

AMENDMENT NO. _____ Calendar No. _____

Purpose: To provide a complete substitute.

IN THE SENATE OF THE UNITED STATES—109th Cong., 2d Sess.

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:

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “_____ Act of
5 2006”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

8 (1) After the terrorist attacks of September 11,
9 2001, President Bush authorized the National Secu-
10 rity Agency to intercept communications between

1 people inside the United States, including American
2 citizens, and terrorism suspects overseas.

3 (2) One of the lessons learned from September
4 11, 2001, is that the enemies who seek to greatly
5 harm and terrorize our Nation utilize technologies
6 and techniques that defy conventional law enforce-
7 ment practices.

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

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

22 (5) It is equally essential, however, that in pro-
23 tecting the United States against our enemies, the
24 President does not compromise the very civil lib-
25 erties that he seeks to safeguard. As Justice Hugo

1 Black observed, “The President’s power, if any, to
2 issue [an] order must stem either from an Act of
3 Congress or from the Constitution itself.” *Youngs-*
4 *town Sheet & Tube Co. v. Sawyer*, 343 U.S. 579,
5 585 (1952) (opinion by Black, J.). Similarly, in
6 2004, Justice Sandra Day O’Connor explained in
7 her plurality opinion for the Supreme Court in
8 *Hamdi v. Rumsfeld*: “We have long since made clear
9 that a state of war is not a blank check for the
10 President when it comes to the rights of the Na-
11 tion’s citizens.” *Hamdi v. Rumsfeld*, 542 U.S. 507,
12 536 (2004) (citations omitted).

13 (6) When deciding issues of national security, it
14 is in our Nation’s best interest that, to the extent
15 feasible, all 3 branches of the Federal Government
16 should be involved. This helps guarantee that elec-
17 tronic surveillance programs do not infringe on the
18 constitutional rights of Americans, while at the same
19 time ensuring that the President has all the powers
20 and means necessary to detect and track our en-
21 emies and protect our Nation from attack.

22 (7) As Justice Sandra Day O’Connor explained
23 in her plurality opinion for the Supreme Court in
24 *Hamdi v. Rumsfeld*, “Whatever power the United
25 States Constitution envisions for the Executive in its

1 exchanges with other nations or with enemy organi-
2 zations in times of conflict, it most assuredly envi-
3 sions a role for all 3 branches when individual lib-
4 erties are at stake.” Hamdi v. Rumsfeld, 542 U.S.
5 507, 536 (2004) (citations omitted).

6 (8) Similarly, Justice Jackson famously ex-
7 plained in his Youngstown concurrence: “When the
8 President acts pursuant to an express or implied au-
9 thorization of Congress, his authority is at its max-
10 imum, for it includes all that he possesses in his own
11 right plus all that Congress can delegate... When the
12 President acts in absence of either a congressional
13 grant or denial of authority, he can only rely upon
14 his own independent powers, but there is a zone of
15 twilight in which he and Congress may have concur-
16 rent authority, or in which its distribution is uncer-
17 tain. Therefore, congressional inertia, indifference or
18 quiescence may sometimes, at least as a practical
19 matter, enable, if not invite, measures on inde-
20 pendent presidential responsibility... When the Presi-
21 dent takes measures incompatible with the expressed
22 or implied will of Congress, his power is at its lowest
23 ebb, for then he can rely only upon his own constitu-
24 tional powers minus any constitutional powers of
25 Congress over the matter. Courts can sustain exclu-

1 sive Presidential control in such a case only by dis-
2 abling the Congress from acting upon the subject.”
3 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S.
4 579, 635–38 (1952) (Jackson, J., concurring).

5 (9) Congress clearly has the authority to enact
6 legislation with respect to electronic surveillance pro-
7 grams. The Constitution provides Congress with
8 broad powers of oversight over national security and
9 foreign policy, under article I, section 8 of the Con-
10 stitution of the United States, which confers on Con-
11 gress numerous powers, including the powers—

12 (A) “To declare War, grant Letters of
13 Marque and Reprisal, and make Rules con-
14 cerning Captures on Land and Water”;

15 (B) “To raise and support Armies”;

16 (C) “To provide and maintain a Navy”;

17 (D) “To make Rules for the Government
18 and Regulation of the land and naval Forces”;

19 (E) “To provide for calling forth the Mili-
20 tia to execute the Laws of the Union, suppress
21 Insurrections and repel Invasions”; and

22 (F) “To provide for organizing, arming,
23 and disciplining the Militia, and for governing
24 such Part of them as may be employed in the
25 Service of the United States”.

1 (10) While Attorney General Alberto Gonzales
2 explained that the executive branch reviews the elec-
3 tronic surveillance program of the National Security
4 Agency every 45 days to ensure that the program is
5 not overly broad, it is the belief of Congress that ap-
6 proval and supervision of electronic surveillance pro-
7 grams should be conducted outside of the executive
8 branch, by the article III court established under
9 section 103 of the Foreign Intelligence Surveillance
10 Act of 1978 (50 U.S.C. 1803). It is also the belief
11 of Congress that it is appropriate for an article III
12 court to pass upon the constitutionality of electronic
13 surveillance programs that may implicate the rights
14 of Americans.

