109TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 109–680
Part 1

ELECTRONIC SURVEILLANCE MODERNIZATION ACT

SEPTEMBER 25, 2006.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany H.R. 5825]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 5825) to update the Foreign Intelligence Surveillance Act of 1978, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

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 new subparagraph:

"(D) possesses or is reasonably expected to transmit or receive foreign intelligence information while in the United States; 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 a surveillance device for the intentional collection of information relating to a person who is reasonably believed to be in the United States by intentionally targeting that person, under circumstances in which the 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, without the consent of a party to the 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 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 ".";

(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) PHYSICAL SEARCH.—Section 301(5) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(5)) is amended by striking "Act, or (B)" and inserting "Act, (B) activities described in section 102(b) of this Act, or (C)".

SEC. 3. AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES.

Section 102 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A)—

(i) in clause (i), by striking "transmitted by means of" and all that follows and inserting "of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a), or an agent of a foreign power, as defined in section 101(b)(1); or"; and

(ii) in clause (ii), by striking "or (3);" and inserting "or (3); and";

(B) by striking subparagraph (B); and

(C) by redesignating subparagraph (C) as subparagraph (B);

(2) by striking subsection (a)(4);

(3) in subsection (b), to read as follows:

"(b)(1) The Attorney General may require, by written certification, any person with authorized access to electronic communications or equipment used to transmit or store electronic communications to provide information, facilities, or technical assistance—

"(A) necessary to accomplish electronic surveillance authorized under subsection (a); or

"(B) to an official designated by the President for a period of up to one year, provided the Attorney General certifies in writing, under oath, that the provision of the information, facilities, or technical assistance does not constitute electronic surveillance.

"(2) The Attorney General may require a person providing information, facilities, or technical assistance under paragraph (1) to—

"(A) provide the information, facilities, or technical assistance in such a manner as will protect the secrecy of the provision of such information, facilities, or technical assistance and produce a minimum of interference with the services that such person is providing the customers of such person; and

"(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning such electronic surveillance or the information, facilities, or technical assistance provided which such person wishes to retain.

"(3) The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or technical assistance pursuant to paragraph (1).";

and

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

"(c) Notwithstanding any other provision of law, the President may designate an official who may authorize electronic surveillance of international radio communications of a diplomat or diplomatic mission or post of the government of a foreign country in the United States in accordance with procedures approved by the Attorney General.".

SEC. 4. APPLICATIONS FOR COURT ORDERS.

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

(1) in subsection (a)—

(A) by striking paragraphs (6), (9), and (11);

(B) by redesignating paragraphs (7), (8), and (10) as paragraphs (6), (7), and (8), respectively;

(C) in paragraph (6), as redesignated by subparagraph (B)—

(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 subparagraphs (D) and (E) and inserting the following:

"(D) including a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated;";

(D) in paragraph (7), as redesignated by subparagraph (B)—

(i) by striking "a statement of the means by which the surveillance will be effected and"; and

(ii) by adding "and" at the end; and

(E) in paragraph (8), as redesignated by subparagraph (B), by striking "; and" and inserting a period;

(2) by striking subsection (b); and

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

SEC. 5. 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), (3), (4), and (5) as paragraphs (1), (2), (3), and (4), respectively;

(2) in subsection (c)(1)—

(A) in subparagraph (B), by striking "known;" and inserting "known; and";

(B) by striking subparagraphs (C), (D), and (F);

(C) by redesignating subparagraph (E) as subparagraph (C); and

(D) in subparagraph (C), as redesignated by subparagraph (C), by striking "approved; and" and inserting "approved.";

(3) by striking subsection (d);

(4) by redesignating subsections (e), (f), (g), (h), and (i) as subsections (d), (e), (f), (g), and (h), respectively;

(5) in subsection (d), as redesignated by paragraph (4)—

(A) in paragraph (1), by striking "for the period necessary" and all that follows and insert "for a period not to exceed one year."; and

(B) in paragraph (2), by striking "original order, except that" and all that follows and inserting "original order 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 employment 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 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 120 hours after the official 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 information sought is obtained, when the application for the order is denied, or after the expiration of 120 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."; and

(7) in subsection (h), as redesignated by paragraph (4), by striking "assistance in accordance with a court order" and all that follows and inserting "assistance—

"(1) in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search; or

"(2) 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 that does not constitute electronic surveillance.".

SEC. 6. 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. 7. 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 60 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 60 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. 8. 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 General, may authorize electronic surveillance without an order under this title to acquire foreign intelligence information for a period not to exceed 45 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 45-day period described in subsection (a), and every 45 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 45 days. The President shall be authorized to conduct electronic surveillance under this section for an additional 45 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 (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 90 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 electronic 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. 9. 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 General, 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 communication 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 8(2), the following new item:

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

SEC. 10. CONGRESSIONAL OVERSIGHT.

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

(1) in paragraph (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 adding at the end the following new paragraph:

"(3) Each report submitted under this subsection shall include reports 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. 11. TECHNICAL AND CONFORMING AMENDMENTS.

