

Calendar No. **635**109TH CONGRESS
2^D SESSION**S. 3931**

To establish procedures for the review of electronic surveillance programs.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 22, 2006

Mr. McCONNELL (for himself and Mr. FRIST) introduced the following bill; which was read the first time pursuant to the order of September 21, 2006, as modified on September 22, 2006

SEPTEMBER 25, 2006

Read the second time and placed on the calendar

A BILL

To establish procedures for the review of electronic surveillance programs.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

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

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) After the terrorist attacks of September 11,
2 2001, President Bush authorized the National Security
3 Agency to intercept communications between
4 people inside the United States, including American
5 citizens, and terrorism suspects overseas.

6 (2) One of the lessons learned from September
7 11, 2001, is that the enemies who seek to greatly
8 harm and terrorize our Nation utilize technologies
9 and techniques that defy conventional law enforcement
10 practices.

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

16 (4) It is equally essential, however, that in protecting
17 the United States against our enemies, the
18 President does not compromise the very civil liberties
19 that he seeks to safeguard. As Justice Hugo
20 Black observed, “The President’s power, if any, to
21 issue [an] order must stem either from an Act of
22 Congress or from the Constitution itself.” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579,
23 585 (1952) (opinion by Black, J.). Similarly, in
24 2004, Justice Sandra Day O’Connor explained in
25

1 her plurality opinion for the Supreme Court in
2 Hamdi v. Rumsfeld: “We have long since made clear
3 that a state of war is not a blank check for the
4 President when it comes to the rights of the Na-
5 tion’s citizens.” Hamdi v. Rumsfeld, 542 U.S. 507,
6 536 (2004) (citations omitted).

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

16 (6) As Justice Sandra Day O’Connor explained
17 in her plurality opinion for the Supreme Court in
18 Hamdi v. Rumsfeld, “Whatever power the United
19 States Constitution envisions for the Executive in its
20 exchanges with other nations or with enemy organi-
21 zations in times of conflict, it most assuredly envi-
22 sions a role for all 3 branches when individual lib-
23 erties are at stake.” Hamdi v. Rumsfeld, 542 U.S.
24 507, 536 (2004) (citations omitted).

1 (7) Similarly, Justice Jackson famously ex-
2 plained in his *Youngstown* concurrence: “When the
3 President acts pursuant to an express or implied au-
4 thorization of Congress, his authority is at its max-
5 imum, for it includes all that he possesses in his own
6 right plus all that Congress can delegate ... When
7 the President acts in absence of either a congres-
8 sional grant or denial of authority, he can only rely
9 upon his own independent powers, but there is a
10 zone of twilight in which he and Congress may have
11 concurrent authority, or in which its distribution is
12 uncertain. Therefore, congressional inertia, indiffer-
13 ence or quiescence may sometimes, at least as a
14 practical matter, enable, if not invite, measures on
15 independent presidential responsibility ... When the
16 President takes measures incompatible with the ex-
17 pressed or implied will of Congress, his power is at
18 its lowest ebb, for then he can rely only upon his
19 own constitutional powers minus any constitutional
20 powers of Congress over the matter. Courts can sus-
21 tain exclusive Presidential control in such a case
22 only by disabling the Congress from acting upon the
23 subject.” *Youngstown Sheet & Tube Co. v. Sawyer*,
24 343 U.S. 579, 635–38 (1952) (Jackson, J., concur-
25 ring).

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

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

11 (B) “To raise and support Armies”;

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

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

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

18 (F) “To provide for organizing, arming,
19 and disciplining the Militia, and for governing
20 such Part of them as may be employed in the
21 Service of the United States”.

22 (9) While Attorney General Alberto Gonzales
23 explained that the executive branch reviews the elec-
24 tronic surveillance program of the National Security
25 Agency every 45 days to ensure that the program is

1 not overly broad, it is the belief of Congress that ap-
2 proval and supervision of electronic surveillance pro-
3 grams should be conducted outside of the executive
4 branch, by the article III court established under
5 section 103 of the Foreign Intelligence Surveillance
6 Act of 1978 (50 U.S.C. 1803) and the congressional
7 intelligence committees. It is also the belief of Con-
8 gress that it is appropriate for an article III court
9 to pass upon the constitutionality of electronic sur-
10 veillance programs that may be directed at Ameri-
11 cans.

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

19 (11) In 1975, [then] Attorney General Edward
20 Levi, a strong defender of executive authority, testi-
21 fied that in times of conflict, the President needs the
22 power to conduct long-range electronic surveillance
23 and that a foreign intelligence surveillance court
24 should be empowered to issue special approval orders
25 in these circumstances.

1 (12) Granting the Foreign Intelligence Surveil-
2 lance Court the authority to review electronic sur-
3 veillance programs and pass upon their constitu-
4 tionality is consistent with well-established, long-
5 standing practices.

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

13 (14) Prosecutors have significant flexibility in
14 investigating domestic conspiracy cases. Courts have
15 held that flexible warrants comply with the 4th
16 amendment to the Constitution of the United States
17 when they relate to complex, far-reaching, and
18 multifaceted criminal enterprises like drug conspir-
19 acies and money laundering rings. The courts recog-
20 nize that applications for search warrants must be
21 judged in a common sense and realistic fashion, and
22 the courts permit broad warrant language where,
23 due to the nature and circumstances of the inves-
24 tigation and the criminal organization, more precise
25 descriptions are not feasible.

1 (15) The Supreme Court, in the “Keith Case”,
2 United States v. United States District Court for
3 the Eastern District of Michigan, 407 U.S. 297
4 (1972), recognized that the standards and proce-
5 dures used to fight ordinary crime may not be appli-
6 cable to cases involving national security. The Court
7 recognized that national “security surveillance may
8 involve different policy and practical considerations
9 from the surveillance of ordinary crime” and that
10 courts should be more flexible in issuing warrants in
11 national security cases. United States v. United
12 States District Court for the Eastern District of
13 Michigan, 407 U.S. 297, 322 (1972).

