(i) the Department of Defense;

"(ii) the Department of Energy;

"(iii) the Department of Homeland Security;

"(iv) the Department of Justice; and

"(v) the National Laboratories (as defined in section 15801 of title 42, United States Code (section 2 of the Energy Policy Act of 2005)).

"(2) Content.—The guidelines developed and reviewed under paragraph (1) shall, consistent with the need to protect information systems from information network security threats and mitigate information network security threats—

"(A) limit the impact on privacy and civil liberties by the United States government under this chapter, including guidelines to ensure that person information of, or information identifying, any person not directly related to an information network security threat is properly removed from information received, retained, used, or disseminated by a United States entity in accordance with this chapter;

"(B) limit the receipt, retention, use, and dissemination of information network threat indicators containing personal information of, or information identifying, any specific person, including by establishing

"(i) a process for the timely destruction of such information that is known or reasonably believe to not be directly related to an information network security threat;

"(ii) specific limitations on the length of any period in which an information network security threat is or may be retained; and

"(iii) a process to inform recipients that such indicators shall only be used for an information network security purpose, or face possible criminal sanctions under subsection (d) or section 3046c(d)(5) or any other civil or criminal law;

"(C) include requirements—

"(i) to safeguard information network threat indicators containing personal information of, or identifying any specific person from unauthorized access or acquisition:

"(ii) for appropriate administrative sanctions, criminal sanctions under subsection (d), or other measures, for activities by officers, employees, or agents of the United States government in contravention of such guidelines;

"(D) include procedures for notifying non-Federal entities if information received pursuant to this section is known or reasonably believed by a United States entity receiving such information not to constitute an information network threat indicator;

"(E) be consistent with any other applicable provisions of law and the fair information practice principles set forth in appendix A of the document entitled

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011; and

"(F) include steps that may be needed so that dissemination of information network threat indicators is consistent with the protection of classified information, and other sensitive national security and national defense information.

"(f) Information shared with or provided to the United States government. —

"(1) No waiver of privilege or protection. — The provision of an information network security threat indicator or defensive measure to the United States government under this chapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

"(2) Proprietary information. — Consistent with section 6 of the Foreign Intelligence Surveillance Reform Act of 2015, an information threat indicator or defensive measure provided by a non-Federal entity to the United States government under this chapter shall be considered the commercial, financial, and proprietary information of the non-Federal entity that is the originator of such information network security threat indicator or defensive measure when so designated by such non-Federal entity acting in accordance with the written authorization of the non-Federal entity that is the originator of such information network threat indicator or defensive measure.

"(3) Exemption from disclosure. — An information network threat indicator or defensive measure provided to the United States government under this chapter shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code (Freedom of Information Act), and any State, tribal, or local law requiring disclosure of such information or records.

"(4) Ex parte communications.—The provision of an information network threat indicator or defensive measure to the United States government under this chapter shall not be subject to a rule of any United States entity or United States judicial doctrine regarding ex parte communications with a decision—making official.

"(5) Disclosure, retention, and usage.—

"(A) Authorized activities.—An information network threat indicator or defensive measure provided to the United States government under this chapter may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of United States law, any department, agency, component, officer, employee, or agent of the United States government solely for—

"(i) an information network security purpose; or

"(ii) foreign intelligence surveillance purposes, upon an approved application for a warrant before a United States district court under section 1805d of title 50, United States Code (Foreign Intelligence Surveillance Act of 1978, as amended).

"(B) Prohibited activities.—An information network threat indicator or defensive measure provided to the United States government under this chapter shall not be disclosed to, retained by, or used by any United States entity for an use not permitted under subparagraph (A).

"(C) Privacy and civil liberties.—An information network threat indicator or defensive measure provided to the United States government under this chapter shall be retained, used, and disseminate by the United States government in accordance with—

"(i) the policies and procedures relating to the receipt of information network threat indicators and defensive measures by the United States government required by subsection (b); and

"(ii) the privacy and civil liberties guidelines required by subsection (e).

"(g) United States government liability for violations of privacy or civil liberties.