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

(1) in section 102(a)(3)(A), by striking "sections 101(h)(4) and" and inserting "section";

(2) in section 105(a)(4), as redesignated by section 5(1)(B)—

(A) by striking "104(a)(7)(E)" and inserting "104(a)(6)(D)"; and

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

(3) in section 106—

(A) in subsection (j) in the matter preceding paragraph (1), by striking "105(e)" and inserting "105(d)"; and

(B) in subsection (k)(2), by striking "104(a)(7)(B)" and inserting "104(a)(6)(B)"; and

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

PURPOSE

The purpose of H.R. 5825 is to modernize the Foreign Intelligence Surveillance Act, to strengthen oversight of the executive branch concerning electronic surveillance and intelligence, and to provide clear electronic surveillance authority to the nation's intelligence agencies in the event of a terrorist attack, armed attack, or imminent threat against the United States.

COMMITTEE STATEMENT AND VIEWS

A. Background and need for legislation

The Foreign Intelligence Surveillance Act ("FISA") provides the legal framework for collecting specified types of foreign intelligence information within the United States. The current legal and technical framework relative to FISA was constructed in 1978. The complexity, variety and means of communications technology has since mushroomed exponentially and globally—but the structure of

our surveillance laws has remained hidebound around the technology of generations-old wired telephones.

The Committee received testimony that the current provisions of FISA are "dangerously obsolete". This bill modernizes the law in a number of critical respects. It updates FISA to make it technology neutral, and neutral as to the means of communication. It streamlines the surveillance approval process to keep the focus on gaining knowledge of those who would do harm to the United States while protecting the civil liberties of average Americans. It gives our intelligence personnel the necessary tools to help detect and prevent acts of terrorism, and to respond to armed attacks and terrorist attacks. As reported, the bill also ensures that adequate authority exists to conduct necessary electronic surveillance when a threat of imminent attack exists.

H.R. 5825 also enhances congressional and judicial oversight of U.S. government electronic surveillance activities to ensure that activities conducted under both FISA and the authorities provided in the bill will be utilized by the President only with the knowledge and coordination of the other branches of government. More broadly than just FISA, the bill as reported also addresses fundamental separation of powers concerns expressed by members of the Committee through amendments to the National Security Act by providing express authority for the Chairmen of the congressional intelligence Committees to broaden reporting on sensitive issues to additional members of the Committee at his or her discretion on a bipartisan basis in the necessary circumstances.

This bill enhances the overall authorities of our nation to act as a whole to protect itself in times of war and heightened threat of attack—both terrorist and otherwise.

B. Legislation

The bill contains provisions relating to modernization of the Foreign Intelligence Surveillance Act, additional authorization to conduct limited electronic surveillance in specifically defined emergency circumstances with enhanced reporting to Congress and the Judiciary, and to enhance congressional oversight of both electronic surveillance and other intelligence and intelligence-related activities of the United States.

1. FISA modernization

Sections two through six of the bill, further detailed in the following section-by-section analysis, contain provisions intended to modernize the Foreign Intelligence Surveillance Act. The bill updates the definition of electronic surveillance contained in the statute to make it technology neutral and to ensure that the FISA process is directed to circumstances where a reasonable expectation of privacy exists and a warrant would be required for law enforcement purposes. The bill also would modernize and simplify the process of getting a FISA warrant in order to focus resources on protecting the civil liberties of Americans.

2. Enhanced authorities

Sections seven through nine of the reported bill provide clear authority to United States intelligence agencies in the event of an armed attack, terrorist attack, or threat of imminent attack on the

United States. These provisions include limits on the type of surveillance that may be conducted, and provide for enhanced accountability.

Section seven expands the authority in current law to conduct electronic surveillance following an armed attack against the United States to a period of sixty days, and adds a requirement that the President submit notification of any authorization under this authority to the congressional intelligence committees.

Section eight provides authority to conduct specified electronic surveillance after a terrorist attack on the United States, on notification to the congressional intelligence committees and a judge of the FISA court. The authority is limited to renewable 45 day periods, and the authorization is limited to electronic surveillance of persons when the President determines there is a reasonable belief that a 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 that the information obtained may be foreign intelligence information. Additional constraints are provided with respect to electronic surveillance of United States persons.

Section nine provides authority to conduct specified electronic surveillance when 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, on notification to the congressional intelligence committees and the FISA court. The authority is limited to renewable 90 day periods, and additional congressional committees must be notified if the authority is renewed. The authorization is limited to electronic surveillance of persons when the President determines there is a reasonable belief that a person is communicating with the entity or an affiliate reasonably believed to be responsible for the imminent threat of attack, and that the information obtained may be foreign intelligence information. Additional constraints are provided with respect to electronic surveillance of United States persons.

3. Enhanced Congressional oversight

The bill enhances congressional oversight not only of electronic surveillance, but also more generally of intelligence and intelligence-related activities of the United States Government. Each of the enhanced authorities provided in the bill includes specific and detailed requirements for reporting to Congress. In addition, Section ten of the bill requires the FISA semi-annual report to include information regarding the authority under which electronic surveillance is conducted, and provides for reporting on any electronic surveillance conducted without a court order.