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

22 (12) In 1975, [then] Attorney General Edward
23 Levi, a strong defender of executive authority, testi-
24 fied that in times of conflict, the President needs the
25 power to conduct long-range electronic surveillance

1 and that a foreign intelligence surveillance court
2 should be empowered to issue special approval orders
3 in these circumstances.

4 (13) The Foreign Intelligence Surveillance Act
5 of 1978 clarifies and definitively establishes that the
6 Foreign Intelligence Surveillance Court has the au-
7 thority to review electronic surveillance programs
8 and pass upon their constitutionality. Such authority
9 is consistent with well-established, longstanding
10 practices.

11 (14) The Foreign Intelligence Surveillance
12 Court already has broad authority to approve sur-
13 veillance of members of international conspiracies, in
14 addition to granting warrants for surveillance of a
15 particular individual under sections 104, 105, and
16 402 of the Foreign Intelligence Surveillance Act of
17 1978 (50 U.S.C. 1804, 1805, and 1842).

18 (15) Prosecutors have significant flexibility in
19 investigating domestic conspiracy cases. Courts have
20 held that flexible warrants comply with the 4th
21 amendment to the Constitution of the United States
22 when they relate to complex, far-reaching, and
23 multifaceted criminal enterprises like drug conspir-
24 acies and money laundering rings. The courts recog-
25 nize that applications for search warrants must be

1 judged in a common sense and realistic fashion, and
2 the courts permit broad warrant language where,
3 due to the nature and circumstances of the inves-
4 tigation and the criminal organization, more precise
5 descriptions are not feasible.

6 (16) Federal agents investigating international
7 terrorism by foreign enemies are entitled to tools at
8 least as broad as those used by law enforcement offi-
9 cers investigating domestic crimes by United States
10 citizens. The Supreme Court, in the “Keith Case”,
11 United States v. United States District Court for
12 the Eastern District of Michigan, 407 U.S. 297
13 (1972), recognized that the standards and proce-
14 dures used to fight ordinary crime may not be appli-
15 cable to cases involving national security. The Court
16 recognized that national “security surveillance may
17 involve different policy and practical considerations
18 from the surveillance of ordinary crime” and that
19 courts should be more flexible in issuing warrants in
20 national security cases. United States v. United
21 States District Court for the Eastern District of
22 Michigan, 407 U.S. 297, 322 (1972).

23 (17) By authorizing the Foreign Intelligence
24 Surveillance Court to review electronic surveillance
25 programs, Congress preserves the ability of the

1 President to use the necessary means to guard our
2 national security, while also protecting the civil lib-
3 erties and constitutional rights that we cherish.

4 **SEC. 3. DEFINITIONS.**

5 The Foreign Intelligence Surveillance Act of 1978
6 (50 U.S.C. 1801 et seq.) is amended—

7 (1) by redesignating title VII as title IX;

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

9 and

10 (3) by inserting after title VI the following:

11 **“TITLE VII—ELECTRONIC**
12 **SURVEILLANCE**

13 **“SEC. 701. DEFINITION.**

14 “As used in this title—

15 “(1) the terms ‘agent of a foreign power’, ‘At-
16 torney General’, ‘foreign power’, ‘international ter-
17 rorism’, ‘minimization procedures’, ‘person’, ‘United
18 States’, and ‘United States person’ have the same
19 meaning as in section 101;

20 “(2) the term ‘congressional intelligence com-
21 mittees’ means the Select Committee on Intelligence
22 of the Senate and the Permanent Select Committee
23 on Intelligence of the House of Representatives;

24 “(3) the term ‘electronic communication’ means
25 any transfer of signs, signals, writing, images,

1 sounds, data, or intelligence of any nature trans-
2 mitted, in whole or in part, by a wire, radio, electro
3 magnetic, photo electronic or photo optical system,
4 cable, or other like connection furnished or operated
5 by any person engaged as a common carrier in pro-
6 viding or operating such facilities for the trans-
7 mission of communications;

8 “(4) the term ‘electronic tracking’ means the
9 acquisition by an electronic, mechanical, or other
10 surveillance device of the substance of any electronic
11 communication sent by, received by, or intended to
12 be received by a person who is reasonably believed
13 to be in the United States, through the intentional
14 targeting of that person’s communications, where a
15 person in the United States participating in the
16 communication has a reasonable expectation of pri-
17 vacy;

18 “(5) the term ‘electronic surveillance program’
19 means a program to engage in electronic tracking—

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

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

1 “(C) where effective gathering of foreign
2 intelligence information requires the flexibility
3 to begin electronic surveillance immediately
4 after learning of suspect activity; and

5 “(D) where effective gathering of foreign
6 intelligence information requires an extended
7 period of electronic surveillance;

8 “(6) the term ‘foreign intelligence information’
9 has the same meaning as in section 101 and in-
10 cludes information necessary to protect against
11 international terrorism;

12 “(7) the term ‘Foreign Intelligence Surveillance
13 Court’ means the court established under section
14 103(a);

15 “(8) the term ‘Foreign Intelligence Surveillance
16 Court of Review’ means the court established under
17 section 103(b);

18 “(9) the term ‘intercept’ means the acquisition
19 of the substance of any electronic communication by
20 a person through the use of any electronic, mechan-
21 ical, or other device; and

22 “(10) the term ‘substance’ means any informa-
23 tion concerning the symbols, sounds, words, purport,
24 or meaning of a communication, and does not in-
25 clude dialing, routing, addressing, or signaling.”.