—

"(1) In general.—If a United States entity intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under subsection (b), or as required by subsection (e), the United States shall be liable to any person injured by such violation in an amount equal to the sum of—

"(A) the actual damages sustained by a result of such violation or \$1,000, whichever is greater; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(2) Venue.—An action to enforce liability created under this section may be brought in the district court of the United States in—

"(A) the district in which the complainant resides;

"(B) the district in which the principal place of business of the complainant is located;

"(C) the district in which the United States entity that violated such privacy and civil liberties guidelines is located; or

"(D) the District of Columbia.



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

“(3) Statute of limitations.—No action shall lie under this subsection unless such action is commenced not later than, the later of either—

“(A) two years after the date of the violation of the privacy and civil liberties guidelines issued by the Attorney General under subsection (b); or

“(B) one year after the discovery of the violation of the privacy and civil liberties guidelines issued by the Attorney General under subsection (b).

“(4) Exclusive cause of action.—A cause of action under this subsection shall be exclusive means available to a complainant seeking a remedy for a violation by a United States entity under section 3046 through 3046d.

“(g) Submittal to Congress.—

“(1) Submissions by the President.—The President shall submit the policies and procedures required in subsection (b)(1) to—

“(A) the Permanent Select Committee on Intelligence of the House of Representatives;

“(B) the Select Committee on Intelligence of the Senate; and

“(C) the Committee on the Judiciary of the Senate.

“(2) Submissions by the Director of National Intelligence—

“(A) Not later than 90 days after the enactment of this section, the Director of National Intelligence shall consult with the heads of—

“(i) the Department of Defense;

“(ii) the Department of Energy;

“(iii) the Department of Homeland Security;

“(iv) the Department of Justice;

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(v) the National Laboratories (as defined in section 15801 of title 42, United States Code (section 2 of the Energy Policy Act of 2005)); and

"(B) shall submit the procedures required by section 3046a of title 50, United States Code to—

"(A) the Permanent Select Committee on Intelligence of the House of Representatives;

"(B) the Select Committee on Intelligence of the Senate; and

"(C) the Committee on the Judiciary of the Senate.";

(3) Title 50, United States Code is amended after section 3046a, as inserted in paragraph (2), by inserting the following:

11 § 3046b. Authorization for private—security defensive monitoring.—

"(a) Authorization for private—sector defensive monitoring.—

"(1) In general.—Notwithstanding any other provision of law, a private entity may, for an information network security purpose, monitor—

"(A) an information system of such private entity;

"(B) an information system of a non-Federal entity, upon the written authorization of such non-Federal entity or such United States entity; and

"(C) information that is stored on, processed by or transiting an information system monitored by the private entity under this paragraph.

"(2) Construction.—Nothing in this subsection shall be construed to—

"(A) authorize the monitoring of an information system, or the use of any information such monitoring, other than provided in this chapter; or

"(B) authorize the United States government to conduct surveillance on any person; or

“(C) limit otherwise lawful activity.

“(b) Authorization for operation of defensive measures. —

“(1) In general. — Except as provided in paragraph (2) and notwithstanding any other provision of law, a private entity may, for an information network security purpose, operate a defensive measure that is applied and limited to—

“(A) an information system of such private entity to protect the rights or property of the private entity; and

“(B) an information system of a non-Federal entity or a United States entity for operation of such defensive measure to protect the rights or property of such private entity, non-Federal entity, or United States entity.

“(2) Limitation. — The authority provided in paragraph (1) does not include the intentional or reckless operation of any defensive measure that is designed or deployed to destroy, render unusable (in whole or in part), substantially harm, or initiate a new action, process or procedure on an information system or information stored on, processed by, or transiting such information system not belonging to—

“(A) the private entity operating such defensive measure; or

“(B) a non-Federal entity or a United States entity that has provided written authorization to that private entity for the operation of such defensive measure in accordance with this subsection.

“(c) Authorization for sharing or receiving information network threat indicators or defensive measures. —

“(1) In general— Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for an information network security purpose and consistent with the requirement under subsection (d)(2) to remove personal

information of, or information of, or information identifying, any person not directly related to an information network security threat and the protection of classified information—

"(A) share an information network threat indicator or defensive measure with any other non-Federal entity or a United States entity; and

"(B) receive an information network threat indicator or defensive measure from any other non-Federal entity or a United States entity.

