109TH CONGRESS
2D SESSION

H. R. 5825

AN ACT

To update the Foreign Intelligence Surveillance Act of 1978.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Electronic Surveillance Modernization Act''.

SEC. 2. FISA DEFINITIONS.

(a) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is amended—

(1) in subparagraph (B), by striking ''; or'' and inserting '';''; and

(2) by adding at the end the following:

''(D) is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the official making the certification required by section 104(a)(7) deems such foreign intelligence information to be significant; or''.

(b) ELECTRONIC SURVEILLANCE.—Subsection (f) of such section is amended to read as follows:

''(f) 'Electronic surveillance' means—

''(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular known person who is reasonably believed to be in the United States under circumstances in which that person has a reasonable expectation of

privacy and a warrant would be required for law enforcement purposes; or

''(2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.''.

(c) MINIMIZATION PROCEDURES.—Subsection (h) of such section is amended—

(1) in paragraph (2), by striking ''importance;'' and inserting ''importance; and'';

(2) in paragraph (3), by striking ''; and'' and inserting ''.''; and

(3) by striking paragraph (4).

(d) WIRE COMMUNICATION AND SURVEILLANCE DEVICE.—Subsection (l) of such section is amended to read as follows:

''(l) 'Surveillance device' is a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that has already been acquired by the Federal Government by lawful means.''.

(e) CONTENTS.—Subsection (n) of such section is amended to read as follows:

''(n) 'Contents', when used with respect to a communication, includes any information concerning the substance, purport, or meaning of that communication.''.

SEC. 3. AUTHORIZATION FOR ELECTRONIC SURVEILLANCE AND OTHER ACQUISITIONS FOR FOREIGN INTELLIGENCE PURPOSES.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended by striking section 102 and inserting the following:

''AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

''SEC. 102. (a) IN GENERAL.—Notwithstanding any other law, the President, acting through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

''(1) the electronic surveillance is directed at—

''(A) the acquisition of the contents of communications of foreign powers, as defined in paragraph (1), (2), or (3) of section 101(a), or an agent of a foreign power, as defined in subparagraph (A) or (B) of section 101(b)(1); or

"(B) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a); and

"(2) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h);

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

"(b) MINIMIZATION PROCEDURES.—An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives

and the Select Committee on Intelligence of the Senate under the provisions of section 108(a).

''(c) SUBMISSION OF CERTIFICATION.—The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—

''(1) an application for a court order with respect to the surveillance is made under section 104; or

''(2) the certification is necessary to determine the legality of the surveillance under section 106(f).

''AUTHORIZATION FOR ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION

''SEC. 102A. (a) IN GENERAL.—Notwithstanding any other law, the President, acting through the Attorney General may, for periods of up to one year, authorize the acquisition of foreign intelligence information concerning a person reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that—

''(1) the acquisition does not constitute electronic surveillance;

''(2) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a wire or electronic communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to wire or electronic communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

''(3) a significant purpose of the acquisition is to obtain foreign intelligence information; and

''(4) the proposed minimization procedures with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

''(b) SPECIFIC PLACE NOT REQUIRED.—A certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

''(c) SUBMISSION OF CERTIFICATION.—The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of a certification made under subsection (a). Such certification shall be

maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless the certification is necessary to determine the legality of the acquisition under section 102B.

''(d) MINIMIZATION PROCEDURES.—An acquisition under this section may be conducted only in accordance with the certification of the Attorney General and the minimization procedures adopted by the Attorney General. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under section 108(a).

''DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE AND OTHER ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION

''SEC. 102B. (a) DIRECTIVE.—With respect to an authorization of electronic surveillance under section 102 or an authorization of an acquisition under section 102A, the Attorney General may direct a person to—

''(1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition of foreign intelligence information in such a manner as will protect the se-

crecy of the electronic surveillance or acquisition and produce a minimum of interference with the services that such person is providing to the target; and

''(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the electronic surveillance or acquisition or the aid furnished that such person wishes to maintain.

''(b) COMPENSATION.—The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (a).