1 **SEC. 4. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
2 **JURISDICTION TO REVIEW ELECTRONIC SUR-**
3 **VEILLANCE PROGRAMS.**

4 (a) IN GENERAL.—Title VII of the Foreign Intel-
5 ligence Surveillance Act of 1978, as amended by section
6 3, is amended by adding at the end the following:

7 **“SEC. 702. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
8 **JURISDICTION TO REVIEW ELECTRONIC SUR-**
9 **VEILLANCE PROGRAMS.**

10 “(a) AUTHORIZATION OF REVIEW.—

11 “(1) INITIAL AUTHORIZATION.—The Foreign
12 Intelligence Surveillance Court shall have jurisdic-
13 tion to issue an order under this title, lasting not
14 longer than 90 days, that authorizes an electronic
15 surveillance program to obtain foreign intelligence
16 information or to protect against international ter-
17 rorism.

18 “(2) REAUTHORIZATION.—The Foreign Intel-
19 ligence Surveillance Court shall have jurisdiction to
20 reauthorize an electronic surveillance program for a
21 period of time not longer than such court determines
22 to be reasonable.

23 “(3) RESUBMISSION OR APPEAL.—In the event
24 that the Foreign Intelligence Surveillance Court re-
25 fuses to approve an application under this sub-
26 section, the Attorney General may submit a new ap-

1 plication. There shall be no limit on the number of
2 times the Attorney General may seek approval of an
3 electronic surveillance program. Alternatively, the
4 Attorney General may appeal the decision of the
5 Foreign Intelligence Surveillance Court to the For-
6 eign Intelligence Surveillance Court of Review.

7 “(b) MANDATORY TRANSFER FOR REVIEW.—

8 “(1) IN GENERAL.—In any case before any
9 court challenging the legality of classified commu-
10 nications intelligence activity relating to a foreign
11 threat, including an electronic surveillance program,
12 or in which the legality of any such activity or pro-
13 gram is in issue, if the Attorney General files an af-
14 fidavit under oath that the case should be trans-
15 ferred to the Foreign Intelligence Court of Review
16 because further proceedings in the originating court
17 would harm the national security of the United
18 States, the originating court shall transfer the case
19 to the Foreign Intelligence Surveillance Court of Re-
20 view for further proceedings under this subsection.

21 “(2) RETRANSFER TO ORIGINATING COURT.—

22 Upon completion of review pursuant to this sub-
23 section, the Foreign Intelligence Surveillance Court
24 of Review shall remand the case to the originating

1 court for further proceedings consistent with its
2 opinion.

3 “(3) PRESERVATION OF LITIGATION.—In any
4 case that is transferred and received under this sub-
5 section, all litigation privileges shall be preserved.

6 “(4) CERTIORARI AND EFFECTS OF DECI-
7 SIONS.—The decision the Foreign Intelligence Sur-
8 veillance Court of Review made under paragraph
9 (1), including a decision that the disclosure of na-
10 tional security information is constitutionally re-
11 quired, shall be subject to certiorari review in the
12 United States Supreme Court, and shall otherwise
13 be binding in all other courts.

14 “(5) DISMISSAL.—The Foreign Intelligence
15 Surveillance Court of Review or a court that is an
16 originating court under paragraph (1) may dismiss
17 a challenge to the legality of an electronic surveil-
18 lance program for any reason provided for under
19 law.

20 “(c) MODIFICATIONS AND APPEAL IN EVENT APPLI-
21 CATION IS DENIED.—In the event that the Foreign Intel-
22 ligence Surveillance Court declines to approve an applica-
23 tion under subsection (a)—

1 “(1) the court shall state its reasons in a writ-
2 ten opinion, which it shall submit to the Attorney
3 General; and

4 “(2) the Attorney General may submit a new
5 application under section 703 for the electronic sur-
6 veillance program.”.

7 **SEC. 5. APPLICATIONS FOR APPROVAL OF ELECTRONIC**
8 **SURVEILLANCE PROGRAMS.**

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

12 **“SEC. 703. APPLICATIONS FOR APPROVAL OF ELECTRONIC**
13 **SURVEILLANCE PROGRAMS.**

14 “(a) IN GENERAL.—Each application for approval of
15 an electronic surveillance program under this title (includ-
16 ing for reauthorization) shall—

17 “(1) be made by the Attorney General or his
18 designee;

19 “(2) include a statement of the authority con-
20 ferred on the Attorney General by the President of
21 the United States;

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

1 “(4) certify that a significant purpose of the
2 electronic surveillance program is to gather foreign
3 intelligence information or to protect against inter-
4 national terrorism;

