Purpose: To provide a complete substitute.

S. 2453

To establish procedures for the review of electronic surveillance programs.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT INTENDED TO BE PROPOSED BY _____

Viz:

In lieu of the matter proposed to be inserted, insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "_____ Act of 2006".

SEC. 2. FINDINGS.

Congress finds the following:

(1) After the terrorist attacks of September 11, 2001, President Bush authorized the National Security Agency to intercept communications between people inside the United States, including American citizens, and terrorism suspects overseas.

(2) One of the lessons learned from September 11, 2001, is that the enemies who seek to greatly harm and terrorize our Nation utilize technologies and techniques that defy conventional law enforcement practices.

(3) For days before September 11, 2001, the Federal Bureau of Investigation suspected that confessed terrorist Zacarias Moussaoui was planning to hijack a commercial plane. The Federal Bureau of Investigation, however, could not meet the requirements to obtain a traditional criminal warrant or an order under the Foreign Intelligence Surveillance Act of 1978 to search his laptop computer. Report of the 9/11 Commission 273–76.

(4) The President, as the constitutional officer most directly responsible for protecting the United States from attack, requires the ability and means to detect and track an enemy that can master and exploit modern technology.

(5) It is equally essential, however, that in protecting us against our enemies, the

President does not compromise the very civil liberties that he seeks to safeguard. As Justice Hugo Black observed, "The President's power, if any, to issue [an] order must stem either from an Act of Congress or from the Constitution itself." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952) (opinion by Black, J.). Similarly, in 2004, Justice Sandra Day O'Connor explained in her plurality opinion for the Supreme Court in Hamdi v. Rumsfeld: "We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens." Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (citations omitted).

(6) When deciding issues of national security, it is in our Nation's best interest that, to the extent feasible, all 3 branches of the Federal Government should be involved. This helps guarantee that electronic surveillance programs do not infringe on the constitutional rights of Americans, while at the same time ensuring that the President has all the powers and means necessary to detect and track our enemies and protect our Nation from attack.

(7) As Justice Sandra Day O'Connor explained in her plurality opinion for the Supreme Court in Hamdi v. Rumsfeld, "Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all 3 branches when individual liberties are at stake." Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (citations omitted).

(8) Similarly, Justice Jackson famously explained in his Youngstown concurrence: "When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate... When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility... When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635–38 (1952) (Jackson, J., concurring).

(9) Congress clearly has the authority to enact legislation with respect to electronic surveillance programs. The Constitution provides Congress with broad powers of oversight over national security and foreign policy, under article I, section 8 of the Constitution of the United States, which confers on Congress numerous powers, including the powers—

(A) "To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water";

(B) "To raise and support Armies";

(C) "To provide and maintain a Navy";

(D) "To make Rules for the Government and Regulation of the land and naval Forces";

(E) "To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions"; and

(F) "To provide for organizing, arming, and disciplining the Militia, and for governing such Part of them as may be employed in the Service of the United States".

(10) While Attorney General Alberto Gonzales explained that the executive branch reviews the electronic surveillance program of the National Security Agency every 45 days to ensure that the program is not overly broad, it is the belief of Congress that approval and supervision of electronic surveillance programs should be conducted outside of the executive branch, by the article III court established under section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803). It is also the belief of Congress that it is appropriate for an article III court to pass upon the constitutionality of electronic surveillance programs that may implicate the rights of Americans.

(11) The Foreign Intelligence Surveillance Court is the proper court to approve and supervise classified electronic surveillance programs because it is adept at maintaining the secrecy with which it was charged and it possesses the requisite expertise and discretion for adjudicating sensitive issues of national security.

(12) In 1975, [then] Attorney General Edward Levi, a strong defender of executive authority, testified that in times of conflict, the President needs the power to conduct long-range electronic surveillance and that a foreign intelligence surveillance court should be empowered to issue special approval orders in these circumstances.

(13) This Act clarifies and definitively establishes that the Foreign Intelligence Surveillance Court has the authority to review electronic surveillance programs and pass upon their constitutionality. Such authority is consistent with well-established, longstanding practices.

(14) The Foreign Intelligence Surveillance Court already has broad authority to approve surveillance of members of international conspiracies, in addition to granting warrants for surveillance of a particular individual under sections 104, 105, and 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804, 1805, and 1842).