14 (16) By authorizing the Foreign Intelligence
15 Surveillance Court to review electronic surveillance
16 programs, Congress enables the President to use the
17 necessary means to guard our national security,
18 while also protecting the civil liberties and constitu-
19 tional rights that we cherish.

20 **SEC. 3. DEFINITIONS.**

21 The Foreign Intelligence Surveillance Act of 1978
22 (50 U.S.C. 1801 et seq.) is amended—

23 (1) by redesignating title VII as title VIII;

24 (2) by redesignating section 701 as section 801;

25 and

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

2 **“TITLE VII—ELECTRONIC**
3 **SURVEILLANCE PROGRAMS**

4 **“SEC. 701. DEFINITIONS.**

5 “As used in this title—

6 “(1) the terms ‘agent of a foreign power’, ‘At-
7 torney General’, ‘contents’, ‘electronic surveillance’,
8 ‘foreign power’, ‘international terrorism’, ‘minimiza-
9 tion procedures’, ‘person’, ‘United States’, and
10 ‘United States person’ have the same meaning as in
11 section 101;

12 “(2) the term ‘congressional intelligence com-
13 mittees’ means the Select Committee on Intelligence
14 of the Senate and the Permanent Select Committee
15 on Intelligence of the House of Representatives;

16 “(3) the term ‘electronic surveillance program’
17 means a program to engage in electronic surveil-
18 lance—

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

22 “(B) where it is not feasible to name every
23 person, address, or location to be subjected to
24 electronic surveillance;

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

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

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

18 **SEC. 4. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
19 **JURISDICTION TO REVIEW ELECTRONIC SUR-**
20 **VEILLANCE PROGRAMS.**

21 (a) IN GENERAL.—Title VII of the Foreign Intel-
22 ligence Surveillance Act of 1978, as amended by section
23 3, is amended by adding at the end the following:

1 **“SEC. 702. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
2 **JURISDICTION TO REVIEW ELECTRONIC SUR-**
3 **VEILLANCE PROGRAMS.**

4 “(a) AUTHORIZATION OF REVIEW.—

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

12 “(2) REAUTHORIZATION.—The Foreign Intel-
13 ligence Surveillance Court shall have jurisdiction to
14 reauthorize an electronic surveillance program for a
15 period of time not longer than such court determines
16 to be reasonable. There shall be no limit on the
17 number of times the Attorney General may seek re-
18 authorization of an electronic surveillance program.

19 “(3) RESUBMISSION OR APPEAL.—In the event
20 that the Foreign Intelligence Surveillance Court re-
21 fuses to approve an application under this sub-
22 section, the court shall state its reasons in a written
23 opinion, which it shall submit to the Attorney Gen-
24 eral. The Attorney General or his designee may sub-
25 mit a new application under section 703 for the elec-
26 tronic surveillance program, with no limit on the

1 number of resubmissions that may be made. Alter-
2 natively, the Attorney General may appeal the deci-
3 sion of the Foreign Intelligence Surveillance Court
4 to the Foreign Intelligence Surveillance Court of Re-
5 view.

6 “(4) CONTINUED SURVEILLANCE UNDER TITLE
7 I.—

8 “(A) IN GENERAL.—If, at any time, the
9 Attorney General determines that the known
10 facts and circumstances relating to any target
11 within the United States under this title satisfy
12 the criteria for an application under section 104
13 for an order for electronic surveillance of the
14 target under section 105, the Attorney General
15 shall—

16 “(i) discontinue the surveillance of the
17 target under this title; or

18 “(ii) continue the surveillance of the
19 target under this title, subject to the re-
20 quirements of subparagraph (B).

21 “(B) CONTINUATION OF SURVEILLANCE.—

22 “(i) IN GENERAL.—The Attorney
23 General may continue surveillance of a tar-
24 get under this title as specified in subpara-
25 graph (A)(ii) only if the Attorney General

1 makes an application under section 104 for
2 an order for electronic surveillance of the
3 target under section 105 as soon as the
4 Attorney General determines practicable
5 after the date on which the Attorney Gen-
6 eral makes the determination to continue
7 surveillance of the target under subpara-
8 graph (A)(ii).

9 “(ii) PERIOD.—The period during
10 which the Attorney General may continue
11 surveillance of a target under this title
12 after the Attorney General has determined
13 that making an application is practicable
14 shall be limited to a reasonable period, as
15 determined by the Attorney General, dur-
16 ing which the application is prepared and
17 the period during which the application of
18 the Attorney General under section 104 for
19 an order for electronic surveillance of the
20 target under section 105 is pending under
21 title I, including during any period in
22 which appeal from the denial of the appli-
23 cation is pending with the Foreign Intel-
24 ligence Surveillance Court of Review or the
25 Supreme Court under section 103(b).

1 “(b) MANDATORY TRANSFER FOR REVIEW.—

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

15 “(2) PROCEDURES FOR REVIEW.—The Foreign
16 Intelligence Surveillance Court shall have jurisdic-
17 tion as appropriate to determine standing and the
18 legality of the program to the extent necessary for
19 resolution of the underlying case. All proceedings
20 under this paragraph shall be conducted in accord-
21 ance with the procedures set forth in section 106(f).
22 In the event the Foreign Intelligence Surveillance
23 Court determines that, in the context of a criminal
24 proceeding, the Constitution of the United States
25 would require the disclosure of national security in-

1 formation, any such constitutionally required disclo-
2 sure shall be governed by the Classified Information
3 Procedures Act, (18 U.S.C. App.), or if applicable,
4 section 2339B(f) of title 18, United States Code.

5 “(3) APPEAL, CERTIORARI, AND EFFECTS OF
6 DECISIONS.—The decision of the Foreign Intel-
7 ligence Surveillance Court made under paragraphs
8 (1) and (2), including a decision that the disclosure
9 of national security information is constitutionally
10 required, shall be subject to review by the Foreign
11 Intelligence Surveillance Court of Review under sec-
12 tion 103(b). The Supreme Court of the United
13 States shall have jurisdiction to review decisions of
14 the Foreign Intelligence Surveillance Court of Re-
15 view by writ of certiorari granted upon the petition
16 of the United States. The decision by the Foreign
17 Intelligence Surveillance Court shall otherwise be
18 binding in all other courts.