5 “(5) certify that the information sought cannot
6 reasonably be obtained by normal investigative tech-
7 niques or through an application under section 104;

8 “(6) include a statement of the means and
9 operational procedures by which the electronic track-
10 ing will be executed and effected;

11 “(7) include an explanation of how the elec-
12 tronic surveillance program is reasonably designed to
13 ensure that the communications that are intercepted
14 are communications of or with—

15 “(A) a foreign power that is engaged in
16 international terrorism activities or in prepara-
17 tion therefor;

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

21 “(C) a person reasonably believed to have
22 communication with or be associated with a for-
23 eign power that is engaged in international ter-
24 rorism activities or in preparation therefor or
25 an agent of a foreign power that is engaged in

1 international terrorism activities or in prepara-
2 tion therefor;

3 “(8) include a statement of the proposed mini-
4 mization procedures;

5 “(9) if the electronic surveillance program that
6 is the subject of the application was initiated prior
7 to the date the application was submitted, specify
8 the date that the program was initiated;

9 “(10) include a description of all previous appli-
10 cations that have been made under this title involv-
11 ing the electronic surveillance program in the appli-
12 cation (including the minimization procedures and
13 the means and operational procedures proposed) and
14 the decision on each previous application; and

15 “(11) include a statement of facts concerning
16 the implementation of the electronic surveillance pro-
17 gram described in the application, including, for any
18 period of operation of the program authorized not
19 less than 90 days prior to the date of submission of
20 the application—

21 “(A) the minimization procedures imple-
22 mented; and

23 “(B) the means and operational procedures
24 by which the electronic tracking was executed
25 and effected.

1 “(b) ADDITIONAL INFORMATION.—The Foreign In-
2 telligence Surveillance Court may require the Attorney
3 General to furnish such other information as may be nec-
4 essary to make a determination under section 704.”.

5 **SEC. 6. APPROVAL OF ELECTRONIC SURVEILLANCE PRO-**
6 **GRAMS.**

7 Title VII of the Foreign Intelligence Surveillance Act
8 18 of 1978, as amended by section 5, is amended by add-
9 ing at the end the following:

10 **“SEC. 704. APPROVAL OF ELECTRONIC SURVEILLANCE**
11 **PROGRAMS.**

12 “(a) NECESSARY FINDINGS.—Upon receipt of an ap-
13 plication under section 703, the Foreign Intelligence Sur-
14 veillance Court shall enter an ex parte order as requested,
15 or as modified, approving the electronic surveillance pro-
16 gram if it finds that—

17 “(1) the President has authorized the Attorney
18 General to make the application for electronic sur-
19 veillance for foreign intelligence information or to
20 protect against international terrorism;

21 “(2) approval of the electronic surveillance pro-
22 gram in the application is consistent with the Con-
23 stitution of the United States;

24 “(3) the electronic surveillance program is rea-
25 sonably designed to ensure that the communications

1 that are intercepted are communications of or
2 with—

3 “(A) a foreign power that is engaged in
4 international terrorism activities or in prepara-
5 tion therefor;

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

9 “(C) a person reasonably believed to have
10 communication with or be associated with a for-
11 eign power that is engaged in international ter-
12 rorism activities or in preparation therefor or
13 an agent of a foreign power that is engaged in
14 international terrorism activities or in prepara-
15 tion therefor;

16 “(4) the proposed minimization procedures
17 meet the definition of minimization procedures
18 under section 101(h); and

19 “(5) the application contains all statements and
20 certifications required by section 703.

21 “(b) **CONSIDERATIONS.**—In considering the constitu-
22 tionality of the electronic surveillance program under sub-
23 section (a), the Foreign Intelligence Surveillance Court
24 may consider—

1 “(1) whether the electronic surveillance pro-
2 gram has been implemented in accordance with the
3 proposal by the Attorney General by comparing—

4 “(A) the minimization procedures proposed
5 with the minimization procedures actually im-
6 plemented;

7 “(B) the nature of the information sought
8 with the nature of the information actually ob-
9 tained; and

10 “(C) the means and operational procedures
11 proposed with the means and operational proce-
12 dures actually implemented; and

13 “(2) whether foreign intelligence information
14 has been obtained through the electronic surveillance
15 program.

16 “(c) CONTENTS OF ORDER.—An order approving an
17 electronic surveillance program under this section shall di-
18 rect—

19 “(1) that the minimization procedures be fol-
20 lowed;

21 “(2) that, upon the request of the applicant,
22 specified communication or other common carriers,
23 landlords, custodians, or other specified person, fur-
24 nish the applicant forthwith with all information, fa-
25 cilities, or technical assistance necessary to under-

1 take the electronic surveillance program in such a
2 manner as will protect its secrecy and produce a
3 minimum of interference with the services that such
4 carriers, landlords, custodians, or other persons are
5 providing potential targets of the electronic surveil-
6 lance program;

7 “(3) that any record concerning the electronic
8 surveillance program or the aid furnished or retained
9 by such carriers, landlords, custodians, or other per-
10 sons are maintained under security procedures ap-
11 proved by the Attorney General and the Director of
12 National Intelligence; and

13 “(4) that the applicant compensate, at the pre-
14 vailing rate, such carriers, landlords, custodians, or
15 other persons for furnishing such aid.”.