''(c) FAILURE TO COMPLY.—In the case of a failure to comply with a directive issued pursuant to subsection (a), the Attorney General may petition the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person or entity to comply with the directive if it finds that the directive was issued in accordance with section 102(a) or 102A(a) and is otherwise lawful. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person or entity may be found.

''(d) REVIEW OF PETITIONS.—(1) IN GENERAL.—(A) CHALLENGE.—A person receiving a directive issued pursuant to subsection (a) may challenge the legality of that directive by filing a petition with the pool established under section 103(e)(1).

''(B) ASSIGNMENT OF JUDGE.—The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges serving in the pool established by section 103(e)(1). Not later than 24 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

''(2) STANDARD OF REVIEW.—A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the

directive, the judge shall affirm such directive, and order the recipient to comply with such directive.

''(3) DIRECTIVES NOT MODIFIED.—Any directive not explicitly modified or set aside under this subsection shall remain in full effect.

''(e) APPEALS.—The Government or a person receiving a directive reviewed pursuant to subsection (d) may file a petition with the court of review established under section 103(b) for review of the decision issued pursuant to subsection (d) not later than 7 days after the issuance of such decision. Such court of review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition by the Government or any person receiving such directive for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

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

''(g) SEALED PETITIONS.—All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

''(h) LIABILITY.—No cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

''(i) USE OF INFORMATION.—Information acquired pursuant to a directive by the Attorney General under this section concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by section 102(a) or 102A(a). No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this section shall lose its privileged character. No information from an electronic surveillance under section 102 or an acquisition pursuant to section 102A may be used or disclosed by Federal officers or employees except for lawful purposes.

''(j) USE IN LAW ENFORCEMENT.—No information acquired pursuant to this section shall be disclosed for law

enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived from such information, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

''(k) DISCLOSURE IN TRIAL.—If the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance conducted under section 102 or an acquisition authorized pursuant to section 102A, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to disclose or use such information.

''(l) DISCLOSURE IN STATE TRIALS.—If a State or political subdivision of a State intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a

State or a political subdivision of a State, against an aggrieved person, any information obtained or derived from an electronic surveillance authorized pursuant to section 102 or an acquisition authorized pursuant to section 102A, the State or political subdivision of such State shall notify the aggrieved person, the court, or other authority in which the information is to be disclosed or used and the Attorney General that the State or political subdivision intends to disclose or use such information.

''(m) MOTION TO EXCLUDE EVIDENCE.—(1) IN GENERAL.—Any person against whom evidence obtained or derived from an electronic surveillance authorized pursuant to section 102 or an acquisition authorized pursuant to section 102A is to be, or has been, used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance or such acquisition on the grounds that—

''(A) the information was unlawfully acquired; or

''(B) the electronic surveillance or acquisition was not properly made in conformity with an authorization under section 102(a) or 102A(a).

''(2) TIMING.—A person moving to suppress evidence under paragraph (1) shall make the motion to suppress the evidence before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

''(n) REVIEW OF MOTIONS.—If a court or other authority is notified pursuant to subsection (k) or (l), a motion is made pursuant to subsection (m), or a motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State—

''(1) to discover or obtain an Attorney General directive or other materials relating to an electronic surveillance authorized pursuant to section 102 or an acquisition authorized pursuant to section 102A, or

''(2) to discover, obtain, or suppress evidence or information obtained or derived from an electronic surveillance authorized pursuant to section 102 or an acquisition authorized pursuant to section 102A,

the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an

affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to such electronic surveillance or such acquisition as may be necessary to determine whether such electronic surveillance or such acquisition authorized under this section was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the directive or other materials relating to the acquisition only where such disclosure is necessary to make an accurate determination of the legality of the acquisition.

''(o) DETERMINATIONS.—If, pursuant to subsection (n), a United States district court determines that the acquisition authorized under this section was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived or otherwise grant the motion of the aggrieved person. If the court determines that such acquisition was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

''(p) BINDING ORDERS.—Orders granting motions or requests under subsection (m), decisions under this section

that an electronic surveillance or an acquisition was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of directives, orders, or other materials relating to such acquisition shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

''(q) COORDINATION.—(1) IN GENERAL.—Federal officers who acquire foreign intelligence information may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State, including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision, to coordinate efforts to investigate or protect against—

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

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

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

''(2) CERTIFICATION REQUIRED.—Coordination authorized under paragraph (1) shall not preclude the certification required by section 102(a) or 102A(a).