(15) Prosecutors have significant flexibility in investigating domestic conspiracy cases. Courts have held that flexible warrants comply with the 4th amendment to the Constitution of the United States when they relate to complex, far-reaching, and multifaceted criminal enterprises like drug conspiracies and money laundering rings. The courts recognize that applications for search warrants must be judged in a common sense and realistic fashion, and the courts permit broad warrant language where, due to the nature and circumstances of the investigation and the criminal organization, more precise descriptions are not feasible.

(16) Federal agents investigating international terrorism by foreign enemies are entitled to tools at least as broad as those used by law enforcement officers investigating domestic crimes by United States citizens. The Supreme Court, in the "Keith Case", United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972), recognized that the standards and procedures used to fight ordinary crime may not be applicable to cases involving national security. The Court recognized that national "security surveillance may involve different policy and practical considerations from the surveillance of ordinary crime" and that courts should be more flexible in issuing warrants in national security cases. United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 322 (1972).

(17) By authorizing the Foreign Intelligence Surveillance Court to review electronic surveillance programs, Congress preserves the ability of the President to use the necessary means to guard our national security, while also protecting the civil liberties and constitutional rights that we cherish.

SEC. 3. DEFINITIONS.

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

(1) by redesignating title VII as title IX;

(2) by redesignating section 701 as section 901; and

(3) by inserting after title VI the following:

"TITLE VII—ELECTRONIC SURVEILLANCE

"SEC. 701. DEFINITION.

"As used in this title—

"(1) the terms 'agent of a foreign power', 'Attorney General', 'foreign power', 'international terrorism', 'minimization procedures', 'person', 'United States', and 'United States person' have the same meaning as in section 101;

"(2) the term 'congressional intelligence committees' means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives;

"(3) the term 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electro magnetic, photo electronic or photo optical system, 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 communications;

"(4) the term 'electronic tracking' means the acquisition by an electronic, mechanical, or other surveillance device of the substance of any electronic communication sent by received by, or intended to be received by a person who is

reasonably believed to be in the United States, through the intentional targeting of that person's communications, where a person in the United States participating in the communication has a reasonable expectation of privacy";

"(5) the term 'electronic surveillance program' means a program to engage in electronic tracking—

"(A) that has as a significant purpose the gathering of foreign intelligence information or protecting against international terrorism;

"(B) where it is not technically feasible to name every person or address every location to be subjected to electronic tracking;

"(C) where effective gathering of foreign intelligence information requires the flexibility to begin electronic tracking immediately after learning of suspect activity; and

"(D) where effective gathering of foreign intelligence information requires an extended period of electronic tracking;

"(6) the term 'foreign intelligence information' has the same meaning as in section 101 and includes information necessary to protect against international terrorism;

"(7) the term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a);

"(8) the term 'Foreign Intelligence Surveillance Court of Review' means the court established under section 103(b);

"(9) the term 'intercept' means the acquisition of the substance of any electronic communication by a person through the use of any electronic, mechanical, or other device; and

"(10) the term 'substance' means means any information concerning the symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling.".

SEC. 4. FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION TO REVIEW ELECTRONIC SURVEILLANCE PROGRAMS.

(a) In General.—Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 3, is amended by adding at the end the following:

"SEC. 702. FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION TO REVIEW ELECTRONIC SURVEILLANCE PROGRAMS.

"(a) Authorization of Review.—

"(1) INITIAL AUTHORIZATION.—The Foreign Intelligence Surveillance Court shall

have jurisdiction to issue an order under this title, lasting not longer than 90 days, that authorizes an electronic surveillance program to obtain foreign intelligence information or to protect against international terrorism.

"(2) REAUTHORIZATION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to reauthorize an electronic surveillance program for a period of time not longer than such court determines to be reasonable.

"(3) RESUBMISSION OR APPEAL.—In the event that the Foreign Intelligence Surveillance Court refuses to approve an application under this subsection, the Attorney General may submit a new application. There shall be no limit on the number of times the Attorney General may seek approval of an electronic surveillance program. Alternatively, the Attorney General may appeal the decision of the Foreign Intelligence Surveillance Court to the Foreign Intelligence Surveillance Court of Review.

"(b) Mandatory Transfer for Review.—

"(1) IN GENERAL.—In any case before any court challenging the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of any such activity or program is in issue, if the Attorney General files an affidavit under oath that further proceedings in such court would harm the national security of the United States, the court shall transfer the case to the Foreign Intelligence Surveillance Court of Review for further proceedings under this subsection.