19 “(4) DISMISSAL.—The Foreign Intelligence
20 Surveillance Court or a court that is an originating
21 court under paragraph (1) may dismiss a challenge
22 to the legality of an electronic surveillance program
23 for any reason provided for under law.

24 “(5) PRESERVATION OF LITIGATION PRIVI-
25 LEGES.—Nothing in this Act shall be construed to

1 abrogate, limit, or affect any litigation privileges in
2 any court.”.

3 **SEC. 5. APPLICATIONS FOR APPROVAL OF ELECTRONIC**
4 **SURVEILLANCE PROGRAMS.**

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

8 **“SEC. 703. APPLICATIONS FOR APPROVAL OF ELECTRONIC**
9 **SURVEILLANCE PROGRAMS.**

10 “(a) IN GENERAL.—Each application for approval of
11 an electronic surveillance program under this title (includ-
12 ing resubmission or application for reauthorization)
13 shall—

14 “(1) be made by the Attorney General or his
15 designee;

16 “(2) include a statement of the authority con-
17 ferred on the Attorney General by the President of
18 the United States;

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

23 “(4) certify that a significant purpose of the
24 electronic surveillance program is to obtain foreign

1 intelligence information or to protect against inter-
2 national terrorism;

3 “(5) certify that the information sought cannot
4 reasonably be obtained by normal investigative tech-
5 niques

6 “(6) certify that the information sought cannot
7 reasonably be obtained through an application under
8 section 104;

9 “(7) include a statement of the means and
10 operational procedures by which the electronic sur-
11 veillance will be executed and effected;

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

16 “(A) a foreign power that engages in inter-
17 national terrorism or activities in preparation
18 therefor;

19 “(B) an agent of a foreign power that en-
20 gages in international terrorism or activities in
21 preparation therefor;

22 “(C) a person reasonably believed to have
23 communication with or be associated with a for-
24 eign power that engages in international ter-
25 rorism or activities in preparation therefor or

1 an agent of a foreign power that engages in
2 international terrorism or activities in prepara-
3 tion therefor; or

4 “(D) a foreign power that poses an immi-
5 nent threat of attack likely to cause death, seri-
6 ous injury, or substantial economic damage to
7 the United States, or an agent of a foreign
8 power thereof;

9 “(9) include a statement of the proposed mini-
10 mization procedures;

11 “(10) if the electronic surveillance program that
12 is the subject of the application was initiated prior
13 to the date the application was submitted, specify
14 the date that the program was initiated;

15 “(11) include a description of all previous appli-
16 cations that have been made under this title involv-
17 ing the electronic surveillance program in the appli-
18 cation (including the minimization procedures and
19 the means and operational procedures proposed) and
20 the decision on each previous application; and

21 “(12) include a statement of facts concerning
22 the implementation of the electronic surveillance pro-
23 gram described in the application, including, for any
24 period of operation of the program authorized not

1 less than 90 days prior to the date of submission of
2 the application—

3 “(A) the minimization procedures imple-
4 mented; and

5 “(B) the means and operational procedures
6 by which the electronic surveillance was exe-
7 cuted and effected.

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

12 **SEC. 6. APPROVAL OF ELECTRONIC SURVEILLANCE PRO-**
13 **GRAMS.**

14 Title VII of the Foreign Intelligence Surveillance Act
15 18 of 1978, as amended by section 5, is amended by add-
16 ing at the end the following:

17 **“SEC. 704. APPROVAL OF ELECTRONIC SURVEILLANCE**
18 **PROGRAMS.**

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

24 “(1) the President has authorized the Attorney
25 General to make the application for electronic sur-

1 veillance for foreign intelligence information or to
2 protect against international terrorism;

3 “(2) approval of the electronic surveillance pro-
4 gram in the application is consistent with the Con-
5 stitution of the United States;

6 “(3) the electronic surveillance program is rea-
7 sonably designed to ensure that the communications
8 that are acquired are communications of or with—

9 “(A) a foreign power that engages in inter-
10 national terrorism or activities in preparation
11 therefor;

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

15 “(C) a person reasonably believed to have
16 communication with or be associated with a for-
17 eign power that is engaged in international ter-
18 rorism or activities in preparation therefor or
19 an agent of a foreign power that is engaged in
20 international terrorism or activities in prepara-
21 tion therefor; or

22 “(D) a foreign power that poses an immi-
23 nent threat of attack likely to cause death, seri-
24 ous injury, or substantial economic damage to

1 the United States, or an agent of a foreign
2 power thereof;

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

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

8 “(b) CONSIDERATIONS.—In considering the constitu-
9 tionality of the electronic surveillance program under sub-
10 section (a), the Foreign Intelligence Surveillance Court
11 may consider—

12 “(1) whether the electronic surveillance pro-
13 gram has been implemented in accordance with the
14 proposal by the Attorney General, by comparing—

15 “(A) the minimization procedures proposed
16 with the minimization procedures actually im-
17 plemented;

18 “(B) the nature of the information sought
19 with the nature of the information actually ob-
20 tained; and

21 “(C) the means and operational procedures
22 proposed with the means and operational proce-
23 dures actually implemented; and

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

4 “(c) CONTENTS OF ORDER.—An order approving an
5 electronic surveillance program under this section shall di-
6 rect—

7 “(1) that the minimization procedures be fol-
8 lowed;

9 “(2) that, upon the request of the applicant,
10 specified communication or other common carriers,
11 landlords, custodians, or other specified persons, fur-
12 nish the applicant forthwith with all information, fa-
13 cilities, or technical assistance necessary to under-
14 take the electronic surveillance program in such a
15 manner as will protect its secrecy and produce a
16 minimum of interference with the services that such
17 carriers, landlords, custodians, or other persons are
18 providing potential targets of the electronic surveil-
19 lance program;

20 “(3) that any records concerning the electronic
21 surveillance program or the aid furnished or retained
22 by such carriers, landlords, custodians, or other per-
23 sons are maintained under security procedures ap-
24 proved by the Attorney General and the Director of
25 National Intelligence; and

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

4 **SEC. 7. CONGRESSIONAL OVERSIGHT.**

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

8 **“SEC. 705. CONGRESSIONAL OVERSIGHT.**

9 “(a) IN GENERAL.—Not less often than every 180
10 days, the Attorney General shall submit to the congres-
11 sional intelligence committees a report in classified form
12 on the activities during the previous 180-day period under
13 any electronic surveillance program authorized under this
14 title.