The bill also makes significant amendments to the National Security Act of 1947 that would authorize the Chair of each of the congressional intelligence committees to inform any or all other members and essential staff of each Committee of reporting of intelligence activities received under that Act, on a bipartisan basis, as such Chair considers necessary in his or her discretion.

COMMITTEE HEARINGS

The Committee held two public hearings with respect to modernization of the Foreign Intelligence Surveillance Act. On July 19,

2006, the Committee received testimony from Judge Richard A. Posner; Mr. Kim Taipale of the Center for Advanced Studies in Science and Technology Policy; Mr. Michael Greco of the American Bar Association; and Mr. James Dempsey of the Center for Democracy and Technology. On July 27, 2006, the Committee received testimony from Representative Heather Wilson regarding H.R. 5825; from Representative John Conyers regarding H.R. 5371; and from Representative Adam Schiff and Representative Jeff Flake regarding H.R. 4976.

COMMITTEE CONSIDERATION AND ROLLCALL VOTES

On September 20, 2006, the Committee met in open session and ordered the bill H.R. 5825 favorably reported, as amended.

Ms. Wilson offered an amendment in the nature of a substitute to H.R. 5825, which was considered as base text by unanimous consent. The contents of the amendment in the nature of a substitute are described in the Section-by-Section analysis and the Explanation of Amendment. The Committee considered the following amendments:

Ms. Harman offered an amendment in the nature of a substitute containing the text of H.R. 5371, the "LISTEN Act". It was not agreed to by a record vote of 9 ayes to 10 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Mr. Gallegly, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi.

Ms. Eshoo offered an amendment making modifications to the definition of electronic surveillance. It was not agreed to by a record vote of 9 ayes to 10 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Mr. Gallegly, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi.

Mr. Hastings offered an amendment relating to acquisition of communications among foreign parties. It was not agreed to by a record vote of 8 ayes to 11 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Mr. Gallegly, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi, Mr. Issa.

Mr. Holt offered an amendment inserting a finding that in passing the Foreign Intelligence Surveillance Act, Congress expressly stated that FISA and specified provisions of title 18, United States Code, were the exclusive means by which surveillance can be conducted in the United States. It was not agreed to by a record vote of 8 ayes to 9 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi.

Mr. Reyes offered an amendment inserting a finding that the Authorization for Use of Military Force (Public Law 107–40) does not constitute legal authorization for electronic surveillance not authorized by specified provisions of Title 18, United States Code, or the Foreign Intelligence Surveillance Act. It was not agreed to by a record vote of 8 ayes to 9 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi.

Mr. Holt offered an amendment inserting a finding that in passing the Foreign Intelligence Surveillance Act, Congress expressly stated that FISA and specified provisions of title 18, United States Code, were the exclusive means by which electronic surveillance can be conducted in the United States. It was not agreed to by a record vote of 8 ayes to 9 noes:

Voting aye: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Mr. Holt, Mr. Ruppersberger, Mr. Tierney.

Voting no: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi

The Committee then adopted the amendment in the nature of a substitute by a record vote of 9 ayes to 8 noes:

Voting aye: Mr. Hoekstra (Chairman), Mr. LaHood, Mr. Everett, Ms. Wilson, Ms. Davis, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Renzi.

Voting no: Ms. Harman, Mr. Hastings, Mr. Reyes, Mr. Boswell, Mr. Cramer, Mr. Holt, Mr. Ruppersberger, Mr. Tierney

By voice vote, the Committee adopted a motion by the Chairman to favorably report the bill H.R. 5825 to the House, as amended.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF THE AMENDMENT

The provisions of the bill are as follows:

Section 1—Short title

Section 1 contains the short title for the bill.

Section 2—FISA definitions

Section 2 would update the definition of electronic surveillance. This change would update the law to take into account significant changes in technology since the enactment of the Foreign Intelligence Surveillance Act ("FISA"). This section would remove the current distinction between treatment of "wire" and "radio" communications, and use a technology-neutral definition of electronic surveillance. This section also provides protection for persons with a reasonable expectation of privacy if both the sender and all intended recipients are located within the United States.

Section 3—Authorization for electronic surveillance for foreign intelligence purposes

Section 3 would modernize the law by including providers of any electronic communication service, landlord, custodian, or other person who has access to electronic communications. This section updates the current "common carrier" definition.

Sections 4 and 5—Applications for court orders/issuance of an order

Sections 4 and 5 would simplify the process for developing information to get approval of a FISA warrant. This section would reduce the volume of material required for a FISA application, including minimizing the detailed description of the nature of foreign intelligence information sought and the detailed descriptions of the intended method of collection. The FISA application should focus on probable cause for a warrant rather than technical details about the means of collection. Current protections and minimization procedures will remain in place to protect unintended targets. In the event of an emergency employment of electronic surveillance, the Attorney General would have up to five days to file for an emergency application.

Section 6—Use of information

Section 6 clarifies and makes conforming changes with respect to previous sections and FISA.