"(2) PROCEDURES FOR REVIEW.—The Foreign Intelligence Surveillance Court of Review shall have jurisdiction as appropriate to determine standing and the legality of the communications intelligence activity or program to the extent necessary for resolution of the underlying case. All proceedings under this paragraph shall be conducted subject to the procedures of section 106(f), except that the Foreign Intelligence Surveillance Court of Review shall not require the disclosure of national security information to any person without the approval of the Director of National Intelligence or the Attorney General, unless in the context of a criminal proceeding disclosure would be constitutionally required.

"(3) RETRANSFER TO ORIGINATING COURT.—Upon completion of review pursuant to this subsection, the Foreign Intelligence Surveillance Court of Review shall remand the case to the originating court for further proceedings consistent with its opinion.

"(4) PRESERVATION OF LITIGATION.—All litigation privileges shall be preserved.

"(5) CERTIORARI AND EFFECTS OF DECISIONS.—The decision the Foreign Intelligence Surveillance Court of Review made under paragraph (2), including a decision that the disclosure of national security information is constitutionally required, shall be subject to certiorari review in the United States Supreme Court, and shall otherwise be binding in all other courts.

"(6) DISMISSAL.—The Foreign Intelligence Surveillance Court of Review or a court that is an originating court under paragraph (1) may dismiss a challenge to the legality of an electronic surveillance program for any reason.

"(c) Modifications and Appeal in Event Application Is Denied.—In the event that the Foreign Intelligence Surveillance Court declines to approve an application under subsection (a)—

"(1) the court shall state its reasons in a written opinion, which it shall submit to the Attorney General; and

"(2) the Attorney General may submit a new application under section 703 for the electronic surveillance program.".

SEC. 5. APPLICATIONS FOR APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 4, is amended by adding at the end the following:

"SEC. 703. APPLICATIONS FOR APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

"(a) In General.—Each application for approval of an electronic surveillance program under this title (including for reauthorization) shall—

"(1) be made by the Attorney General or his designee;

"(2) include a statement of the authority conferred on the Attorney General by the President of the United States;

"(3) include a statement setting forth the legal basis for the conclusion by the Attorney General that the electronic surveillance program is consistent with the Constitution of the United States;

"(4) certify that a significant purpose of the electronic surveillance program is to gather foreign intelligence information or to protect against international terrorism;

"(5) certify that the information sought cannot reasonably be obtained by normal investigative techniques or through an application under section 104;

"(6) include a statement of the means and operational procedures by which the electronic tracking will be executed and effected;

"(7) include an explanation of how the electronic surveillance program is reasonably designed to ensure that the communications that are intercepted are communications of or with—

"(A) a foreign power that is engaged in international terrorism activities or in preparation therefor;

"(B) an agent of a foreign power that is engaged in international terrorism activities or in preparation therefor; or

"(C) a person reasonably believed to have communication with or be associated with a foreign power that is engaged in international terrorism activities or in preparation therefor or an agent of a foreign power that is engaged in international terrorism activities or in preparation therefor;

"(8) include a statement of the proposed minimization procedures;

"(9) if the electronic surveillance program that is the subject of the application was initiated prior to the date the application was submitted, specify the date that the program was initiated;

"(10) include a description of all previous applications that have been made under this title involving the electronic surveillance program in the application (including the minimization procedures and the means and operational procedures proposed) and the decision on each previous application; and

"(11) include a statement of facts concerning the implementation of the electronic surveillance program described in the application, including, for any period of operation of the program authorized not less than 90 days prior to the date of submission of the application—

"(A) the minimization procedures implemented; and

"(B) the means and operational procedures by which the electronic tracking was executed and effected.

"(b) Additional Information.—The Foreign Intelligence Surveillance Court may require the Attorney General to furnish such other information as may be necessary to make a determination under section 704.".