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

18 “(1) the minimization procedures implemented;

19 “(2) the means and operational procedures by
20 which the electronic surveillance program was exe-
21 cuted and effected;

22 “(3) significant decisions of the Foreign Intel-
23 ligence Surveillance Court on applications made
24 under section 703;

1 “(4) the total number of applications made for
2 orders approving electronic surveillance programs
3 pursuant to this title; and

4 “(5) the total number of orders applied for that
5 have been granted, modified, or denied.

6 “(c) **RULE OF CONSTRUCTION.**—Nothing in this title
7 shall be construed to limit the authority or responsibility
8 of any committee of either House of Congress to obtain
9 such information as such committee may need to carry
10 out its respective functions and duties.”.

11 **SEC. 8. CLARIFICATION OF THE FOREIGN INTELLIGENCE**

12 **SURVEILLANCE ACT OF 1978.**

13 (a) **REPEAL.**—Sections 111, 309, and 404 of the
14 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.
15 1811, 1829, and 1844) are repealed.

16 (b) **CLARIFYING AMENDMENTS.**—

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

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

1 (B) in paragraph (f), by striking “from
2 international or foreign communications,” and
3 all that follows through the end of the para-
4 graph and inserting “that is authorized under
5 a Federal statute or the Constitution of the
6 United States.”.

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

10 (A) in subsection (a)—

11 (i) in paragraph (1)—

12 (I) by striking “authorized by
13 statute” and inserting “authorized by
14 law”; and

15 (II) by striking “or” at the end;

16 (ii) in paragraph (2)—

17 (I) by striking “authorized by
18 statute” and inserting “authorized by
19 law”; and

20 (II) by striking the period and
21 inserting “; or”; and

22 (iii) by adding at the end the fol-
23 lowing:

24 “(3) and knowingly discloses or uses informa-
25 tion obtained under color of law by electronic sur-

1 veillance in a manner or for a purpose not author-
2 ized by law.”; and

3 (B) in subsection (c)—

4 (i) by striking “\$10,000” and insert-
5 ing “\$100,000”; and

6 (ii) by striking “five years” and in-
7 serting “15 years”.

8 **SEC. 9. MODERNIZING AMENDMENTS TO FISA.**

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

12 (b) DEFINITIONS.—Section 101 of FISA (50 U.S.C.
13 1801) is amended—

14 (1) in subsection (b)(1)—

15 (A) in subparagraph (C), by striking “or”
16 after the semicolon; and

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

18 “(D) otherwise is reasonably expected to
19 possess, control, transmit, or receive foreign in-
20 telligence information while that person is in
21 the United States, provided that the official
22 making the certification required by section
23 104(a)(6) deems such foreign intelligence infor-
24 mation to be significant; or”;

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

3 “(f) ‘Electronic surveillance’ means—

4 “(1) the installation or use of an electronic, me-
5 chanical, or other surveillance device for acquiring
6 information by intentionally directing the surveil-
7 lance at a particular known person who is reason-
8 ably believed to be in the United States under cir-
9 cumstances in which that person has a reasonable
10 expectation of privacy and a warrant would be re-
11 quired for law enforcement purposes; or

12 “(2) the intentional acquisition of the contents
13 of any communication under circumstances in which
14 a person has a reasonable expectation of privacy and
15 a warrant would be required for law enforcement
16 purposes, and if both the sender and all intended re-
17 cipients are reasonably believed to be located within
18 the United States.”;

19 (3) in subsection (h), by striking paragraph (4)
20 and inserting the following:

21 “(4) notwithstanding paragraphs (1), (2), and
22 (3), with respect to any electronic surveillance ap-
23 proved pursuant to section 102 or 704, procedures
24 that require that no contents of any communication
25 originated or sent by a United States person shall

1 be disclosed, disseminated, used or retained for
2 longer than 7 days unless a court order under sec-
3 tion 105 is obtained or unless the Attorney General
4 determines that the information indicates a threat of
5 death or serious bodily harm to any person.”.

6 (4) by striking subsection (l); and

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

9 “(n) ‘contents’, when used with respect to a commu-
10 nication, includes any information concerning the sub-
11 stance, symbols, sounds, words, purport, or meaning of a
12 communication, and does not include dialing, routing, ad-
13 dressing, or signaling information.”.

14 (c) ELECTRONIC SURVEILLANCE AUTHORIZATION.—
15 Section 102 of FISA (50 U.S.C. 1802) is amended to read
16 as follows:

17 “ELECTRONIC SURVEILLANCE AUTHORIZATION WITHOUT
18 COURT ORDER; CERTIFICATION BY ATTORNEY GEN-
19 ERAL; REPORTS TO CONGRESSIONAL COMMITTEES;
20 TRANSMITTAL UNDER SEAL; DUTIES AND COM-
21 PENSATION OF COMMUNICATION COMMON CARRIER;
22 APPLICATIONS; JURISDICTION OF COURT

23 “SEC. 102. (a)(1) Notwithstanding any other law, the
24 President through the Attorney General, may authorize
25 electronic surveillance without a court order under this
26 title to acquire foreign intelligence information for periods

1 of up to 1 year if the Attorney General certifies in writing
2 under oath that the electronic surveillance is directed at—

3 “(A)(i) the acquisition of the contents of com-
4 munications of foreign powers, as defined in para-
5 graph (1), (2), or (3) of section 101(a), or a person
6 other than a United States person acting as an
7 agent of a foreign power, as defined in section
8 101(b)(1)(A) or (B); or

9 “(ii) the acquisition of technical intelligence,
10 other than the spoken communications of individ-
11 uals, from property or premises under the open and
12 exclusive control of a foreign power, as defined in
13 paragraph (1), (2), or (3) of section 101(a); and

14 “(B) the proposed minimization procedures
15 with respect to such surveillance meet the definition
16 of minimization procedures under section 101(h);

17 if the Attorney General reports such minimization proce-
18 dures and any changes thereto to the Select Committee
19 on Intelligence of the Senate and the Permanent Select
20 Committee on Intelligence of the House of Representatives
21 at least 30 days prior to their effective date, unless the
22 Attorney General determines immediate action is required
23 and notifies the committees immediately of such minimiza-
24 tion procedures and the reason for their becoming effective
25 immediately.