"(2) Lawful restriction.—A non-Federal entity receiving an information network threat indicator or defensive measure from another non-Federal entity or a United States entity shall comply with otherwise lawful restrictions placed on the sharing or use of such information network threat indicator or defensive measure by the sharing non-Federal entity or United States entity.

"(3) Construction.—Nothing in this subsection shall be construed to—

"(A) authorize the sharing or receiving of an information network threat indicator or defensive measure other than as provided in this subsection;

"(B) authorize the sharing or receiving of classified information, or national defense information by or with any person not authorized to access such information;

"(C) prohibit any United States entity from engaging in formal or informal technical discussion regarding information network threat indicators or defensive measures with a non-Federal entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such an entity;

"(D) authorize the United States government to conduct surveillance measures on any person; or

"(E) limit otherwise lawful activity.

“(d) Protection and use of information. —

“(1) Security of information. — A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving an information network threat indicator or defensive measure under this section shall implement an appropriate security control to protect against unauthorized access to, or acquisition of, such information network threat indicator or defensive measure.

“(2) Removal of certain personal information. — A non-Federal entity sharing an information network threat indicator or defensive measure pursuant to this section shall, prior to such sharing, make reasonable efforts to—

“(A) review such information network threat indicator to assess whether such information network threat indicator contains any information that the non— Federal entity reasonably believes to be, or reasonably believes to contain—

“(i) any information that may reasonably identify any person not directly related to an information network security threat; or

“(ii) any personal information of, or belong to, any person not directly related to an information network security threat; or

“(B) implement a technical capability configured to remove any information contained within such indicator that the non-Federal entity reasonably believes to be, or reasonably believes to contain—

“(i) any information that may reasonably identify any person not directly related to an information security threat; or

“(ii) any personal information of, or belonging to, any person not directly related to an information security threat.

"(3) Use of information network threat indicator and defensive measures by non-Federal entities.—A non-Federal entity may, for an information network threat indicator

—

"(A) use an information network threat indicator, or defensive measure shared or received under this section to monitor or operate a defensive measure on—

"(i) an information system of another non-Federal entity or a United States entity; or

"(ii) an information system of another non-Federal entity or a United States entity upon the written authorization of that other non-Federal entity or that United States entity; and

"(B) otherwise use, retain, or further share such information network threat indicator or defensive measure subject to—

"(i) an otherwise lawful restriction placed by the sharing non-Federal entity or United States entity on such information network threat indicator or defensive measure; or

"(ii) an otherwise applicable provision of law.

"(4) Use of information network threat indicators by State, tribal, or local government.—

"(A) Law enforcement use.—

"(i) Prior written consent.—Except as provided in clause (ii), an information network threat indicator shared with a State, tribal, or local government under this section, may with the prior written consent of the non-Federal entity sharing such indicator, be used by a State, tribal, or local government for the limited purpose of

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

preventing, investigating, or prosecuting criminal acts directly related to such information network threat indicator.

"(ii) Oral consent—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent between both non-Federal entities.

"(iii) Construction.—Nothing in this subparagraph shall be construed to allow a State, tribal or local government to use any information from any shared information network threat indicators for—

"(I) the prevention, investigation, or prosecution of criminal or civil acts not directly related to such information network threat indicator, without probable cause for an immediate threat of death or serious bodily harm;

"(II) intelligence collection or analysis;

"(III) counterintelligence purposes; or

"(IV) any other surveillance purposes;

(B) Exemption from disclosure.—An information network threat indicator shared with a State, tribal, or local government under this section shall be—

“(i) deemed voluntarily shared information; and

“(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records, except as otherwise required by applicable State, tribal, or local law requiring disclosure in a criminal prosecution directly related to such information network threat indicator.

"(5) Criminal sanctions.—

"(A) Prohibited activities.—Any person is guilty of an offense if that person—

"(i) Intentionally uses any information network threat indicator shared under paragraph (3) or (4), or any personal information of, or information identifying, any person not directly related to a specific information network security threat, and engages in—

"(I) under color of law, any prevention, investigation, or prosecution of any criminal or civil acts not directly related to an information network indicator in paragraph (4);

"(II) under color of law, any intelligence collection or analysis;

"(III) under color of law, any counterintelligence purpose;

"(IV) under color of law, any surveillance purpose;

"(ii) discloses or uses any information network threat indicator shared under paragraph (3) or (4), knowing having reason to know, or reasonably believing that the information network security threat indicator or defensive measure share was shared under paragraph (3) or (4).