SEC. 6. APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

Title VII of the Foreign Intelligence Surveillance Act 18 of 1978, as amended by section 5, is amended by adding at the end the following:

"SEC. 704. APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

"(a) Necessary Findings.—Upon receipt of an application under section 703, the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested, or as modified, approving the electronic surveillance program if it finds that—

"(1) the President has authorized the Attorney General to make the application for electronic surveillance for foreign intelligence information or to protect against international terrorism;

"(2) approval of the electronic surveillance program in the application is consistent with the Constitution of the United States;

"(3) the electronic surveillance program is reasonably designed to ensure that the communications that are intercepted are communications of or with—

"(A) a foreign power that is engaged in international terrorism activities or in preparation therefor;

"(B) an agent of a foreign power that is engaged in international terrorism activities or in preparation therefor; or

"(C) a person reasonably believed to have communication with or be associated with a foreign power that is engaged in international terrorism activities or in preparation therefor or an agent of a foreign power that is engaged in international terrorism activities or in preparation therefor;

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

"(5) the application contains all statements and certifications required by section 703.

"(b) Considerations.—In considering the constitutionality of the electronic surveillance program under subsection (a), the Foreign Intelligence Surveillance Court may consider—

"(1) whether the electronic surveillance program has been implemented in accordance with the proposal by the Attorney General by comparing—

"(A) the minimization procedures proposed with the minimization procedures actually implemented;

"(B) the nature of the information sought with the nature of the information actually obtained; and

"(C) the means and operational procedures proposed with the means and operational procedures actually implemented; and

"(2) whether foreign intelligence information has been obtained through the electronic surveillance program.

"(c) Contents of Order.—An order approving an electronic surveillance program under this section shall direct—

"(1) that the minimization procedures be followed;

"(2) that, upon the request of the applicant, specified communication or other common carriers, landlords, custodians, or other specified person, furnish the applicant forthwith with all information, facilities, or technical assistance necessary to undertake the electronic surveillance program in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carriers, landlords, custodians, or other persons are providing potential targets of the electronic surveillance program;

"(3) that any record concerning the electronic surveillance program or the aid furnished retained by such carriers, landlords, custodians, or other persons are maintained under security procedures approved by the Attorney General and the Director of National Intelligence; and

"(4) that the applicant compensate, at the prevailing rate, such carriers, landlords, custodians, or other persons for furnishing such aid.".

SEC. 7. CONGRESSIONAL OVERSIGHT.

Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section

6, is amended by adding at the end the following:

"SEC. 705. CONGRESSIONAL OVERSIGHT.

"(a) In General.—Not less often than every 180 days, the Attorney General shall submit to the congressional intelligence committees a report in classified form on the activities during the previous 180-day period under any electronic surveillance program authorized under this title.

"(b) Contents.—Each report submitted under subsection (a) shall provide, with respect to the previous 180-day period, a description of—

"(1) the minimization procedures implemented;

"(2) the means and operational procedures by which the surveillance was executed and effected; and

"(3) significant decisions of the Foreign Intelligence Surveillance Court on applications made under section 703.

"(c) Rule of Construction.—Nothing in this title shall be construed to limit the authority or responsibility of any committee of either House of Congress to obtain such information as such committee may need to carry out its respective functions and duties.".

SEC. 9. CLARIFICATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) In General.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after title VII, as amended by this Act, the following:

"TITLE VIII—EXECUTIVE AUTHORITY

"SEC. 801. EXECUTIVE AUTHORITY.

"Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers.".

(b) Repeal.—Sections 111, 309, and 404 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1811, 1829, and 1844) are repealed.

(c) Conforming Amendments.—

(1) TITLE 18.—Section 2511(2) of title 18, United States Code, is amended—

(A) in paragraph (e), by striking ", as defined in section 101" and all that follows through the end of the paragraph and inserting the following: "under the constitutional authority of the executive or the Foreign Intelligence Surveillance Act of 1978."; and

(B) in paragraph (f), by striking "from international or foreign communications," and all that follows through the end of the paragraph and inserting "that is authorized under a Federal statute or the Constitution of the

United States."

(2) FISA.—Section 109 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809) is amended—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by inserting "or under the Constitution" after "authorized by statute"; and

(II) by striking "or" at the end;

(ii) in paragraph (2)—

(I) by inserting "or under the Constitution" after "authorized by statute"; and

(II) by striking the period and inserting "; or"; and

(iii) by adding at the end the following:

"(3) knowingly discloses or uses information obtained under color of law by electronic surveillance in a manner or for a purpose not authorized by law."; and

(B) in subsection (c)—

(i) by striking "$10,000" and inserting "$100,000"; and

(ii) by striking "five years" and inserting "15 years".

SEC. 10. OTHER CONFORMING AMENDMENTS TO FISA.