1 “(2) An electronic surveillance authorized by this
2 subsection may be conducted only in accordance with the
3 Attorney General’s certification and the minimization pro-
4 cedures. The Attorney General shall assess compliance
5 with such procedures and shall report such assessments
6 to the Select Committee on Intelligence of the Senate and
7 the Permanent Select Committee on Intelligence of the
8 House of Representatives under section 108(a). If an elec-
9 tronic surveillance authorized by this subsection is di-
10 rected at an agent of a foreign power, the Attorney Gen-
11 eral’s report assessing compliance with the minimization
12 procedures shall also include a statement of the facts and
13 circumstances relied upon to justify the belief that the tar-
14 get of the electronic surveillance is an agent of a foreign
15 power.

16 “(3) The Attorney General shall immediately trans-
17 mit under seal to the court established under section
18 103(a) a copy of any certification under this subsection.
19 Such certification shall be maintained under security
20 measures established by the Chief Justice with the concur-
21 rence of the Attorney General, in consultation with the
22 Director of National Intelligence, and shall remain sealed
23 unless—

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

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

6 “(b)(1) Notwithstanding any other provision of law,
7 the President, through the Attorney General, may author-
8 ize the acquisition of foreign intelligence information for
9 periods of up to 1 year concerning a person reasonably
10 believed to be outside the United States if the Attorney
11 General certifies in writing under oath that he has deter-
12 mined that—

13 “(A) the acquisition does not constitute elec-
14 tronic surveillance as defined in section 101(f);

15 “(B) the acquisition involves obtaining the for-
16 eign intelligence information from or with the assist-
17 ance of a wire or electronic communications service
18 provider, custodian, or other person (including any
19 officer, employee, agent, or other specified person
20 thereof) who has access to wire or electronic commu-
21 nications, either as they are transmitted or while
22 they are stored, or equipment that is being or may
23 be used to transmit or store such communications;

24 “(C) a significant purpose of the acquisition is
25 to obtain foreign intelligence information; and

1 “(D) the minimization procedures to be em-
2 ployed with respect to such acquisition activity meet
3 the definition of minimization procedures under sec-
4 tion 101(h).

5 “(2) Such certification need not identify the specific
6 facilities, places, premises, or property at which the acqui-
7 sition will be directed.

8 “(3) An acquisition undertaken pursuant to this sub-
9 section may be conducted only in accordance with the At-
10 torney General’s certification and the minimization proce-
11 dures adopted by the Attorney General. The Attorney
12 General shall assess compliance with such procedures and
13 shall report such assessments to the Select Committee on
14 Intelligence of the Senate and the Permanent Select Com-
15 mittee on Intelligence of the House of Representatives
16 under section 108(a).

17 “(4) The Attorney General shall immediately trans-
18 mit under seal to the court established under section
19 103(a) a copy of any certification of the Attorney General
20 under this subsection. Such certification shall be main-
21 tained under security measures established by the Chief
22 Justice with the concurrence of the Attorney General, in
23 consultation with the Director of National Intelligence,
24 and shall remain sealed unless the certification is nec-

1 essary to determine the legality of the acquisition under
2 subsection (o).

3 “(c) With respect to the acquisition authorized under
4 this section, the Attorney General may direct a specified
5 person to—

6 “(1) furnish the government forthwith all infor-
7 mation, facilities, and assistance necessary to accom-
8 plish the acquisition in such a manner as will protect
9 its secrecy and produce a minimum of interference
10 with the services that such person is providing to the
11 target; and

12 “(2) maintain under security procedures ap-
13 proved by the Attorney General and the Director of
14 National Intelligence any records concerning the ac-
15 quisition or the aid furnished that such person wish-
16 es to maintain.

17 “(d) The government shall compensate, at the pre-
18 vailing rate, such specified person for furnishing the aid
19 set forth in subsection (c).

20 “(e) In the case of a failure to comply with a directive
21 issued pursuant to this section, the Attorney General may
22 invoke the aid of the court established under section
23 103(a) to compel compliance with the directive. The court
24 shall issue an order requiring the person or entity to com-
25 ply with the directive forthwith if it finds that the directive

1 was issued in accordance with subsection (a) or (b) and
2 is otherwise lawful. Any failure to obey the order of the
3 court may be punished by the court as contempt thereof.
4 Any process under this section may be served in any judi-
5 cial district in which the person or entity may be found.

6 “(f)(1)(A) A person receiving an Attorney General di-
7 rective issued pursuant to this section may challenge the
8 legality of that directive by filing a petition with the pool
9 established by section 103(e)(1).

10 “(B) The presiding judge shall immediately assign a
11 petition to one of the judges serving in the pool established
12 by section 103(e)(1). Not later than 24 hours after the
13 assignment of such petition, the assigned judge shall con-
14 duct an initial review of the directive. If the assigned judge
15 determines that the petition is frivolous, the assigned
16 judge shall immediately deny the petition and affirm the
17 directive or any part thereof that is the subject of the peti-
18 tion. If the assigned judge determines the petition is not
19 frivolous, the assigned judge shall within 72 hours con-
20 sider the petition in accordance with the procedures estab-
21 lished under section 103(e)(2) and provide a written state-
22 ment for the record of the reasons for any determination
23 under this subsection.