"(iii) knowingly, deliberately, or negligently, fails to destroy, discloses, or misuses any personal information of, or information identifying, a specific person not directly related to a specific information network security threat.

"(B) Defense.—It is a defense to a prosecution under subparagraph (A) that the person was a law enforcement or investigative officer engaged in the course of that person's official duties and the information network threat indicator shared under paragraph (3) or (4) was authorized by and conducted pursuant to a search warrant or a court order of a court of competent jurisdiction.



"(C) Penalties.—An offense described in this paragraph is punishable by a fine of not more than \$50,000 or imprisonment for not more than five years, or both.

"(D) Jurisdiction.—The United States shall have jurisdiction over an offense under this paragraph if the person committing the offense was an officer or employee of any State, tribal, or local government at the time the offense was committed.

"(e) Anti—trust exemption.—

"(1) In general—Except as provided elsewhere in this section, it shall not be considered a violation of any provision of antitrust laws for two or more private entities to exchange or provide an information network threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of an information network security threat, for any information network security purposes under this chapter.

"(2) Applicability.—Paragraph (1) shall not apply to information that is exchanged or assistance provided in order to assist with—

"(A) facilitating the prevention, investigation, or mitigation of an information network security threat to an information system or information that is stored on, processed by, or transiting an information system.

"(f) No right or benefit— The sharing of any information network threat indicator with a non-Federal entity under this section shall not create a right or benefit to similar information by such non-Federal entity or any non-Federal entity.

(4) Title 50, United States Code is amended after section 3046b, as inserted in paragraph (3), by inserting the following:

"§ 3046c. Report on information network security threats.

"(a) Report required.—Not later than 180 days after the date of the enactment of this section, the Director of National Intelligence, in coordination with other elements of the

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

intelligence community, shall submit a report on information network security threats, including information network attacks, theft, and data breaches to—

“(1) the Select Committee on Intelligence of the Senate; and

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

“(b) Contents.—The report required by subsection (a) shall include—

“(1) an assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding information network security threats, including information network attacks, theft, and data breaches directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, and whether and how such relationship could be improved;

“(2) a list and an assessment of the countries and nonstate actors that are primary threats of carrying out an information network security threat, including an information network attack, theft, and data breach directed against the United States and which threatens the United States national security interests and economy and intellectual property;

“(3) A description of the extent to which the capabilities of the United States government to respond to or prevent information network security threats, including information network attacks, theft, and data breaches directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or information network attacks, theft, and data breaches;

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"(4) an assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to information network security threats, including information network attacks, theft, and data breaches; and

"(5) an assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to information network security threats.

"(c) Form of report.—The report required by subsection (a) shall be made available in an unclassified form, with the option of a classified annex.

"(d) Intelligence community defined.—In this section, the term 'intelligence community' has the meaning given that term in section 3003 of title 50, United States Code (National Security Act of 1947).

(5) Title 50, United States Code is amended after section 3046c, as inserted in paragraph (4), by inserting the following:

"§ 3046d. Oversight of government activities related to information network security sharing.

"(a) Biennial report on implementation.—

"(1) in general.— Not later than one year after the date of enactment of this section, and not less frequently than once every two years thereafter, a detailed report concerning the implementation of section 3046 through 3046c of this chapter shall be jointly submitted—

"(A) by—

"(i) the heads of—

"(I) the Department of Defense;

"(II) the Department of Energy;

"(III) the Department of Homeland Security;

"(IV) the Department of Justice; and

"(ii) the Inspector General of—

"(I) the Department of Defense;

"(II) the Department of Energy;

"(III) the Department of Homeland Security;

"(IV) the Department of Justice; and

"(B) to—

"(i) the Permanent Select Committee on Intelligence of the House of Representatives;

"(ii) the Select Committee on Intelligence of the Senate; and

"(iii) the Committee of the Judiciary of the Senate.