(a) Reference.—In this section, a reference to "FISA" shall mean the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)

(b) Definitions.—Section 101 of FISA (50 U.S.C. 1801) is amended—

(1) in subsection (b)(1)—

(A) in subparagraph (B), by striking "or" after the semicolon;

(B) by adding at the end the following:

"(D) otherwise possesses or is expected to transmit or receive foreign intelligence information while within the United States; or";

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

"(f) 'Electronic surveillance' means—

"(1) the installation or use of an electronic, mechanical, or other surveillance device for the intentional collection of information concerning a particular known person who is reasonably believed to be in the United States by intentionally targeting that person under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement

purposes; or

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

(3) in subsection (g), by inserting before the period the following: "or a person or persons designated by the Attorney General or Acting Attorney General";

(4) in subsection (h)—

(A) in paragraph (2), by inserting "and" after the semicolon;

(B) in paragraph (3), by striking "; and" and inserting a period; and

(C) by striking paragraph (4);

(5) by striking subsection (n) and inserting the following:

"(n) 'contents' has the meaning set forth in section 2510(8) of title 18, United states Code."

(c) Electronic Surveillance Authorization.—Section 102 of FISA (50 U.S.C. 1802) is amended to read as follows:

"ELECTRONIC SURVEILLANCE AUTHORIZATION WITHOUT COURT ORDER; CERTIFICATION BY ATTORNEY GENERAL; REPORTS TO CONGRESSIONAL COMMITTEES; TRANSMITTAL UNDER SEAL; DUTIES AND COMPENSATION OF COMMUNICATION COMMON CARRIER; APPLICATIONS; JURISDICTION OF COURT

"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 1 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 of a foreign power, as defined in 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 paragraph (1), (2), or (3) of section 101(a); and

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

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

"(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence under the provisions of section 108(a).

"(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 section 104; or

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

"(b) The Attorney General is also authorized to deliver to a provider of any electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) who has access to electronic communications, either as they are transmitted or while they are stored or equipment that is being or may be used to transmit or store such communications, a certificate requiring that such person or persons furnish any information, facilities, or technical assistance to an official authorized by the President to engage in electronic surveillance for foreign intelligence purposes, for periods of up to 1 year if the Attorney General certifies in writing to the carrier under oath that such provision of information, facilities, or technical assistance does not constitute electronic surveillance as defined in section 101(f).

"(c) With respect to electronic surveillance or the furnishing of any information, facilities, or technical assistance authorized by this section, the Attorney General may direct a provider of any electronic communication service, landlord, custodian or other person (including any officer, employee, agent, or other specified person thereof) who has access to electronic communications, either as they are transmitted or while they are stored or equipment that is being or may be used to transmit or store such communications to—

"(1) 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 provider of any electronic communication service, landlord, custodian, or other person is providing its customers; and

"(2) 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 provider of any electronic communication service, landlord, custodian, or other person wishes to retain.

The Government shall compensate, at the prevailing rate, such provider of any electronic communication service, landlord, custodian, or other person for furnishing such aid.

"(d) Electronic surveillance directed solely at the collection of international radio

communications of diplomatically immune persons in the United States may be authorized by an official authorized by the President to engage in electronic surveillance for foreign intelligence purposes in accordance with procedures approved by the Attorney General.

"(d) Designation of judges. Section 103 of FISA (50 USC 1803) is amended in subsection (a), by inserting, "at least" before "seven of the United States Judiciary.".

(d) Applications for Court Orders.—Section 104 of FISA (50 U.S.C. 1804) is amended:

(1) in subsection (a), by striking paragraphs (7) through (11) and inserting the following:

"(6) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official authorized by the President to conduct electronic surveillance for foreign intelligence purposes—

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

"(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

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

"(D) 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;;

"(7) A statement whether physical entry is required to effect the surveillance;; and

"(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.";

(2) by striking subsection (b); and

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

(e) Issuance of Order.—Section 105 of FISA (50 U.S.C. 1805) is amended—

(1) in subsection (a), by—

(A) striking paragraph (1); and

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

(2) by striking paragraph (1) of subsection (c) and inserting the following:

"(1) An order approving an electronic surveillance under this section shall specify—

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

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

"(C) the period of time during which the electronic surveillance is approved.";

(3) by striking subsection (d) and inserting the following:

"(d) Each order under this section shall specify the type of electronic surveillance involved, including whether physical entry is required.";

(4) by striking paragraphs (1) and (2) of subsection (e) and inserting the following:

"(1) An order issued under this section may approve an electronic surveillance may be for a period not to exceed 1 year. If such emergency employment of electronic surveillance is authorized, the official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

"(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not to exceed 1 year.";

(5) by striking subsection (f) and inserting the following:

"(f)(1) Notwithstanding any other provision of this title, when an official authorized by the President to conduct electronic surveillance reasonably determines that—

"(A) 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

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

that official may authorize the emergency employment of electronic surveillance in accordance with paragraph (2).