''(r) RETENTION OF DIRECTIVES AND ORDERS.—A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.''.

(b) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 102 the following:

''102A. Authorization for acquisition of foreign intelligence information.
''102B. Directives relating to electronic surveillance and other acquisitions of foreign intelligence information.''.

SEC. 4. JURISDICTION OF FISA COURT.

Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by adding at the end the following new subsection:

''(g) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under this section, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with

section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.''.

SEC. 5. APPLICATIONS FOR COURT ORDERS.

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

(1) in subsection (a)—

(A) in paragraph (6), by striking ''detailed description'' and inserting ''summary description'';

(B) in paragraph (7)—

(i) in the matter preceding subparagraph (A), by striking ''or officials designated'' and all that follows through ''consent of the Senate'' and inserting ''designated by the President to authorize electronic surveillance for foreign intelligence purposes'';

(ii) in subparagraph (C), by striking ''techniques;'' and inserting ''techniques; and'';

(iii) by striking subparagraph (D); and

(iv) by redesignating subparagraph (E) as subparagraph (D);

(C) in paragraph (8), by striking ''a statement of the means'' and inserting ''a summary statement of the means'';

(D) in paragraph (9)—

(i) by striking ''a statement'' and inserting ''a summary statement''; and

(ii) by striking ''application;'' and inserting ''application; and'';

(E) in paragraph (10), by striking ''thereafter; and'' and inserting ''thereafter.''; and

(F) by striking paragraph (11).

(2) by striking subsection (b);

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

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

SEC. 6. ISSUANCE OF AN ORDER.

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

(1) in subsection (a)—

(A) by striking paragraph (1); and

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

(2) in subsection (c)(1)—

(A) in subparagraph (D), by striking ''surveillance;'' and inserting ''surveillance; and'';

(B) in subparagraph (E), by striking ''approved; and'' and inserting ''approved.''; and

(C) by striking subparagraph (F);

(3) by striking subsection (d);

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

(5) in subsection (d), as redesignated by paragraph (4), by amending paragraph (2) to read as follows:

''(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not to exceed one year.'';

(6) in subsection (e), as redesignated by paragraph (4), to read as follows:

''(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency em-

ployment of electronic surveillance if the Attorney General—

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

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

''(3) informs a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

''(4) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not more than 168 hours after the Attorney General authorizes such surveillance.

If the Attorney General authorizes such emergency employment of electronic surveillance, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the in-

formation sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103.'';

(7) in subsection (h), as redesignated by paragraph (4)—

(A) by striking ''a wire or'' and inserting ''an''; and

(B) by striking ''physical search'' and inserting ''physical search or in response to a certification by the Attorney General or a designee of the Attorney General seeking information, facilities, or technical assistance from such person under section 102B''; and

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

''(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, the judge shall also authorize the installation and use of pen registers and trap and trace devices to acquire dialing, routing, addressing, and signaling information related to such communications and such dialing, routing, addressing, and signaling information shall not be subject to minimization procedures.''.

SEC. 7. USE OF INFORMATION.

Section 106(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(i)) is amended—

(1) by striking ''radio communication'' and inserting ''communication''; and

(2) by striking ''contents indicates'' and inserting ''contents contain significant foreign intelligence information or indicate''.

SEC. 8. CONGRESSIONAL OVERSIGHT.

(a) ELECTRONIC SURVEILLANCE UNDER FISA.—Section 108 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808) is amended—

(1) in subsection (a)(2)—

(A) in subparagraph (B), by striking ''and'' at the end;

(B) in subparagraph (C), by striking the period and inserting ''; and''; and

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

''(D) the authority under which the electronic surveillance is conducted.''; and

(2) by striking subsection (b) and inserting the following:

''(b) On a semiannual basis, the Attorney General additionally shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on electronic surveillance conducted without a court order.''.