"(2) Contents.—Each report submitted under paragraph (1) shall include—

"(A) an assessment of the sufficiency of the policies, procedures, and guidelines required by section 3046a in ensuring that information network threat indicators are shared effectively and responsibly within the United States government;

"(B) an evaluation of the effectiveness of the sharing in a reasonable period of time with other United States entities deemed to have a clear interest in information network security threat indicators under section 3046a(b), including any impediments to such sharing;

"(C) an assessment of the sufficiency of the procedure developed under section 3046a in ensuring that information network threat indicators in the possession of the United States government are shared in a timely and adequate manner with appropriate non-Federal entities, or, if appropriate, are made publicly available;

"(D) an assessment of whether information network threat indicators have been properly classified and an accounting of the number of security clearances authorized by the United States government for the implementation of section 3046 through 3046d of this chapter;

"(E) a review of the type of information network threat indicators shared with the United States government under section 3046 through 3046d of this chapter, including—

"(i) the degree to which such information may impact the privacy and civil liberties of any person;

"(ii) a quantitative and qualitative assessment of the impact of the sharing of such information network threat indicators with the United States government on privacy and civil liberties of any' person; and

"(iii) the adequacy of any steps taken by the United States government to reduce such impact;

"(F) a review of actions taken by the United States government based on information network threat indicators shared with the United States government under section 3046 through 3046d of this chapter;

"(G) a description of any significant violations of the requirements of section 3046 through 3046d of this chapter by the United States government; and

"(H) a summary of the number and type of non-Federal entities that

received classified information network threat indicators from the United States government under section 3046a of this chapter, and an evaluation of the risks and benefits of sharing such information network threat indicators.

"(3) Recommendations.—Each report submitted under paragraph (1) may include recommendations for improvements or modifications to the authorities and process under section 3046 through 3046d of this chapter.

"(4) Form of report.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

"(b) Reports on privacy and civil liberties.—

"(1) Biennial report from Privacy and Civil Liberties Oversight Board.— Not later than two years after the date of enactment of this section and not less frequently than once every two years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

"(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under section 3046 through 3046d of this chapter; and

"(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 3046a in addressing concerns relating to privacy and civil liberties.

"(2) Biennial report of inspectors general.—

"(A) in general—Not later than two years after the date of the enactment of this section and not less frequently than once every two years thereafter, a report on the receipt, use, and dissemination of information network threat indicators and defensive measures that have been shared with United States entities under section 3046 through 3046c of this chapter, shall be jointly submitted by the Inspector General of—

"(i) the Department of Defense;

"(ii) the Department of Energy;

"(iii) the Department of Homeland Security;

"(iv) the Department of Justice.

“(B) Contents. — Each report submitted under subparagraph (A) shall include—

“(i) a review of the types of information network threat indicators shared with United States entities;

“(ii) a review of the actions taken by United States entities as a result of the receipt of such information network threat indicators;

“(iii) a list of United States entities receiving such information network threat indicators; and

“(iv) a review of the sharing of such information network threat indicators among United States entities to identify inappropriate barriers to sharing information.

“(3) Recommendations. — Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements to the authorities under section 3046 through 3046c.

“(4) Form. — Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

(6) Title 50, United States Code, is amended in the table of contents after the item relating to section 3045 of title 50, United States Code, by inserting the following:

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

"§ 3046. Definitions for information network security sharing.

"§ 3046a. Sharing of information network threat indicators or defensive measures between the United States government with non-Federal entities.

"§ 3046b. Authorization for private sector defensive monitoring.

"§ 3046c. Report on information network security threats.

"§ 3046d. Oversight of government activities related to information network security sharing.

**(b) Amendments to the Foreign Intelligence Surveillance Act for Information network security threats.—**

(1) Title 50, United States Code, is amended after section 1805, as amended in section 2(a)(5) of this Act, by inserting the following:

"§ 1805d. Applications for Information network security threats.

"(a) Definitions.—As used in this section.—

"(1) the term 'defensive measure' has the meaning given the term in section 3046(3) of title 50, United States Code;

"(2) the term 'information network security purpose' has the meaning given the term in section 3046(5) of title 50, United States Code;

"(3) the term 'information network security threat' has the meaning given the term in section 3046(6) of title 50, United States Code; and

"(4) the term 'information network threat indicator' has the meaning given the term in section 3046(7) of title 50, United States Code.