"(2) Under paragraph (1), the following requirements shall be satisfied:

"(A) The Attorney General shall be informed of the emergency electronic surveillance.

"(B) A judge having jurisdiction under section 103 shall be informed by the Attorney General or his designee as soon as practicable following such authorization that the decision has been made to employ emergency electronic surveillance.

"(C) An application in accordance with this title shall be made to that judge or another judge having jurisdiction under section 103 as soon as practicable, but not more than 7 days after such surveillance is authorized. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when

the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of emergency authorization, 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

(6) in subsection (i), by—

(A) striking "a wire or" and inserting "any";

(B) striking "chapter" and inserting "title"; and

(C) by adding at the end ", or in response to certification by the Attorney General or his designee seeking information, facilities, or technical assistance from such person that does not constitute electronic surveillance as defined in section 101(f)".

"(f) Use of information – Section 106 of FISA (50 USC 1806) is amended –

(1) in subsection (i), by –

(a) deleting "radio", and

(b) inserting after "Attorney general determines that the content" "contain significant foreign intelligence or"; and

(2) in subsection (k), by deleting "104(a)(7)" and inserting "104(a)(6)".

(g) Congressional Oversight.—Section 108 of FISA (50 U.S.C. 1808) is amended by adding at the end the following:

"(c) Document Management System for Applications for Orders Approving Electronic Surveillance.—

"(1) SYSTEM PROPOSED.—The Attorney General and Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, the Director of the National Security Agency, and the Foreign Intelligence Surveillance Court, conduct a feasibility study to develop and implement a secure, classified document management system that permits the prompt preparation, modification, and review by appropriate personnel of the Department of Justice, the Federal Bureau of Investigation, the National Security Agency, and other applicable elements of the United States Government of applications under section 104 before their submittal to the Foreign Intelligence Surveillance Court.

"(2) SCOPE OF SYSTEM.—The document management system proposed in

paragraph (1) shall—

"(A) permit and facilitate the prompt submittal of applications to the Foreign Intelligence Surveillance Court under section 104 or 105(g)(5); and

"(B) permit and facilitate the prompt transmittal of rulings of the Foreign Intelligence Surveillance Court to personnel submitting applications described in paragraph (1).".

(h) Criminal Sanctions.—Section 109 of FISA (50 U.S.C. 1809) is amended by striking subsection (a) and inserting the following:

"(a) Prohibited Activities.—A person is guilty of an offense if he intentionally—

"(1) engages in electronic surveillance as defined in section 101(f) under color of law except as authorized by law; or

"(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by law.".

(i) Authorization During Time of War.—Title I of FISA is amended by striking section 111.

(i) Physical Searches.—Title III of FISA (50 U.S.C. 1821 et seq.) is amended—

(1) in section 301 (50 U.S.C. 1821), by striking paragraph (5) and inserting the following:

"(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 activities conducted in accordance with sections 102 or 105.";

(2) in section 307, by striking subsection (a) and inserting the following:

"(a) A person is guilty of an offense if he intentionally—

"(1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute or under the Constitution; or

"(2) discloses or uses information obtained under color of law by physical search within the United States, knowing or having reason to know that the information was obtained through physical search not authorized by statute or the Constitution"; and

(3) by striking section 309.

SEC. 11. CONFORMING AMENDMENT TO TABLE OF CONTENTS.

1 The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended
2 by striking the items related to title VII and section 701 and inserting the following:

3 "TITLE VII—ELECTRONIC SURVEILLANCE

4 "Sec.701.Definition.

5 "Sec.702.Foreign intelligence surveillance court jurisdiction to review electronic
6 surveillance programs.

7 "Sec.703.Applications for approval of electronic surveillance programs.

8 "Sec.704.Approval of electronic surveillance programs.

9 "Sec.705.Congressional oversight.

10 "TITLE VIII—EXECUTIVE AUTHORITY

11 "Sec.801.Executive authority.".
12