(b) INTELLIGENCE ACTIVITIES.—The National Security Act of 1947 (50 U.S.C. 401 et seq.) is amended—

(1) in section 501 (50 U.S.C. 413)—

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

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

''(f) The Chair of each of the congressional intelligence committees, in consultation with the ranking member of the committee for which the person is Chair, may inform—

''(1) on a bipartisan basis, all members or any individual members of such committee, and

''(2) any essential staff of such committee,

of a report submitted under subsection (a)(1) or subsection (b) as such Chair considers necessary.'';

(2) in section 502 (50 U.S.C. 414), by adding at the end the following new subsection:

''(d) INFORMING OF COMMITTEE MEMBERS.—The Chair of each of the congressional intelligence committees, in consultation with the ranking member of the committee for which the person is Chair, may inform—

''(1) on a bipartisan basis, all members or any individual members of such committee, and

''(2) any essential staff of such committee,

of a report submitted under subsection (a) as such Chair considers necessary.''; and

(3) in section 503 (50 U.S.C. 415), by adding at the end the following new subsection:

''(g) The Chair of each of the congressional intelligence committees, in consultation with the ranking member of the committee for which the person is Chair, may inform—

''(1) on a bipartisan basis, all members or any individual members of such committee, and

''(2) any essential staff of such committee,

of a report submitted under subsection (b), (c), or (d) as such Chair considers necessary.''.

SEC. 9. INTERNATIONAL MOVEMENT OF TARGETS.

(a) ELECTRONIC SURVEILLANCE.—Section 105(d) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(d)), as redesignated by section 6(4), is amended by adding at the end the following new paragraph:

''(4) An order issued under this section shall remain in force during the authorized period of surveillance notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion.''.

(b) PHYSICAL SEARCH.—Section 304(d) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)) is amended by adding at the end the following new paragraph:

''(4) An order issued under this section shall remain in force during the authorized period of surveillance notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion.''.

SEC. 10. COMPLIANCE WITH COURT ORDERS AND ANTITERRORISM PROGRAMS.

(a) IN GENERAL.—Notwithstanding any other provision of law, and in addition to the immunities, privileges, and defenses provided by any other provision of law, no action, claim, or proceeding shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for an activity arising from or relating to the provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or assistance during the period of time beginning on September 11, 2001, and ending on the date that is 60 days after the date of the enactment of this Act, in connection with any alleged communications intelligence program that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, or would be intended to protect the

United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.

(b) JURISDICTION.—Any action, claim, or proceeding described in subsection (a) that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable pursuant to section 1441 of title 28, United States Code.

(c) DEFINITIONS.—In this section:

(1) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(2) PERSON.—The term ''person'' has the meaning given the term in section 2510(6) of title 18, United States Code.

SEC. 11. REPORT ON MINIMIZATION PROCEDURES.

(a) REPORT.—Not later than two years after the date of the enactment of this Act, and annually thereafter until December 31, 2009, the Director of the National Security Agency, in consultation with the Director of National Intelligence and the Attorney General, shall submit to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report on the effectiveness and use

of minimization procedures applied to information concerning United States persons acquired during the course of a communications activity conducted by the National Security Agency.

(b) REQUIREMENTS.—A report submitted under subsection (a) shall include—

(1) a description of the implementation, during the course of communications intelligence activities conducted by the National Security Agency, of procedures established to minimize the acquisition, retention, and dissemination of nonpublicly available information concerning United States persons;

(2) the number of significant violations, if any, of such minimization procedures during the 18 months following the effective date of this Act; and

(3) summary descriptions of such violations.

(c) RETENTION OF INFORMATION.—Information concerning United States persons shall not be retained solely for the purpose of complying with the reporting requirements of this section.

SEC. 12. AUTHORIZATION AFTER AN ARMED ATTACK.

(a) ELECTRONIC SURVEILLANCE.—Section 111 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1811) is amended by striking ''for a period not to exceed'' and all that follows and inserting the following:

''for a period not to exceed 90 days following an armed attack against the territory of the United States if the President submits to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate notification of the authorization under this section.''.