24 “(2) A judge considering a petition to modify or set
25 aside a directive may grant such petition only if the judge

1 finds that such directive does not meet the requirements
2 of this section or is otherwise unlawful. If the judge does
3 not modify or set aside the directive, the judge shall imme-
4 diately affirm such directive, and order the recipient to
5 comply therewith.

6 “(3) Any directive not explicitly modified or set aside
7 consistent with this subsection shall remain in full effect.

8 “(g) A petition for review of a decision under sub-
9 section (f) to affirm, modify, or set aside a directive by
10 the Government or any person receiving such directive
11 shall be made within 7 days of issuance of the decision
12 required by subsection (f) to the court of review estab-
13 lished under section 103(b), which shall have jurisdiction
14 to consider such petitions. The court of review shall pro-
15 vide for the record a written statement of the reasons for
16 its decision and, on petition by the Government or any
17 person receiving such directive for a writ of certiorari, the
18 record shall be transmitted under seal to the Supreme
19 Court of the United States, which shall have jurisdiction
20 to review such decision.

21 “(h) Judicial proceedings under this section shall be
22 concluded as expeditiously as possible. The record of pro-
23 ceedings, including petitions filed, orders granted, and
24 statements of reasons for decision, shall be maintained
25 under security measures established by the Chief Justice

1 of the United States, in consultation with the Attorney
2 General and the Director of National Intelligence.

3 “(i) All petitions under this section shall be filed
4 under seal. In any proceedings under this section, the
5 court shall, upon request of the Government, review ex
6 parte and in camera any Government submission, or por-
7 tions thereof, which may include classified information.

8 “(j) No cause of action shall lie in any court against
9 any provider of a communication service or other person
10 (including any officer, employee, agent, or other specified
11 person thereof) for furnishing any information, facilities,
12 or assistance in accordance with a directive under sub-
13 section (a) or (b).

14 “(k) Information acquired pursuant to an Attorney
15 General authorization under this section concerning any
16 United States person may be used and disclosed by Fed-
17 eral officers and employees without the consent of the
18 United States person only in accordance with the mini-
19 mization procedures required by subsection (a) or (b), as
20 applicable. No otherwise privileged communication ob-
21 tained in accordance with, or in violation of, the provisions
22 of this section shall lose its privileged character. No infor-
23 mation from an acquisition under this section may be used
24 or disclosed by Federal officers or employees except for
25 lawful purposes.

1 “(l) No information acquired pursuant to this section
2 shall be disclosed for law enforcement purposes unless
3 such disclosure is accompanied by a statement that such
4 information, or any information derived therefrom, may
5 only be used in a criminal proceeding with the advance
6 authorization of the Attorney General.

7 “(m) Whenever the Government intends to enter into
8 evidence or otherwise use or disclose in any trial, hearing,
9 or other proceeding in or before any court, department,
10 officer, agency, regulatory body, or other authority of the
11 United States, against an aggrieved person, any informa-
12 tion obtained or derived from an acquisition under this
13 section, the Government shall, prior to the trial, hearing,
14 or other proceeding or at a reasonable time prior to an
15 effort to so disclose or so use that information or submit
16 it in evidence, notify the aggrieved person and the court
17 or other authority in which the information is to be dis-
18 closed or used that the Government intends to so disclose
19 or so use such information.

20 “(n) Whenever any State or political subdivision
21 thereof intends to enter into evidence or otherwise use or
22 disclose in any trial, hearing, or other proceeding in or
23 before any court, department, officer, agency, regulatory
24 body, or other authority of a State or a political subdivi-
25 sion thereof, against an aggrieved person any information

1 obtained or derived from an acquisition under this section,
2 the State or political subdivision thereof shall notify the
3 aggrieved person, the court or other authority in which
4 the information is to be disclosed or used, and the Attor-
5 ney General that the State or political subdivision thereof
6 intends to so disclose or so use such information.

7 “(o) Any person against whom evidence obtained or
8 derived from an acquisition authorized pursuant to this
9 section to which he is an aggrieved person is to be, or
10 has been, introduced or otherwise used or disclosed in any
11 trial, hearing, or other proceeding in or before any court,
12 department, officer, agency, regulatory body, or other au-
13 thority of the United States, a State, or a political subdivi-
14 sion thereof, may move to suppress the evidence obtained
15 or derived from such acquisition on the grounds that—

16 “(1) the information was unlawfully acquired;

17 or

18 “(2) the acquisition was not made in conformity
19 with an order of authorization or approval.

20 Such a motion shall be made before the trial, hearing, or
21 other proceeding unless there was no opportunity to make
22 such a motion or the person was not aware of the grounds
23 of the motion.

24 “(p) Whenever a court or other authority is notified
25 pursuant to subsection (m) or (n), whenever a motion is

1 made pursuant to subsection (o), or whenever any motion
2 or request is made by an aggrieved person pursuant to
3 any other statute or rule of the United States or any State
4 before any court or other authority of the United States
5 or any State to discover or obtain an Attorney General
6 directive or other materials relating to the acquisition au-
7 thorized under this section or to discover, obtain, or sup-
8 press evidence or information obtained or derived from the
9 acquisition authorized under this section, the United
10 States district court or, where the motion is made before
11 another authority, the United States district court in the
12 same district as the authority, shall, notwithstanding any
13 other law, if the Attorney General files an affidavit under
14 oath that disclosure or an adversary hearing would harm
15 the national security of the United States, review in cam-
16 era and ex parte the directive, and such other materials
17 relating to the acquisition as may be necessary to deter-
18 mine whether the acquisition authorized under this section
19 was lawfully authorized and conducted. In making this de-
20 termination, the court may disclose to the aggrieved per-
21 son, under appropriate security procedures and protective
22 orders, portions of the directive or other materials relating
23 to the acquisition only where such disclosure is necessary
24 to make an accurate determination of the legality of the
25 acquisition.