Section 7—Authorization after an armed attack

Section 7 updates the current FISA provisions for electronic surveillance to provide clear authority for U.S. intelligence agencies to conduct electronic surveillance in the event of an armed attack on the United States. The President, through the Attorney General, is authorized to collect electronic surveillance without a court order to acquire foreign intelligence information for a period not to exceed 60 days following an armed attack against the territory of the United States. The current statute allows for 15 days after a declaration of war by the Congress. Notification to the House Permanent Select Committee on Intelligence ("HPSCI") and Senate Select Committee on Intelligence ("SSCI") is required.

Section 8—Authorization of electronic surveillance after a terrorist attack

Section 8 governs electronic surveillance after a terrorist attack. The President, acting through the Attorney General, would have the authority to authorize electronic surveillance to acquire foreign intelligence information without an order when the terrorist organizations and their affiliates responsible for the attack have been identified and notified to the Congress and the FISA court, when there is a reasonable belief that the target is communicating with a terrorist organization, for a period not to exceed 45 days following a terrorist attack against the U.S. Notification to the HPSCI and SSCI and to the FISA court is required. The President may submit a subsequent certification to Congress which would allow for an additional 45 days of electronic surveillance.

Section 9—Authorization of electronic surveillance after threat of imminent attack

Section 9 allows the President to authorize electronic surveillance when there exists an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States when the entities and their affiliates responsible for the threat have been identified and notified to the Congress and the FISA court, when there is a reasonable belief that the target is communicating with those entities and affiliates, for a period not to exceed 90 days. The President must submit notification to Congress as soon as practicable, but not later than five days after the authorization. The President may submit subsequent certifications to Congress which would allow for additional 90 day periods of surveillance, with notification to additional congressional committees.

Section 10—Congressional oversight

Section 10 of the Act would strengthen congressional oversight by amending current law to provide authority to the Chairman of each of the Intelligence Committees to notify all members or any individual members of the Committees, on a bipartisan basis and as the Chair considers necessary, of reporting of intelligence activities received under the National Security Act.

Section 11—Technical and conforming amendments

Section 11 makes technical clarifications and conforming amendments to FISA.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held two open hearings, receiving testimony from outside experts, interested citizens, and Members of Congress. The Committee reports that the findings and recommendations of the Committee are reflected in the bill, as reported by the Committee.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with Clause (3)(c) of House rule XIII, the Committee's performance goals and objectives are reflected in the descriptive portions of this report.

CONSTITUTIONAL AUTHORITY STATEMENT

The intelligence and intelligence-related activities of the United States government are carried out to support the national security interests of the United States.

Article 1, section 8 of the Constitution of the United States provides, in pertinent part, that 'Congress shall have power * * * to pay the debts and provide for the common defense and general welfare of the United States; * * *'; and 'to make all laws which shall be necessary and proper for carrying into execution * * * all other powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.'

UNFUNDED MANDATE STATEMENT

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

APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that the legislation does not address the terms of conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

EARMARKS STATEMENT

The reported bill contains no earmarks, as defined in H. Res. 1000.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of 3(c)(3) of rule XIII of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 5825 from the Director of the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 25, 2006.

Hon. PETER HOEKSTRA,
Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5825, the Electronic Surveillance Modernization Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 5825—Electronic Surveillance Modernization Act

Summary: H.R. 5825 would modify the rules and procedures the government must follow to use electronic surveillance programs in the investigation of international terrorism. The bill would amend the definition of electronic surveillance under the Foreign Intelligence Surveillance Act (FISA) to remove the current distinction between treatment of wire and radio communications, and to focus FISA protections on domestic communications.

The bill also would expand the ability of the government to conduct electronic surveillance without warrant when:

- The target of the surveillance is an agent of a foreign power;
- There has been an armed attack against the territory of the United States;
- There has been a terrorist attack against the United States; or
- There exists an imminent threat of attack likely of cause death, serious injury, or substantial economic damage to the United States.

H.R. 5825 would also authorize the Attorney General, after obtaining the certification required under the bill, to require any U.S. citizen, legal alien, or organization with access to electronic communications to provide the government with all assistance necessary to conduct electronic surveillance and to acquire foreign intelligence information. Under current law, the Attorney General may direct a "common carrier" to provide such assistance with electronic surveillance. Thus, implementing H.R. 5825 could expand the number of entities that may be required to provide assistance to the government when it conducts electronic surveillance.

The bill would also make a number of changes that could reduce the volume of material required for a FISA application, including minimizing the detailed descriptions of both the nature of the foreign intelligence information sought and the intended method of collection.

CBO has no basis for predicting how the volume or type of surveillance would be changed if H.R. 5825 were enacted. Furthermore, information regarding surveillance techniques and their associated costs is classified. For these reasons, CBO cannot estimate the impact on the federal budget of implementing H.R. 5825.

Section 4 of the Unfunded Mandates Reform Act (UMRA) excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that section 9 of this bill, which would authorize certain electronic surveillance without a warrant due to an imminent threat of attack, falls under that exclusion; we have not reviewed it for intergovernmental or private-sector mandates.