(b) PHYSICAL SEARCH.—Section 309 of such Act (50 U.S.C. 1829) is amended by striking ''for a period not to exceed'' and all that follows and inserting the following: ''for a period not to exceed 90 days following an armed attack against the territory of the United States if the President submits to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate notification of the authorization under this section.''.

SEC. 13. AUTHORIZATION OF ELECTRONIC SURVEILLANCE AFTER A TERRORIST ATTACK.

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

(1) by adding at the end of title I the following new section:

''AUTHORIZATION FOLLOWING A TERRORIST ATTACK UPON THE UNITED STATES

''SEC. 112. (a) IN GENERAL.—Notwithstanding any other provision of law, but subject to the provisions of this section, the President, acting through the Attorney Gen-

eral, may authorize electronic surveillance without an order under this title to acquire foreign intelligence information for a period not to exceed 90 days following a terrorist attack against the United States if the President submits a notification to the congressional intelligence committees and a judge having jurisdiction under section 103 that—

''(1) the United States has been the subject of a terrorist attack; and

''(2) identifies the terrorist organizations or affiliates of terrorist organizations believed to be responsible for the terrorist attack.

''(b) SUBSEQUENT CERTIFICATIONS.—At the end of the 90-day period described in subsection (a), and every 90 days thereafter, the President may submit a subsequent certification to the congressional intelligence committees and a judge having jurisdiction under section 103 that the circumstances of the terrorist attack for which the President submitted a certification under subsection (a) require the President to continue the authorization of electronic surveillance under this section for an additional 90 days. The President shall be authorized to conduct electronic surveillance under this section for an additional 90 days after each such subsequent certification.

''(c) ELECTRONIC SURVEILLANCE OF INDIVIDUALS.—The President, or an official designated by the President to authorize electronic surveillance, may only conduct electronic surveillance of a person under this section if the President or such official determines that—

''(1) there is a reasonable belief that such person is communicating with a terrorist organization or an affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack; and

''(2) the information obtained from the electronic surveillance may be foreign intelligence information.

''(d) MINIMIZATION PROCEDURES.—The President may not authorize electronic surveillance under this section until the Attorney General approves minimization procedures for electronic surveillance conducted under this section.

''(e) UNITED STATES PERSONS.—Notwithstanding subsection (a) or (b), the President may not authorize electronic surveillance of a United States person under this section without an order under this title for a period of more than 60 days unless the President, acting through the Attorney General, submits a certification to the congressional intelligence committees that—

''(1) the continued electronic surveillance of the United States person is vital to the national security of the United States;

''(2) describes the circumstances that have prevented the Attorney General from obtaining an order under this title for continued surveillance;

''(3) describes the reasons for believing the United States person is affiliated with or in communication with a terrorist organization or affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack; and

''(4) describes the foreign intelligence information derived from the electronic surveillance conducted under this section.

''(f) USE OF INFORMATION.—Information obtained pursuant to electronic surveillance under this subsection may be used to obtain an order authorizing subsequent electronic surveillance under this title.

''(g) REPORTS.—Not later than 14 days after the date on which the President submits a certification under subsection (a), and every 30 days thereafter until the President ceases to authorize electronic surveillance under subsection (a) or (b), the President shall submit to the congressional intelligence committees a report on the elec-

tronic surveillance conducted under this section, including—

''(1) a description of each target of electronic surveillance under this section; and

''(2) the basis for believing that each target is in communication with a terrorist organization or an affiliate of a terrorist organization.

''(h) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, the term 'congressional intelligence committees' means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.''; and

(2) in the table of contents in the first section, by inserting after the item relating to section 111 the following new item:

''Sec. 112. Authorization following a terrorist attack upon the United States.''.

SEC. 14. AUTHORIZATION OF ELECTRONIC SURVEILLANCE DUE TO IMMINENT THREAT.