"(b) Jurisdiction of the district court.—



“(1) In general— A judge of the United States shall have jurisdiction for the purpose of acquiring foreign intelligence information, to review an application and to enter an order approving the usage of—

“(A) an information network security threat;

“(B) an information network threat indicator;

“(C) a defensive measure provided to the United States government under chapter 44 of title 50, United States Code;

“(D) any personal information of, or information identifying, a specific person not directly related to a specific information network security threat under section 3046 through 3046d of title 50, United States Code.

“(E) an acquisition constituting electronic surveillance or the acquisition of stored electronic communications or stored electronic data related to the usage of—

“(i) an information network security threat;

“(ii) an information network threat indicator;

“(iii) a defensive measure provided to the United States government under chapter 44 of title 50, United States Code;

“(iv) any personal information of, or information identifying, a specific person not directly related to a specific information network security threat under section 3046 through 3046d of title 50, United States Code.

“(2) Limitation.—

“(A) If any information network security threat, information network threat indicator, or defensive measure targeted under this subsection is reasonably believed to involve any United States person during the effective period of an order issued pursuant

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

to subsection (d), an acquisition targeting such United States person under this section shall immediately cease, unless an application targeting such United States person is issued under a different provision of this chapter.

"(B) Nothing in this section shall be construed to limit the authority of the United States to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this chapter.

"(c) Application.—

"(1) In general.—Each application for an order under this section shall—

"(A) be made by a Federal officer in writing upon oath or affirmation to a judge of the United States;

"(B) require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section;

"(C) include—

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

(ii) the identity, if known, or a description of any United States person who is the target of an acquisition;

"(iii) a description of the specific—

"(I) information network security threat; “

(II) information network threat indicator;

"(III) defensive measure provided to the United States government; or

"(IV) personal information of, or information identifying, a specific person not directly related to a specific information network security threat or

information network threat indicator under section 3046 through 3046d of title 50, United States Code.

"(iv) a statement of the facts and circumstances relied upon to justify the applicant's belief that any United States person who is the target of an acquisition is—

"(I) a foreign power;

"(II) an agent of a foreign power; or

"(III) an officer or employee of a foreign power;

"(v) a statement of the proposed minimization procedures that meet the definition of minimization procedures under section 1801(h) or 821(4) chapter, as appropriate;

"(vi) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;

"(vii) a certification made by the Attorney General or an official specified in section 1804(a)(6) that—

"(I) the certifying official deems the information sought to be foreign intelligence information;

"(II) a significant purpose of the acquisition is to obtain foreign intelligence information:

"(III) such information cannot reasonably be obtained by normal investigative techniques;

"(IV) designates the type of foreign intelligence information being sought according to the categories described in section 1801(e); and

"(V) includes a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated, and such information cannot reasonably be obtained by normal investigative techniques;

"(vii) a summary statement of the means by which any acquisition will be conducted and whether physical entry is required to effect such acquisition:

"(viii) the identity of any electronic communication service provider necessary to effect any acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;

"(ix) a statement of the facts concerning any pervious applications that have been made to any judge of the United States, as specified in the application and the action taken on each pervious application, including—

"(I) any United States person specified in the application and the action taken on each pervious application;

"(II) information network security threat;

"(III) information network threat indicator;

"(IV) defensive measures provided to the United States government; or

"(V) personal information of, or information identifying, a specific person not directly related to a specific information network security threat or information network threat indicator under section 3046 through 3046d of title 50, United States Code; and

"(VI) a statement of the period of time for which the acquisition is required to be maintained provided that such period of time shall not exceed 90 days per application.

"(2) Other requirements of the Attorney General. — The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

"(3) Other requirements of the judge of the United States. — That judge of the United States may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (d)(1).

"(d) Order. —

"(1) Findings. — Upon an application made pursuant to subsection (c), that judge of the United States shall enter an ex parte order as requested or as modified by that judge of the United States approving the acquisition if that judge of the United States finds that—

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

"(B) on the basis of the facts submitted by the applicant, for any United States person who is the target of an acquisition, there is probable cause to believe that the target is—

"(i) a foreign power;

"(ii) an agent of a foreign power; or

"(iii) an officer or employee of a foreign power;

"(C) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate and

"(D) the application that has been filed contains all statements and certifications required by subsection (c) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (c)(1)(F)(v) and any other information furnished under subsection ©(3).