One of the other provisions of H.R. 5825 contains an intergovernmental mandate, but CBO estimates that costs to state and local governments would fall well below the annual threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 5825 contains a private-sector mandate, as defined in UMRA, because it would require certain entities to assist the government with electronic surveillance. Because CBO has no information about the prevalence of electronic surveillance and the cost of compliance for entities assisting the government with electronic surveillance, CBO has no basis for estimating the costs of the mandate or whether those costs would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Estimated cost to the Federal Government: CBO cannot estimate the budgetary impact of implementing H.R. 5825 because we cannot predict how the volume or type of surveillance would change

under this legislation. Moreover, information regarding surveillance technologies and their associated costs are classified.

Any changes in federal spending under the bill would be subject to the appropriation of the necessary funds. Enacting H.R. 5825 would not affect direct spending or revenues.

Estimated impact on state, local, and tribal governments: Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that section 9 of the bill, which authorizes certain electronic surveillance without a warrant due to an imminent threat of attack, falls under that exclusion; we have not reviewed it for intergovernmental mandates.

One of the other provisions of the bill contains an intergovernmental mandate, as defined in UMRA, because it would allow federal law enforcement officers to direct public institutions such as libraries to provide information. Because data about the number of public entities currently complying with similar requests and the costs of that compliance are classified, CBO cannot estimate the total costs state and local governments would incur to comply with this mandate. Based on information from a recent survey of public libraries, however, CBO estimates that the number of requests would probably be small and that the total costs to those entities would be well below the annual threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

Estimated impacts on the private sector: Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that section 9 of the bill, which authorizes certain electronic surveillance without a warrant due to imminent threat of attack, falls under that exclusion and has not reviewed it for private-sector mandates.

H.R. 5825 contains a private-sector mandate, as defined in UMRA, because it would require certain entities to assist the government with electronic surveillance. CBO has no basis for estimating the costs of the mandate or whether those costs would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

H.R. 5825 would authorize the Attorney General, after obtaining the certification required under the bill, to direct a person to immediately provide the government with all information, facilities, and assistance necessary to conduct electronic surveillance and to acquire foreign intelligence. Under current law, the Attorney General may direct a "common carrier" to provide such assistance with electronic surveillance. This bill would expand the scope of entities that must comply with the government's orders in such cases. Because CBO has no information about how often such entities would be directed to provide assistance or the costs associated with providing assistance, CBO has no basis for estimating the costs of this mandate. The bill also would authorize the government to compensate, at the prevailing rate, a person for providing such information, facilities, or assistance.

Previous CBO estimate: On September 25, 2006, CBO transmitted a cost estimate for H.R. 5825, as ordered reported by the House Committee on the Judiciary on September 20, 2006. The language of the two versions of the bill is similar. CBO cannot esti-

mate the federal budgetary impact of implementing either version of H.R. 5825 because we cannot predict how the volume or type of surveillance would change under either version.

The House Judiciary version includes an intergovernmental and private-sector mandate that is not included in the Intelligence Committee's bill. That provision would provide protection from a cause of action for any person providing information, facilities, or assistance as well as conducting physical searches in accordance with a directive from the Attorney General under the bill.

Estimate prepared by: Federal Costs: Jason Wheelock. Impact on State, Local, and Tribal Governments: Melissa Merrell. Impact on the Private Sector: Victoria Liu.

Estimate approved by: Robert A. Sunshine, Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

AN ACT To authorize electronic surveillance to obtain foreign intelligence information.

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

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 101. As used in this title:

(a) * * *

(b) "Agent of a foreign power" means—

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

(A) * * *

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

tivities or knowingly conspires with any person to engage in such activities; [or]

* * * * * * *

(D) possesses or is reasonably expected to transmit or receive foreign intelligence information while in the United States; or

* * * * * * *

[(f) "Electronic surveillance" means—

[(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

[(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

[(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

[(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.]

(f) "Electronic surveillance" means—

(1) the installation or use of a surveillance device for the intentional collection of information relating to a person who is reasonably believed to be in the United States by intentionally targeting that person, under circumstances in which the 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, without the consent of a party to the 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 located within the United States.

* * * * * * *

(h) "Minimization procedures", with respect to electronic surveillance, means—

(1) * * *

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; *and*

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes**[**; and**]**.

[(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.**]**

* * * * * * *

[(l) "Wire communication" means any communications while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.**]**

(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.

* * * * * * *

AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 102. (a)(1) Notwithstanding any other law, the President, 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—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications **[**transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3); or**]** *of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a), or an agent of a foreign power, as defined in section 101(b)(1); or*

(ii) 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 section 101(a) (1), (2), or (3); *and*

[(B) there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party; and**]**

[(C)] *(D)* the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

* * * * * * *

(3) 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—

(A) an application for a court order with respect to the surveillance is made under [sections 101(h)(4) and] *section* 104; or

* * * * * * *

[(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

[(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

[(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.]

[(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103, 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, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.]