1 “(q) If the United States district court pursuant to
2 subsection (o) determines that the acquisition authorized
3 under this section was not lawfully authorized or con-
4 ducted, it shall, in accordance with the requirements of
5 law, suppress the evidence which was unlawfully obtained
6 or derived or otherwise grant the motion of the aggrieved
7 person. If the court determines that such acquisition was
8 lawfully authorized and conducted, it shall deny the mo-
9 tion of the aggrieved person except to the extent that due
10 process requires discovery or disclosure.

11 “(r) Orders granting motions or requests under sub-
12 section (o), decisions under this section that an acquisition
13 was not lawfully authorized or conducted, and orders of
14 the United States district court requiring review or grant-
15 ing disclosure of directives or other materials relating to
16 such acquisition shall be final orders and binding upon
17 all courts of the United States and the several States ex-
18 cept a United States court of appeals and the Supreme
19 Court.

20 “(s) Federal officers who acquire foreign intelligence
21 information under this section may consult with Federal
22 law enforcement officers or law enforcement personnel of
23 a State or political subdivision of a State (including the
24 chief executive officer of that State or political subdivision
25 who has the authority to appoint or direct the chief law

1 enforcement officer of that State or political subdivision)
2 to coordinate efforts to investigate or protect against—

3 “(1) actual or potential attack or other grave
4 hostile acts of a foreign power or an agent of a for-
5 eign power;

6 “(2) sabotage, international terrorism, or the
7 development or proliferation of weapons of mass de-
8 struction by a foreign power or an agent of a foreign
9 power; or

10 “(3) clandestine intelligence activities by an in-
11 telligence service or network of a foreign power or by
12 an agent of a foreign power.

13 “(t) Coordination authorized by subsection (s) shall
14 not preclude the certification required by subsection (a)
15 or (b), as applicable.

16 “(u) RETENTION OF DIRECTIVES AND ORDERS.—Di-
17 rectives made and orders granted under this section shall
18 be retained for a period of at least 10 years from the date
19 when they were made.”.

20 (d) DESIGNATION OF JUDGES.—Section 103 of FISA
21 (50 U.S.C. 1803) is amended—

22 (1) in subsection (a), by inserting, “at least”
23 before “seven of the United States judicial circuits”;
24 and

1 (2) at the end by adding the following new sub-
2 section:

3 “(g) Applications for a court order under this title
4 are authorized if the President has, by written authoriza-
5 tion, empowered the Attorney General to approve applica-
6 tions to the court having jurisdiction under this section,
7 and a judge to whom an application is made may, notwith-
8 standing any other law, grant an order, in conformity with
9 section 105, approving electronic surveillance of a foreign
10 power or an agent of a foreign power for the purpose of
11 obtaining foreign intelligence information.”.

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;

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;

1 “(8) a summary description of the nature of the
2 information sought and the type of communications
3 or activities to be subject to the surveillance;

4 “(9) a summary statement of the facts con-
5 cerning all previous applications that have been
6 made to any judge under this title involving any of
7 the persons, facilities, or places specified in the ap-
8 plication, and the action taken on each previous ap-
9 plication; and

10 “(10) a summary statement of the means by
11 which the surveillance will be effected and a state-
12 ment whether physical entry is required to effect the
13 surveillance.”;

14 (2) by striking subsection (b);

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

17 (4) in subsection (d)(1)(A), as redesignated by
18 paragraph (3), by inserting after “Secretary of
19 State” inserting “Director of the Central Intel-
20 ligence Agency”.

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

23 (1) in subsection (a), by—

24 (A) striking paragraph (1); and

1 (B) redesignating paragraphs (2) through
2 (5) as paragraphs (1) through (4), respectively;
3 (2) by striking paragraph (1) of subsection (c)
4 and inserting the following:

5 “(1) An order approving an electronic surveil-
6 lance under this section shall specify—

7 “(A) the identity, if known, or a descrip-
8 tion of the target of the electronic surveillance
9 identified or described in the application pursu-
10 ant to section 104(a)(3);

11 “(B) the nature and location of each of the
12 facilities or places at which the electronic sur-
13 veillance will be directed, if known;

14 “(C) the period of time during which the
15 electronic surveillance is approved;

16 “(D) the type of information sought to be
17 acquired and the type of communications or ac-
18 tivities to be subjected to the surveillance; and

19 “(E) the means by which the electronic
20 surveillance will be effected and whether phys-
21 ical entry will be used to effect the surveil-
22 lance.”;

23 (3) by striking subsection (d) and inserting the
24 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 paragraph (2) of subsection (e)
5 and inserting the following:

6 “(2) Extensions of an order issued under this title
7 may be granted on the same basis as an original order
8 upon an application for an extension and new findings
9 made in the same manner as required for an original order
10 and may be for a period not longer than the court deter-
11 mines to be reasonable or 1 year, whichever is less.”;

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

14 “(f)(1) Notwithstanding any other provision of this
15 title, when an executive branch officer appointed by the
16 President with the advice and consent of the Senate who
17 is authorized by the President to conduct electronic sur-
18 veillance reasonably determines that—

19 “(A) an emergency situation exists with respect
20 to the employment of electronic surveillance to ob-
21 tain foreign intelligence information before an order
22 authorizing such surveillance can with due diligence
23 be obtained; and

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

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

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

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

7 “(B) A judge having jurisdiction under section
8 103 shall be informed by the Attorney General or
9 his designee as soon as practicable following such
10 authorization that the decision has been made to
11 employ emergency electronic surveillance.

12 “(C) An application in accordance with this
13 title shall be made to that judge or another judge
14 having jurisdiction under section 103 as soon as
15 practicable, but not more than 7 days after such
16 surveillance is authorized. In the absence of a judi-
17 cial order approving such electronic surveillance, the
18 surveillance shall terminate when the information
19 sought is obtained, when the application for the
20 order is denied, or after the expiration of 7 days
21 from the time of emergency authorization, whichever
22 is earliest. In the event that such application for ap-
23 proval is denied, or in any other case where the elec-
24 tronic surveillance is terminated and no order is
25 issued approving the surveillance, no information ob-

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

17 “(D) The official authorizing the emergency
18 employment of electronic surveillance shall require
19 that the minimization procedures required by this
20 title for the issuance of a judicial order be fol-
21 lowed.”; and

22 (6) in subsection (i)—

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

1 (B) by striking “chapter” and inserting
2 “title”; and

3 (C) by adding at the end “, or in response
4 to certification by the Attorney General or his
5 designee seeking information, facilities, or tech-
6 nical assistance from such person under section
7 102 of this title”.