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

(1) by adding at the end of title I the following new section:

''AUTHORIZATION DUE TO IMMINENT THREAT

''SEC. 113. (a) IN GENERAL.—Notwithstanding any other provision of law, but subject to the provisions of this section, the President, acting through the Attorney Gen-

eral, may authorize electronic surveillance without an order under this title to acquire foreign intelligence information for a period not to exceed 90 days if the President submits to the congressional leadership, the congressional intelligence committees, and the Foreign Intelligence Surveillance Court a written notification that the President has determined that there exists an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States. Such notification—

''(1) shall be submitted as soon as practicable, but in no case later than 5 days after the date on which the President authorizes electronic surveillance under this section;

''(2) shall specify the entity responsible for the threat and any affiliates of the entity;

''(3) shall state the reason to believe that the threat of imminent attack exists;

''(4) shall state the reason the President needs broader authority to conduct electronic surveillance in the United States as a result of the threat of imminent attack;

''(5) shall include a description of the foreign intelligence information that will be collected and the

means that will be used to collect such foreign intelligence information; and

''(6) may be submitted in classified form.

''(b) SUBSEQUENT CERTIFICATIONS.—At the end of the 90-day period described in subsection (a), and every 90 days thereafter, the President may submit a subsequent written notification to the congressional leadership, the congressional intelligence committees, the other relevant committees, and the Foreign Intelligence Surveillance Court that the circumstances of the threat for which the President submitted a written notification under subsection (a) require the President to continue the authorization of electronic surveillance under this section for an additional 90 days. The President shall be authorized to conduct electronic surveillance under this section for an additional 90 days after each such subsequent written notification.

''(c) ELECTRONIC SURVEILLANCE OF INDIVIDUALS.—The President, or an official designated by the President to authorize electronic surveillance, may only conduct electronic surveillance of a person under this section if the President or such official determines that—

''(1) there is a reasonable belief that such person is communicating with an entity or an affiliate

of an entity that is reasonably believed to be responsible for imminent threat of attack; and

''(2) the information obtained from the electronic surveillance may be foreign intelligence information.

''(d) MINIMIZATION PROCEDURES.—The President may not authorize electronic surveillance under this section until the Attorney General approves minimization procedures for electronic surveillance conducted under this section.

''(e) UNITED STATES PERSONS.—Notwithstanding subsections (a) and (b), the President may not authorize electronic surveillance of a United States person under this section without an order under this title for a period of more than 60 days unless the President, acting through the Attorney General, submits a certification to the congressional intelligence committees that—

''(1) the continued electronic surveillance of the United States person is vital to the national security of the United States;

''(2) describes the circumstances that have prevented the Attorney General from obtaining an order under this title for continued surveillance;

''(3) describes the reasons for believing the United States person is affiliated with or in commu-

nication with an entity or an affiliate of an entity that is reasonably believed to be responsible for imminent threat of attack; and

''(4) describes the foreign intelligence information derived from the electronic surveillance conducted under this section.

''(f) USE OF INFORMATION.—Information obtained pursuant to electronic surveillance under this subsection may be used to obtain an order authorizing subsequent electronic surveillance under this title.

''(g) DEFINITIONS.—In this section:

''(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

''(2) CONGRESSIONAL LEADERSHIP.—The term 'congressional leadership' means the Speaker and minority leader of the House of Representatives and the majority leader and minority leader of the Senate.

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

''(4) OTHER RELEVANT COMMITTEES.—The term 'other relevant committees' means the Committees on Appropriations, the Committees on Armed Services, and the Committees on the Judiciary of the House of Representatives and the Senate.''; and

(2) in the table of contents in the first section, by inserting after the item relating to section 112, as added by section 13(2), the following new item:

''Sec. 113. Authorization due to imminent threat.''.

SEC. 15. TECHNICAL AND CONFORMING AMENDMENTS.

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

(1) in section 105(a)(4), as redesignated by section 6(1)(B)—

(A) by striking ''104(a)(7)(E)'' and inserting ''104(a)(7)(D)''; and

(B) by striking ''104(d)'' and inserting ''104(c)'';

(2) in section 106(j), in the matter preceding paragraph (1), by striking ''105(e)'' and inserting ''105(d)''; and

(3) in section 108(a)(2)(C), by striking "105(f)" and inserting "105(e)".

Passed the House of Representatives September 28, 2006.

Attest:

Clerk.

109TH CONGRESS
2D SESSION

H. R. 5825

AN ACT

To update the Foreign Intelligence Surveillance Act of 1978.