(b)(1) The Attorney General may require, by written certification, any person with authorized access to electronic communications or equipment used to transmit or store electronic communications to provide information, facilities, or technical assistance—

(A) necessary to accomplish electronic surveillance authorized under subsection (a); or

(B) to an official designated by the President for a period of up to one year, provided the Attorney General certifies in writing, under oath, that the provision of the information, facilities, or technical assistance does not constitute electronic surveillance.

(2) The Attorney General may require a person providing information, facilities, or technical assistance under paragraph (1) to—

(A) provide the information, facilities, or technical assistance in such a manner as will protect the secrecy of the provision of such information, facilities, or technical assistance and produce a minimum of interference with the services that such person is providing the customers of such person; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning such electronic surveillance or the information, facilities, or technical assistance provided which such person wishes to retain.

(3) The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or technical assistance pursuant to paragraph (1).

(c) Notwithstanding any other provision of law, the President may designate an official who may authorize electronic surveillance of international radio communications of a diplomat or diplomatic mission or post of the government of a foreign country in the United States in accordance with procedures approved by the Attorney General.

* * * * * * *

APPLICATION FOR AN ORDER

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

(1) * * *

* * * * * * *

[(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;**]**

[(7)**]** *(6)* a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official **[**or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate**]** *designated by the President to authorize electronic surveillance for foreign intelligence purposes*—

(A) * * *

* * * * * * *

(C) that such information cannot reasonably be obtained by normal investigative techniques; *and*

[(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

[(E) including 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;]

(D) including a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated;

[(8) a statement of the means by which the surveillance will be effected and] *(7)* a statement whether physical entry is required to effect the surveillance; *and*

[(9) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;]

[(10)] *(8)* a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter[; and].

[(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.]

[(b) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a), but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.]

[(c)] *(b)* The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

[(d)] *(c)* The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

[(e)] *(d)*(1)(A) * * *

* * * * * * *

ISSUANCE OF AN ORDER

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

[(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;]

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

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

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

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

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

[(5)] *(4)* the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section [104(a)(7)(E)] *104(a)(6)(D)* and any other information furnished under section [104(d)] *104(c)*.

* * * * * * *

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

(A) * * *

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

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

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

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

[(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device.]

* * * * * * *

[(d) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order used need not contain the information required by subparagraphs (C), (D), and (F) of subsection (c)(1), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.]

[(e)] *(d)*(1) An order issued under this section may approve an electronic surveillance [for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted

against a foreign power, as defined in section 101(a), (1), (2), or (3), for the period specified in the application or for one year, whichever is less, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.] *for a period not to exceed one year.*

(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an [original order, except that (A) an extension of an order under this Act for a surveillance targeted against a foreign power, a defined in section 101(a) (5) or (6), or against a foreign power as defined in section 101(a)(4) that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.] *original order for a period not to exceed one year.*

[(f) Notwithstanding any other provision of this title, when the Attorney General reasonably determines that—

[(1) 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; and

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

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 103 is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this title is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he 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 information sought is obtained, when the application for the order is denied, or after the expiration of 72 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.]

(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment 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 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 120 hours after the official 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 information sought is obtained, when the application for the order is denied, or after the expiration of 120 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.

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

(1) * * *

* * * * * * *

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

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

(1) in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search; or

(2) 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 that does not constitute electronic surveillance.

USE OF INFORMATION

SEC. 106. (a) * * *

* * * * * * *

(i) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any [radio] communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the [contents indicates] *contents contain significant foreign intelligence information or indicate* a threat of death or serious bodily harm to any person.

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

(1) * * *

* * * * * * *

(k)(1) * * *

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section [104(a)(7)(B)] *104(a)(6)(B)* or the entry of an order under section 105.

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 108. (a)(1) * * *

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

(A) * * *

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

(C) the total number of emergency employments of electronic surveillance under section [105(f)] *105(e)* and the

total number of subsequent orders approving or denying such electronic surveillance[.]*; and*

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

(3) Each report submitted under this subsection shall include reports on electronic surveillance conducted without a court order.

* * * * * * *

AUTHORIZATION DURING TIME OF WAR

SEC. 111. Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information [for a period not to exceed fifteen calendar days following a declaration of war by the Congress.] *for a period not to exceed 60 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.—*

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 General, may authorize electronic surveillance without an order under this title to acquire foreign intelligence information for a period not to exceed 45 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 45-day period described in subsection (a), and every 45 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 45 days. The President shall be authorized to conduct electronic surveillance under this section for an additional 45 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 (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 90 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 electronic 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.

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 General, 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 communication 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.

* * * * * * *

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

DEFINITIONS

SEC. 301. As used in this title:

(1) * * *

* * * * * * *

(5) "Physical search" means any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 101(f) of this [Act, or (B)] *Act, (B) activities described in section 102(b) of this Act, or (C)* the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101(f) of this Act.

* * * * * * *

AUTHORIZATION DURING TIME OF WAR

SEC. 309. Notwithstanding any other provision of law, the President, through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information [for a period not to exceed 15 calendar days following a declaration of war by the Congress.] *for a period not to exceed 60 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.*

* * * * * * *

NATIONAL SECURITY ACT OF 1947

* * * * * * *

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

GENERAL CONGRESSIONAL OVERSIGHT PROVISIONS

SEC. 501. (a) * * *

* * * * * * *

(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.