16 **SEC. 7. CONGRESSIONAL OVERSIGHT.**

17 Title VII of the Foreign Intelligence Surveillance Act
18 of 1978, as amended by section 6, is amended by adding
19 at the end the following:

20 **“SEC. 705. CONGRESSIONAL OVERSIGHT.**

21 “(a) IN GENERAL.—Not less often than every 180
22 days, the Attorney General shall submit to the congres-
23 sional intelligence committees a report in classified form
24 on the activities during the previous 180-day period under

1 any electronic surveillance program authorized under this
2 title.

3 “(b) CONTENTS.—Each report submitted under sub-
4 section (a) shall provide, with respect to the previous 180-
5 day period, a description of—

6 “(1) the minimization procedures implemented;

7 “(2) the means and operational procedures by
8 which the surveillance was executed and effected;

9 “(3) significant decisions of the Foreign Intel-
10 ligence Surveillance Court on applications made
11 under section 703;

12 “(4) the total number of applications made for
13 orders approving electronic surveillance pursuant to
14 this title; and

15 “(5) the total number of orders applied for that
16 are granted, modified, or denied.

17 “(c) RULE OF CONSTRUCTION.—Nothing in this title
18 shall be construed to limit the authority or responsibility
19 of any committee of either House of Congress to obtain
20 such information as such committee may need to carry
21 out its respective functions and duties.”

22 **SEC. 8. CLARIFICATION OF THE FOREIGN INTELLIGENCE**
23 **SURVEILLANCE ACT OF 1978.**

24 (a) IN GENERAL.—The Foreign Intelligence Surveil-
25 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended

1 by inserting after title VII, as amended by this Act, the
2 following:

3 **“TITLE VIII—EXECUTIVE**
4 **AUTHORITY**

5 **“SEC. 801. EXECUTIVE AUTHORITY.**

6 “Nothing in this Act shall be construed to limit the
7 constitutional authority of the President to collect intel-
8 ligence with respect to foreign powers and agents of for-
9 eign powers.”.

10 (b) REPEAL.—Sections 111, 309, and 404 of the
11 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.
12 1811, 1829, and 1844) are repealed.

13 (c) CONFORMING AMENDMENTS.—

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

16 (A) in paragraph (e), by striking “, as de-
17 fined in section 101” and all that follows
18 through the end of the paragraph and inserting
19 the following: “under the Constitution or the
20 Foreign Intelligence Surveillance Act of 1978.”;
21 and

22 (B) in paragraph (f), by striking “from
23 international or foreign communications,” and
24 all that follows through the end of the para-
25 graph and inserting “that is authorized under

1 a Federal statute or the Constitution of the
2 United States.”

3 (2) FISA.—Section 109 of the Foreign Intel-
4 ligence Surveillance Act of 1978 (50 U.S.C. 1809)
5 is amended—

6 (A) in subsection (a)—

7 (i) in paragraph (1)—

8 (I) by inserting “or under the
9 Constitution” after “authorized by
10 statute”; and

11 (II) by striking “or” at the end;

12 (ii) in paragraph (2)—

13 (I) by inserting “or under the
14 Constitution” after “authorized by
15 statute”; and

16 (II) by striking the period and
17 inserting “; or”; and

18 (iii) by adding at the end the fol-
19 lowing:

20 “(3) knowingly discloses or uses information ob-
21 tained under color of law by electronic surveillance
22 in a manner or for a purpose not authorized by
23 law.”; and

24 (B) in subsection (c)—

- 1 (i) by striking “\$10,000” and insert-
2 ing “\$100,000”; and
3 (ii) by striking “five years” and in-
4 sserting “15 years”.

5 **SEC. 9. OTHER CONFORMING AMENDMENTS TO FISA.**

6 (a) REFERENCE.—In this section, a reference to
7 “FISA” shall mean the Foreign Intelligence Surveillance
8 Act of 1978 (50 U.S.C. 1801 et seq.)

9 (b) DEFINITIONS.—Section 101 of FISA (50 U.S.C.
10 1801) is amended—

11 (1) in subsection (b)(1)—

12 (A) in subparagraph (B), by striking “or”
13 after the semicolon; and

14 (B) by adding at the end the following:

15 “(D) otherwise possesses or is expected to
16 transmit or receive foreign intelligence informa-
17 tion within the United States; or”;

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

20 “(f) ‘Electronic surveillance’ means—

21 “(1) the installation or use of an electronic, me-
22 chanical, or other surveillance device for the inten-
23 tional collection of information concerning a par-
24 ticular known person who is reasonably believed to
25 be in the United States by intentionally targeting

1 that person under circumstances in which that per-
2 son has a reasonable expectation of privacy and a
3 warrant would be required for law enforcement pur-
4 poses; or

5 “(2) the intentional acquisition of the contents
6 of any communication under circumstances in which
7 a person has a reasonable expectation of privacy and
8 a warrant would be required for law enforcement
9 purposes, and if both the sender and all intended re-
10 cipients are located within the United States.”;

11 (3) in subsection (g), by inserting before the pe-
12 riod the following: “or a person or persons des-
13 igned by the Attorney General or Acting Attorney
14 General”;

15 (4) in subsection (h)—

16 (A) in paragraph (2), by inserting “and”
17 after the semicolon;

18 (B) in paragraph (3), by striking “; and”
19 and inserting a period; and

20 (C) by striking paragraph (4); and

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

23 “(n) ‘contents’ has the meaning set forth in section
24 2510(8) of title 18, United States Code.”.