"(2) Probable cause.—

"(A) In determining whether or not probable cause exists for the purposes of paragraph (1)(B), a judge of the United States may consider the past activities of any target and facts and circumstances relating to current or future activities of such target.

1' (B) No United States person may be considered a foreign power, an agent of a foreign power, or an officer or employee of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

"(3) Review.—

"(A) Limitation on review.—Review by a judge of the United States shall be limited to that required to make the findings described in paragraph (1).

"(B) Review of probable cause.—If that judge of the United States determines that the facts submitted under subsection (c) are insufficient to establish probable cause under paragraph (1)(8), that judge of the United States shall enter an order so stating.

"(C) Review of minimization procedures.—If that judge of the United States determines that the proposed minimization procedures referred to in paragraph (1)

(C) do not meet the definition of minimization procedures under section 1801(h) or 1821(4) of this chapter, as appropriate, that judge of the United States shall enter an order so stating.

"(D) Review of certification. — If that judge of the United States determines that an application pursuant to subsection (c) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (C)(1)(F)(v) and any other information furnished under subsection (c)(3), that judge of the United States shall enter an order so stating.

"(E) Appeal of review. — The United States may appeal an order under subparagraph (B) through (D) pursuant to subsection (g).

"(F) Record. — For any determination made under subparagraph (B) through (D), that judge of the United States shall provide a written statement for the record of the reasons for the determination.

"(4) Specifications. — An order approving an acquisition under this subsection shall specify —

"(A) the identity, if known, or a description of any United States person who is the target of an acquisition identified or described in the application pursuant to subsection (c)(1)(C)(ii);

"(B) if provided in the application pursuant to (c)(1)(C)(vii), the nature

"(C) the nature and location of each of the facilities or places at which the acquisition will be directed;

"(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

"(E) the period of time during which the acquisition is approved.

"(5) Directives.—An order approving an acquisition under this subsection shall direct—

"(A) that the minimization procedures referred to in paragraph (l)(C), as approved or modified by that judge of the United States, be followed;

"(B) if applicable, an electronic communication service provider to provide the United States forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

"(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

"(D) if applicable, that the United States compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

(6) Duration.— An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90—day periods upon submission of renewal applications meeting the requirements of subsection(c).

"(7) Compliance.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, that judge of the United States may assess compliance with the minimization procedures referred to in paragraph



(1)(C) by reviewing the circumstances under which Information concerning United States persons was acquired, retained or disseminated.

"(e) Emergency authorization.—

“(1) Authority for emergency authorization.— Notwithstanding any other provision of this chapter, if the Attorney General may authorize an emergency acquisition if

—

“(A) a judge of the United States having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition;

“(B) an application in accordance with this section is made to a judge of the United States as soon as practicable, but not more than seven days after the Attorney General authorizes such acquisition; and

“(C) the Attorney General reasonably determines that—

“(i) an emergency situation exists with respect to any acquisition of foreign intelligence information for which an order may be obtained under subsection (d) before an order under that subsection can, with due diligence, be obtained; and

“(ii) that the factual basis for the issuance of an order under this section exists;

“(2) Minimization procedures.— If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (d)(1)(C) for the issuance of a judicial order be followed.

"(3) Termination of emergency authorization. — In the absence of a judicial order approving an acquisition under paragraph (1), such acquisition shall, at the earliest of the following, terminate—

"(A) when the information sought is obtained;

"(B) when the application for the order is denied; or

"(C) after the expiration of seven days from the time of authorization by the Attorney General.

"(4) Use of information. — If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person 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 an imminent threat of death or serious bodily harm to any person.

(f) Release from liability. — No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (d) or (e), respectively.

"(g) Appeal. —

"(1) Appeal to the courts of appeal.—

"(A) The United States may file a petition with the respective court of appeals for review of an order issued pursuant to subsection (c).

"(B) That court of appeals shall—

"(i) have jurisdiction to consider such petition; and

"(ii) provide a written statement for the record of the reasons for a decision under this paragraph.

"(2) Certiorari to the Supreme Court.—

"(A) The United States may file a petition for a writ of certiorari for review of a decision of the court of appeals issued under paragraph (1).

"(B) 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.

(2) Title 50, United States Code, is amended in the table of contents after the item relating to section 1805 of title 50, United States Code, by inserting the following item: "§ 1805d.