[(f)] *(g)* As used in this section, the term "intelligence activities" includes covert actions as defined in section 503(e), and includes financial intelligence activities.

REPORTING OF INTELLIGENCE ACTIVITIES OTHER THAN COVERT ACTIONS

SEC. 502. (a) * * *

* * * * * * *

(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.

PRESIDENTIAL APPROVAL AND REPORTING OF COVERT ACTIONS

SEC. 503. (a) * * *

* * * * * * *

(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.

* * * * * * *

MINORITY VIEWS

All nine Democratic Members of the House Permanent Select Committee on Intelligence support strong, modem, and lawful tools to fight terrorism. We want to intercept their communications, track their whereabouts, and disrupt their plans. We stand ready and willing to respond to any reasonable request from the Administration for additional legal tools for the National Security Agency (NSA). But we believe that how we use these tools is a measure of who we are as a nation—a yardstick by which the rest of the world will view our commitment to the values upon which this country was founded. Those who founded our country created a system of checks and balances and we believe their vision should be preserved. Congress should not give any President unchecked authority to eavesdrop on Americans.

The Foreign Intelligence Surveillance Act (FISA) is a modern, flexible statute that allows the government to conduct electronic surveillance on Americans. As the record in our Committee has made clear, FISA is a vital tool for the Federal Bureau of Investigation (FBI) and the NSA in their investigations of terrorism and espionage.

There is no evidence in the record of our Committee that FISA must be rewritten in favor of a new regime permitting broad warrantless surveillance of Americans. Yet H.R. 5825 does exactly that.

We have heard the claim that the law is "outmoded," but FISA has been amended and modernized numerous times over the past 28 years, including most recently in the reauthorization of the USA PATRIOT Act in March. The Congressional Research Service (CRS) provided a report to this Committee showing that 51 separate provisions in twelve different bills have amended FISA—many of those in just the past five years.

Given that H.R. 5825 is intended to address concerns over the President's domestic surveillance program, it is stunning how little oversight this Committee has actually conducted and how little information we have about the program.

For months we have asked that Committee members meet with the NSA Inspector General, members of the Foreign Intelligence Surveillance Court, the Department of Justice (DOJ), the FBI, and the Central Intelligence Agency (CIA) to learn whether the program has helped stop any terrorist attacks. The Majority denied each of those requests. We have asked for a copy of the President's Authorization for the program and for other core documents. The Administration has refused to produce them. In June, the Ranking Member asked the Chairman to join her in sending a letter to the NSA Inspector General asking to review his seven reports on the program. The Chairman did not agree to send that letter.

We have received occasional briefings from NSA officials, but none of these briefings have been on the record, on the purported theory that we could not find a single cleared stenographer. This problem persisted despite the fact that thousands of Executive Branch officials have been briefed into this program.

The Chairman committed in public to hold hearings with Administration officials to help determine what changes to FISA, if any, were needed to accommodate the President's program. We had hoped to have Attorney General Gonzales testify. But no such hearings were held. In fact, the Committee never even extended an invitation to the Attorney General.

H.R. 5825 is a dangerously broad bill that would turn FISA on its head by making warrantless surveillance the rule rather than the exception. It does so by altering the definition of key terms within FISA that govern what forms of surveillance require a warrant and by carving out giant loopholes that give the Administration broad powers to conduct all types of surveillance without a warrant.

H.R. 5825 proposes sweeping alterations to the definition of "electronic surveillance" that would drastically shrink the universe of communications for which a warrant is required. It radically expands the definition of "agent of a foreign power." It seriously erodes the protections against dissemination of information collected on U.S. persons. And it offers a new definition of "surveillance device" that would allow the government to conduct unregulated data retention and mining operations on all the information collected from the vast warrantless surveillance that this bill authorizes.

In other sections, H.R. 5825 grants the Administration the authority, under poorly defined circumstances, to conduct surveillance without a warrant. The bill grants the government the power to conduct unlimited surveillance in the event of an "armed attack" and in the event of a "terrorist attack." Though neither of these terms is defined anywhere in the law. Therefore, these sweeping exceptions give the Executive Branch carte blanche authority to conduct surveillance as it sees fit.

Further, the Majority offered an Amendment in the Nature of a Substitute to H.R. 5825 to create yet another loophole that would allow the same sort of warrantless surveillance when the United States is facing an "imminent threat of attack." Here, again, the terms are so loosely defined that the potential for abusive interpretation threatens to swallow the statute whole.

In sum, H.R. 5825's vague definitions and broad loopholes allow the Executive Branch to conduct electronic surveillance of telephone calls and e-mail in the United States without court orders and without meaningful oversight.

The Minority offered several amendments to address these concerns; sadly, all were rejected during markup on a party-line vote.

First, Representatives Harman and Boswell offered an amendment that would have substituted H.R. 5825 with H.R. 5371, the LISTEN Act (Lawful Intelligence and Surveillance of Terrorists in an Emergency by the NSA). The strength of the LISTEN Act is that it only fixes what is broken.