8 (g) USE OF INFORMATION.—Section 106 of FISA
9 (50 U.S.C. 1806) is amended—

10 (1) in subsection (i)—

11 (A) by striking “radio”; and

12 (B) by inserting “contain foreign intel-
13 ligence information or” after “the Attorney
14 General determines that the contents” inserting
15 “contain foreign intelligence information or”;
16 and

17 (2) in subsection (k), by striking “1804(a)(7)”
18 and inserting “104(a)(6)”.

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

22 “(c) DOCUMENT MANAGEMENT SYSTEM FOR APPLI-
23 CATIONS FOR ORDERS APPROVING ELECTRONIC SURVEIL-
24 LANCE.—

1 “(1) SYSTEM PROPOSED.—The Attorney Gen-
2 eral and Director of National Intelligence shall, in
3 consultation with the Director of the Federal Bu-
4 reau of Investigation, the Director of the National
5 Security Agency, the Director of the Central Intel-
6 ligence Agency, and the court established under sec-
7 tion 103(b), conduct a feasibility study to develop
8 and implement a secure, classified document man-
9 agement system that permits the prompt prepara-
10 tion, modification, and review by appropriate per-
11 sonnel of the Department of Justice, the Federal
12 Bureau of Investigation, the National Security
13 Agency, and other applicable elements of the United
14 States Government of applications under section 104
15 before their submittal to that court.

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

18 “(A) permit and facilitate the prompt sub-
19 mittal of applications and all other matters, in-
20 cluding electronic filings, to the court estab-
21 lished under section 103(b) under section 104
22 or 105(g)(5); and

23 “(B) permit and facilitate the prompt
24 transmittal of rulings of that court to personnel

1 submitting applications described in paragraph
2 (1).”.

3 (i) AMENDMENTS TO FISA TITLE I RELATING TO
4 WEAPONS OF MASS DESTRUCTION.—

5 (1) Section 101 of FISA, as amended by sub-
6 section (b) of this section, is further amended—

7 (A) in subsection (b)(1)—

8 (i) by striking “or” at the end of sub-
9 paragraph (D);

10 (ii) by redesignating subparagraph
11 (E) as subparagraph (F); and

12 (iii) by inserting after subparagraph
13 (D) the following new subparagraph (E):

14 “(E) engages in the development or pro-
15 liferation of weapons of mass destruction, or ac-
16 tivities in preparation therefor; or;”;

17 (B) in subsection (b)(2)(C), by striking
18 “sabotage or international terrorism” and in-
19 serting “sabotage, international terrorism, or
20 the development or proliferation of weapons of
21 mass destruction”; and

22 (C) by inserting after subsection (k) the
23 following new subsection (l):

24 “(l) ‘Weapon of mass destruction’ means—

1 “(1) any destructive device (as that term is de-
2 fined in section 921 of title 18, United States Code)
3 that is intended or has the capability, to cause death
4 or serious bodily injury to a significant number of
5 people;

6 “(2) any weapon that is designed or intended to
7 cause death or serious bodily injury through the re-
8 lease, dissemination, or impact of toxic or poisonous
9 chemicals, or their precursors;

10 “(3) any weapon involving a biological agent,
11 toxin, or vector (as those terms are defined in sec-
12 tion 178 of title 18, United States Code); or

13 “(4) any weapon that is designed to release ra-
14 diation or radioactivity at a level dangerous to
15 human life.”.

16 (2) Sections 101(e)(1)(B), 106(k)(1)(B), and
17 305(k)(1)(B) of FISA are each amended by striking
18 “sabotage or international terrorism” and inserting
19 “sabotage, international terrorism, or the develop-
20 ment or proliferation of weapons of mass destruc-
21 tion”.

22 (j) CONFORMING AMENDMENTS TO TITLES I AND III
23 OF FISA TO ACCOMMODATE INTERNATIONAL MOVEMENTS
24 OF TARGETS.—

1 (1) Section 105(e) of FISA is amended by add-
2 ing at the end the following new paragraph:

3 “(4) An order issued under this section shall remain
4 in force during the authorized period of surveillance not-
5 withstanding the absence of the target from the United
6 States, unless the Government files a motion to extinguish
7 the order and the court grants the motion.”.

8 (2) Section 304(d) of FISA is amended by add-
9 ing at the end the following new paragraph:

10 “(4) An order issued under this section shall remain
11 in force during the authorized period of physical search
12 notwithstanding the absence of the target from the United
13 States, unless the Government files a motion to extinguish
14 the order and the court grants the motion.”.

15 **SEC. 10. CONFORMING AMENDMENT TO TABLE OF CON-**
16 **TENTS.**

17 The table of contents for the Foreign Intelligence
18 Surveillance Act of 1978 is amended—

19 (1) by striking the item relating to section 102
20 and inserting the following new item:

“Sec. 102. Electronic surveillance authorization without court order; certifi-
 cation by attorney general; reports to congressional commit-
 tees; transmittal under seal; duties and compensation of com-
 munication common carrier; applications; jurisdiction of
 court.”;

21 (2) by striking the items relating to sections
22 111, 309, and 404; and

1 (3) by striking the items related to title VII and
2 section 701 and inserting the following:

“TITLE VII—ELECTRONIC SURVEILLANCE PROGRAMS

“Sec. 701. Definitions.

“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—EFFECTIVE DATE

“Sec. 801. Effective date.”.

Calendar No. 635

109TH CONGRESS
2^D SESSION

S. 3931

A BILL

To establish procedures for the review of electronic surveillance programs.

SEPTEMBER 25, 2006

Read the second time and placed on the calendar