1 (c) ELECTRONIC SURVEILLANCE AUTHORIZATION.—

2 Section 102 of FISA (50 U.S.C. 1802) is amended to read

3 as follows:

4 “ELECTRONIC SURVEILLANCE AUTHORIZATION WITHOUT

5 COURT ORDER; CERTIFICATION BY ATTORNEY GEN-

6 ERAL; REPORTS TO CONGRESSIONAL COMMITTEES;

7 TRANSMITTAL UNDER SEAL; DUTIES AND COM-

8 PENSATION OF COMMUNICATION COMMON CARRIER;

9 APPLICATIONS; JURISDICTION OF COURT

10 “SEC. 102. (a)(1) Notwithstanding any other law, the

11 President through the Attorney General, may authorize

12 electronic surveillance without a court order under this

13 title to acquire foreign intelligence information for periods

14 of up to 1 year if the Attorney General certifies in writing

15 under oath that—

16 “(A)(i) the acquisition of the contents of com-

17 munications of foreign powers, as defined in section

18 101(a), an agent of a foreign power as defined in

19 section 101(b)(1); or

20 “(ii) the acquisition of technical intelligence,

21 other than the spoken communications of individ-

22 uals, from property or premises under the open and

23 exclusive control of a foreign power, as defined in

24 paragraph (1), (2), or (3) of section 101(a); and

1 “(B) the proposed minimization procedures
2 with respect to such surveillance meet the definition
3 of minimization procedures under section 101(h);
4 if the Attorney General reports such minimization proce-
5 dures and any changes thereto to the Senate Select Com-
6 mittee on Intelligence and the House Permanent Select
7 Committee on Intelligence at least 30 days prior to their
8 effective date, unless the Attorney General determines im-
9 mediate action is required and notifies the committees im-
10 mediately of such minimization procedures and the reason
11 for their becoming effective immediately.

12 “(2) An electronic surveillance authorized by this
13 subsection may be conducted only in accordance with the
14 Attorney General’s certification and the minimization pro-
15 cedures. The Attorney General shall assess compliance
16 with such procedures and shall report such assessments
17 to the Senate Select Committee on Intelligence and the
18 House Permanent Select Committee on Intelligence under
19 the provisions of section 108(a).

20 “(3) The Attorney General shall immediately trans-
21 mit under seal to the court established under section
22 103(a) a copy of his certification. Such certification shall
23 be maintained under security measures established by the
24 Chief Justice with the concurrence of the Attorney Gen-

1 eral, in consultation with the Director of National Intel-
2 ligence, and shall remain sealed unless—

3 “(A) an application for a court order with re-
4 spect to the surveillance is made under section 104;
5 or

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

8 “(b) The Attorney General is also authorized to de-
9 liver to a provider of any electronic communication service,
10 landlord, custodian, or other person (including any officer,
11 employee, agent, or other specified person thereof) who
12 has access to electronic communications, either as they are
13 transmitted or while they are stored, or equipment that
14 is being or may be used to transmit or store such commu-
15 nications, a certificate requiring that such person or per-
16 sons furnish any information, facilities, or technical assist-
17 ance to an official authorized by the President to engage
18 in electronic surveillance for foreign intelligence purposes,
19 for periods of up to 1 year if the Attorney General certifies
20 in writing to the carrier under oath that such provision
21 of information, facilities, or technical assistance does not
22 constitute electronic surveillance as defined in section
23 101(f).

24 “(c) With respect to electronic surveillance or the fur-
25 nishing of any information, facilities, or technical assist-

1 ance authorized by this section, the Attorney General may
2 direct a provider of any electronic communication service,
3 landlord, custodian or other person (including any officer,
4 employee, agent, or other specified person thereof) who
5 has access to electronic communications, either as they are
6 transmitted or while they are stored or equipment that
7 is being or may be used to transmit or store such commu-
8 nications to—

9 “(1) furnish all information, facilities, or tech-
10 nical assistance necessary to accomplish the elec-
11 tronic surveillance in such a manner as will protect
12 its secrecy and produce a minimum of interference
13 with the services that such provider of any electronic
14 communication service, landlord, custodian, or other
15 person is providing its customers; and

16 “(2) maintain under security procedures ap-
17 proved by the Attorney General and the Director of
18 National Intelligence any records concerning the sur-
19 veillance or the aid furnished which such provider of
20 any electronic communication service, landlord, cus-
21 todian, or other person wishes to retain.