This amendment would have made clear that FISA is the exclusive means by which the Executive Branch may conduct electronic surveillance of Americans for intelligence purposes. It would have reiterated that the Authorization for the Use of Military Force (AUMF) did not authorize the President's domestic surveillance program; it did not repeal FISA. It would have invited the President and the Attorney General to tell us what is wrong with the FISA process so that we can fix it. It would have also required the President to identify any additional resources needed to help the NSA and the DOJ fight the war on terror using FISA authorities. And it would have pledged that Congress would fund additional attorneys, analysts and information technology upgrades to make FISA more efficient.

An amendment offered by Representatives Eshoo and Holt would have altered FISA's definition of "electronic surveillance" to make the statute technology neutral. Making this fix would require changing only a few words in the statute to eliminate the distinction between wire and radio communications. Unlike H.R. 5825, the tailored fix offered by Representatives Eshoo and Holt would have updated the law without gutting FISA.

An amendment offered by Representatives Holt and Ruppersberger would have reaffirmed the principle that FISA is the exclusive means for conducting electronic surveillance in the United States. This amendment would have ensured that the President would be held to the rules—even the permissive rules of H.R. 5825. As it stands today, if H.R. 5825 passes, the President can avail himself of its loose rules when he wishes or circumvent those loose rules if he so chooses.

Representative Reyes offered an amendment finding that the AUMF does not constitute legal authorization for electronic surveillance outside of FISA. We do not believe that any Member's vote on the AUMF was a vote for warrantless surveillance of law-abiding citizens in contravention of the Fourth Amendment of the Constitution.

Representative Hastings offered an amendment that would have clarified existing law by reaffirming that FISA does not require a warrant to monitor telephone calls where all participants are located outside the United States. This amendment would have allowed free surveillance of foreign-to-foreign communications but would have left the other critical FISA provisions intact. There is no reasonable explanation why the Majority would oppose this provision.

Protecting America from terrorism is our highest duty. We need to get serious about the task. It is election season, and a debate on surveillance brings political benefits to some. But that is a terrible reason to legislate. We do not want to suspend our 217-year-old Constitution, whether for political reasons or for no reason at all.

JANE HARMAN.
Ranking Democrat
SILVESTRE REYES.
BUD CRAMER.
RUSH HOLT.
JOHN F. TIERNEY.

ALCEE L. HASTINGS.
LEONARD L. BOSWELL.
ANNA ESHOO.
C.A. DUTCH RUPPERSBERGER.

ADDITIONAL VIEWS

I have joined my Democratic colleagues in signing the minority views as they reflect the "mark-up" session's events and general overview of the situation surrounding the meeting. It is instructive, I believe, to make some brief additional observations.

The Administration has yet to articulate on record specific justifications for arguing that executive powers broader than those within the Foreign Intelligence Surveillance Act would be necessary in order to intercept communications under the so-called "President's Program." As more than one witness pointed out in the course of related hearings, the President and his Administration assert only broadly that there may be some issue with respect to complying in a timely manner with emergency provisions for seeking a warrant. Any problems in this regard seem self-induced as a result of bureaucratic processes established within the originating agency or the Department of Justice, and not from any delay in the Foreign Intelligence Surveillance Court. Additional staff or revised procedures could address the matter without statutory amendment. Nevertheless, the LISTEN Act, proposed by Representative Harman and co-sponsored by 64 of other members, including the minority HPSCI members, would make clear Congress' willingness to make additional resources available as requested.

There was some assertion that agencies were interpreting the law to indicate that they felt certain foreign-to-foreign communications routed in any way through domestic infrastructure might necessitate a warrant, thus burdening the process. Experts have indicated that a clear reading of existing statutory language would obviate such concerns as it addresses intercepts of communications from and to foreign persons. A simple clarification of the statute (offered as an amendment by Representative Hastings of Florida) could resolve any lingering doubts, and Senator Feinstein's bill even goes so far as to clarify it statutorily.

A wholesale revision of the FISA, especially one so radical as that proposed in Representative Wilson's bill, is not necessary to address the only concerns of record articulated by the Administration. It would be reasonable for the public to then wonder whether the Administration is being forthcoming in its real purposes for having surreptitiously conducted the "President's Program" for so long or for seeking new legislation. Is there more to the Executive's intentions under such broad authority, or, as some have speculated, are those within the Administration who have chafed under what they perceived as a loss of executive authority under FISA simply asserting a point here? With respect to the latter, we should note that the United States Supreme Court has recently made it abundantly clear that when Congress has spoken by law on a matter within its purview, the Executive is not at liberty simply to controvert Congress' intentions unilaterally. Congress should not be an

accomplice to a diminution of its rightful authority by passing unnecessarily broad legislation absent specific evidence of its necessity for the nation's security. That burden has not been met in this instance. The Executive, under FISA, has ample authority to intercept terrorists' communications as appropriate to protect the country, and a Congress willing—as shown over time and most recently since 9/11 via the PATRIOT Act—to amend FISA if necessary to resolve clearly articulated needs.

JOHN TIERNEY.

○