Applications for information network security threats.

(3) Section 1873 of title 50, United States Code, as amended in section 2(32) of this Act, is further amended in subsection (a)(1)(A) by striking "sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this chapter" and inserting "sections 1805, 1805d, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this chapter";

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

Subject: Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S.  
Congress

**Sec. 5. Effective Date.**

This Act, and the amendments made by this Act, shall be effective 180 days after the enactment of this Act.

**Sec. 6. Rule of Construction.** —

(a) **Definitions.** — As used in this section—

(1) the term "information network threat indicator" has the meaning given in section 3046(7) of title 50, United States Code, as inserted in section 4(a)(1) of this Act;

(2) the term "non-Federal entity" has the meaning given in section 3046(12) of title 50, United States Code, as inserted in section 4(a)(1) of this Act; and

(3) the term "United States entity" has the meaning given in section 3046(16) of title 50, United States Code, as inserted in section 4(a)(1) of this Act.

(b) **Otherwise lawful disclosures.** — Nothing in section 4 of this Act shall be construed—

(1) to limit or prohibit disclosures of communications, records, or other information including reporting of known or suspected criminal activity directly related to an imminent threat of death or serious bodily harm, by a non-Federal entity, to any other non-Federal entity or the United States government under this Act; or

(2) to limit or otherwise prohibit lawful use of such disclosures by any United States entity even when such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

(c) **Whistle-blower protections.** — Nothing in this Act shall be construed to prohibit or limit the disclosure of information protected under—

(1) section 2302(b)(8) of title 5, United States Code;

(2) section 7211 of title 5, United States Code;

(3) section 1034 of title 10, United States Code; (4) section 3234 of title 50, United States Code;

(d) **Protection of sources and methods.**—Nothing in this Act shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the United States government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified and national defense information;

(2) to affect the conduct of authorized law enforcement or intelligence activities;

(3) to modify the authority of a department of agency of the United States government to protect classified and national defense information and sources and methods and the national security of the United States.

(e) **Relationship to other laws.**—Nothing in this Act shall be construed to affect any requirement under any provision of law for an entity to provide information to the United States government.

(f) **Prohibited conduct.**—Nothing in this Act shall be construed to permit price—fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(g) **Information sharing relationships.**—Nothing in this Act shall be construed—

(1) to limit or modify an existing Information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the United States government; or

(4) to require the use of the capability and process within section 3046a(b) of title 50, United States Code.

(h) **Preservation of contractual obligation and rights.**—Nothing in this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entity and United States entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity and United States entity.

(i) **Anti-tasking restriction.**—Nothing in this Act shall be construed to permit the United States government—

(1) to require an entity to provide information to the United States government without a warrant or other statutory requirements;

(2) to condition the sharing of information network threat indicators with a non—Federal entity to the United States government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of an information network threat indicator to a United States entity.

(j) **No liability for non-participating.**—Nothing in this Act shall be construed to subject any non-Federal entity to liability for choosing not to engage in the voluntary activities authorized under section 4 of this Act.

(k) **Use and retention of Information.**—Nothing in section 4 of this Act shall be construed to author, or to modify any existing authority of, a department or agency of the United States government to retain or use any information shared under this Act for any other use other than permitted under this Act.

(l) **Federal preemption.**—

**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

(1) In general.—This Act shall supersede any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act.

(2) State of law enforcement.—Nothing in this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(m) **Regulator authority.**—Nothing in this Act shall be construed—

(1) to authorize the promulgation of any regulation not specifically authorized by this Act.

(2) to establish or limit any regulator authority not specifically established or limited under this Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(n) **Authority of the Secretary of Defense to respond to Information network attacks—**

Nothing in this Act shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military information network operation in response to a malicious information network activity carried out against the United States, any United States entity, or the interests of the United States by a foreign government or an organization sponsored by a foreign government or a terrorist organization.



**Subject:** Foreign Intelligence Surveillance Reform Act (FISRA)—Proposed Bill for U.S. Congress

**Sec 6.** No additional funds authorized.—No additional funds are allocated or authorized by this Act.

Respectfully submitted,

A handwritten signature in cursive script that reads "Chelsea Manning".

CHELSEA E. MANNING