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

1 “(d) Electronic surveillance directed solely at the col-
2 lection of international radio communications of diplomati-
3 cally immune persons in the United States may be author-
4 ized by an official authorized by the President to engage
5 in electronic surveillance for foreign intelligence purposes
6 in accordance with procedures approved by the Attorney
7 General.”.

8 (d) DESIGNATION OF JUDGES.—Section 103 of FISA
9 (50 U.S.C. 1803) is amended in subsection (a), by insert-
10 ing, “at least” before “seven of the United States Judici-
11 ary”.

12 (e) APPLICATIONS FOR COURT ORDERS.—Section
13 104 of FISA (50 U.S.C. 1804) is amended:

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

16 “(6) a certification or certifications by the As-
17 sistant to the President for National Security Af-
18 fairs or an executive branch official authorized by
19 the President to conduct electronic surveillance for
20 foreign intelligence purposes—

21 “(A) that the certifying official deems the
22 information sought to be foreign intelligence in-
23 formation;

1 “(B) that a significant purpose of the sur-
2 veillance is to obtain foreign intelligence infor-
3 mation;

4 “(C) that such information cannot reason-
5 ably be obtained by normal investigative tech-
6 niques; and

7 “(D) including a statement of the basis for
8 the certification that—

9 “(i) the information sought is the type
10 of foreign intelligence information des-
11 ignated; and

12 “(ii) such information cannot reason-
13 ably be obtained by normal investigative
14 techniques; and

15 “(7) a statement of the period of time for which
16 the electronic surveillance is required to be main-
17 tained, and if the nature of the intelligence gath-
18 ering is such that the approval of the use of elec-
19 tronic surveillance under this title should not auto-
20 matically terminate when the described type of infor-
21 mation has first been obtained, a description of facts
22 supporting the belief that additional information of
23 the same type will be obtained thereafter.”;

24 (2) by striking subsection (b); and

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

3 (f) ISSUANCE OF ORDER.—Section 105 of FISA (50
4 U.S.C. 1805) is amended—

5 (1) in subsection (a), by—

6 (A) striking paragraph (1); and

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

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

11 “(1) An order approving an electronic surveillance
12 under this section shall specify—

13 “(A) the identity, if known, or a description of
14 the specific target of the electronic surveillance iden-
15 tified or described in the application pursuant to sec-
16 tion 104(a)(3);

17 “(B) the nature and location of each of the fa-
18 cilities or places at which the electronic surveillance
19 will be directed, if known; and

20 “(C) the period of time during which the elec-
21 tronic surveillance is approved.”;

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

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

4 (4) by striking paragraphs (1) and (2) of sub-
5 section (e) and inserting the following:

6 “(1) An order issued under this section may approve
7 an electronic surveillance may be for a period not to exceed
8 1 year. If such emergency employment of electronic sur-
9 veillance is authorized, the official authorizing the emer-
10 gency employment of electronic surveillance shall require
11 that the minimization procedures required by this title for
12 the issuance of a judicial order be followed.

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

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

20 “(f)(1) Notwithstanding any other provision of this
21 title, when an official authorized by the President to con-
22 duct electronic surveillance reasonably determines that—

23 “(A) an emergency situation exists with respect
24 to the employment of electronic surveillance to ob-
25 tain foreign intelligence information before an order

1 authorizing such surveillance can with due diligence
2 be obtained; and

3 “(B) the factual basis for issuance of an order
4 under this title to approve such surveillance exists;
5 that official may authorize the emergency employment of
6 electronic surveillance in accordance with paragraph (2).

7 “(2) Under paragraph (1), the following require-
8 ments shall be satisfied:

9 “(A) The Attorney General shall be informed of
10 the emergency electronic surveillance.

11 “(B) A judge having jurisdiction under section
12 103 shall be informed by the Attorney General or
13 his designee as soon as practicable following such
14 authorization that the decision has been made to
15 employ emergency electronic surveillance.

16 “(C) An application in accordance with this
17 title shall be made to that judge or another judge
18 having jurisdiction under section 103 as soon as
19 practicable, but not more than 7 days after such
20 surveillance is authorized. In the absence of a judi-
21 cial order approving such electronic surveillance, the
22 surveillance shall terminate when the information
23 sought is obtained, when the application for the
24 order is denied, or after the expiration of 7 days
25 from the time of emergency authorization, whichever

1 is earliest. In the event that such application for ap-
2 proval is denied, or in any other case where the elec-
3 tronic surveillance is terminated and no order is
4 issued approving the surveillance, no information ob-
5 tained or evidence derived from such surveillance
6 shall be received in evidence or otherwise disclosed
7 in any trial, hearing, or other proceeding in or be-
8 fore any court, grand jury, department, office, agen-
9 cy, regulatory body, legislative committee, or other
10 authority of the United States, a State, or political
11 subdivision thereof, and no information concerning
12 any United States person acquired from such sur-
13 veillance shall subsequently be used or disclosed in
14 any other manner by Federal officers or employees
15 without the consent of such person, except with the
16 approval of the Attorney General if the information
17 indicates a threat of death or serious bodily harm to
18 any person. A denial of the application made under
19 this subsection may be reviewed as provided in sec-
20 tion 103.”; and

21 (6) in subsection (i) by—

22 (A) striking “a wire or” and inserting
23 “any”;

24 (B) striking “chapter” and inserting
25 “title”; and

1 (C) by adding at the end “, or in response
2 to certification by the Attorney General or his
3 designee seeking information, facilities, or tech-
4 nical assistance from such person that does not
5 constitute electronic surveillance as defined in
6 section 101(f)”.

7 (g) USE OF INFORMATION.—Section 106 of FISA
8 (50U.S.C. 1806) is amended—

9 (1) in subsection (i), by—

10 (A) deleting “radio”; and

11 (B) inserting “Attorney General deter-
12 mines that the content” after “contain signifi-
13 cant foreign intelligence or”; and

14 (2) in subsection (k), by deleting “104(a)(7)”
15 and inserting “104(a)(6)”.

16 (h) CONGRESSIONAL OVERSIGHT.—Section 108 of
17 FISA (50 U.S.C. 1808) is amended by adding at the end
18 the following:

19 “(c) DOCUMENT MANAGEMENT SYSTEM FOR APPLI-
20 CATIONS FOR ORDERS APPROVING ELECTRONIC SURVEIL-
21 LANCE.—

22 “(1) SYSTEM PROPOSED.—The Attorney Gen-
23 eral and Director of National Intelligence shall, in
24 consultation with the Director of the Federal Bu-
25 reau of Investigation, the Director of the National

1 Security Agency, the Director of the Central Intel-
2 ligence Agency, and the Foreign Intelligence Surveil-
3 lance Court, conduct a feasibility study to develop
4 and implement a secure, classified document man-
5 agement system that permits the prompt prepara-
6 tion, modification, and review by appropriate per-
7 sonnel of the Department of Justice, the Federal
8 Bureau of Investigation, the National Security
9 Agency, and other applicable elements of the United
10 States Government of applications under section 104
11 before their submittal to the Foreign Intelligence
12 Surveillance Court.

13 “(2) SCOPE OF SYSTEM.—The document man-
14 agement system proposed in paragraph (1) shall—

15 “(A) permit and facilitate the prompt sub-
16 mittal of applications and all other matters, in-
17 cluding electronic filings, to the Foreign Intel-
18 ligence Surveillance Court under section 104 or
19 105(g)(5); and

20 “(B) permit and facilitate the prompt
21 transmittal of rulings of the Foreign Intel-
22 ligence Surveillance Court to personnel submit-
23 ting applications described in paragraph (1).”.

1 (i) CRIMINAL SANCTIONS.—Section 109 of FISA (50
2 U.S.C. 1809) is amended by striking subsection (a) and
3 inserting the following:

4 “(a) PROHIBITED ACTIVITIES.—A person is guilty of
5 an offense if he intentionally—

6 “(1) engages in electronic surveillance, as de-
7 fined in section 101(f), under color of law except as
8 authorized by law; or

9 “(2) discloses or uses information obtained
10 under color of law by electronic surveillance, know-
11 ing or having reason to know that the information
12 was obtained through electronic surveillance not au-
13 thorized by law.”.

14 (j) AUTHORIZATION DURING TIME OF WAR.—Title
15 I of FISA is amended by striking section 111.

16 (k) PHYSICAL SEARCHES.—Title III of Foreign Intel-
17 ligence Surveillance Act of 1978 (50 U.S.C. 1821 et seq.)
18 is amended—

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

21 “(5) ‘Physical search’ means any physical intru-
22 sion within the United States into premises or prop-
23 erty (including examination of the interior of prop-
24 erty by technical means) that is intended to result
25 in a seizure, reproduction, inspection, or alteration

1 of information, material, or property, under cir-
2 cumstances in which a person has a reasonable ex-
3 pectation of privacy and a warrant would be re-
4 quired for law enforcement purposes, but does not
5 include activities conducted in accordance with sec-
6 tions 102 or 105.”;

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

9 “(a) A person is guilty of an offense if he inten-
10 tionally—

11 “(1) under color of law for the purpose of ob-
12 taining foreign intelligence information, executes a
13 physical search within the United States except as
14 authorized by statute or under the Constitution; or

15 “(2) discloses or uses information obtained
16 under color of law by physical search within the
17 United States, knowing or having reason to know
18 that the information was obtained through physical
19 search not authorized by statute or the Constitu-
20 tion.”; and

21 (3) by striking section 309.

22 **SEC. 10. CONFORMING AMENDMENT TO TABLE OF CON-**
23 **TENTS.**

24 The table of contents for the Foreign Intelligence
25 Surveillance Act of 1978 is amended by striking the items

1 related to title VII and section 701 and inserting the fol-
2 lowing:

“TITLE VII—ELECTRONIC SURVEILLANCE

“Sec. 701. Definition.

“Sec. 702. Foreign intelligence surveillance court jurisdiction to review elec-
tronic surveillance programs.

“Sec. 703. Applications for approval of electronic surveillance programs.

“Sec. 704. Approval of electronic surveillance programs.

“Sec. 705. Congressional oversight.

“TITLE VIII—EXECUTIVE AUTHORITY

“Sec. 801. Executive authority.”.