

## Calendar No. 599

109TH CONGRESS  
2D SESSION**S. 3876**Entitled The National Security Surveillance Act.

---

## IN THE SENATE OF THE UNITED STATES

SEPTEMBER 7 (legislative day, SEPTEMBER 6), 2006

Mr. SPECTER introduced the following bill; which was read the first time

SEPTEMBER 8, 2006

Read the second time and placed on the calendar

---

**A BILL**

Entitled The National Security Surveillance Act.

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 “National Security Sur-  
5 veillance Act of 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-

1 rity Agency to intercept communications between  
2 people inside the United States, including American  
3 citizens, and terrorism suspects overseas.

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

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

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

23 (5) It is equally essential, however, that in pro-  
24 tecting the United States against our enemies, the  
25 President does not compromise the very civil lib-

1       erties that he seeks to safeguard. As Justice Hugo  
2       Black observed, “The President’s power, if any, to  
3       issue [an] order must stem either from an Act of  
4       Congress or from the Constitution itself.” *Youngs-*  
5       *town Sheet & Tube Co. v. Sawyer*, 343 U.S. 579,  
6       585 (1952) (opinion by Black, J.). Similarly, in  
7       2004, Justice Sandra Day O’Connor explained in  
8       her plurality opinion for the Supreme Court in  
9       *Hamdi v. Rumsfeld*: “We have long since made clear  
10      that a state of war is not a blank check for the  
11      President when it comes to the rights of the Na-  
12      tion’s citizens.” *Hamdi v. Rumsfeld*, 542 U.S. 507,  
13      536 (2004) (citations omitted).

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

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

1 States Constitution envisions for the Executive in its  
2 exchanges with other nations or with enemy organi-  
3 zations in times of conflict, it most assuredly envi-  
4 sions a role for all 3 branches when individual lib-  
5 erties are at stake.” Hamdi v. Rumsfeld, 542 U.S.  
6 507, 536 (2004) (citations omitted).

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

1 Congress over the matter. Courts can sustain exclu-  
2 sive Presidential control in such a case only by dis-  
3 abling the Congress from acting upon the subject.”  
4 *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S.  
5 579, 635–38 (1952) (Jackson, J., concurring).

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

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

16 (B) “To raise and support Armies”;

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

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

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

23 (F) “To provide for organizing, arming,  
24 and disciplining the Militia, and for governing

1           such Part of them as may be employed in the  
2           Service of the United States”.

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

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

24          (12) In 1975, [then] Attorney General Edward  
25          Levi, a strong defender of executive authority, testi-

1       fied that in times of conflict, the President needs the  
2       power to conduct long-range electronic surveillance  
3       and that a foreign intelligence surveillance court  
4       should be empowered to issue special approval orders  
5       in these circumstances.

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

13              (14) The Foreign Intelligence Surveillance  
14      Court already has broad authority to approve sur-  
15      veillance of members of international conspiracies, in  
16      addition to granting warrants for surveillance of a  
17      particular individual under sections 104, 105, and  
18      402 of the Foreign Intelligence Surveillance Act of  
19      1978 (50 U.S.C. 1804, 1805, and 1842).

20              (15) Prosecutors have significant flexibility in  
21      investigating domestic conspiracy cases. Courts have  
22      held that flexible warrants comply with the 4th  
23      amendment to the Constitution of the United States  
24      when they relate to complex, far-reaching, and  
25      multifaceted criminal enterprises like drug conspir-

1       acies and money laundering rings. The courts recog-  
2       nize that applications for search warrants must be  
3       judged in a common sense and realistic fashion, and  
4       the courts permit broad warrant language where,  
5       due to the nature and circumstances of the inves-  
6       tigation and the criminal organization, more precise  
7       descriptions are not feasible.

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

1           (17) By authorizing the Foreign Intelligence  
2           Surveillance Court to review electronic surveillance  
3           programs, Congress preserves the ability of the  
4           President to use the necessary means to guard our  
5           national security, while also protecting the civil lib-  
6           erties and constitutional rights that we cherish.

7 **SEC. 3. DEFINITIONS.**

8           The Foreign Intelligence Surveillance Act of 1978  
9 (50 U.S.C. 1801 et seq.) is amended—

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

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

12           and

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

14           **“TITLE VII—ELECTRONIC**  
15           **SURVEILLANCE**

16 **“SEC. 701. DEFINITION.**

17           “As used in this title—

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

23           “(2) the term ‘congressional intelligence com-  
24           mittees’ means the Select Committee on Intelligence

1 of the Senate and the Permanent Select Committee  
2 on Intelligence of the House of Representatives;

3 “(3) the term ‘electronic communication’ means  
4 any transfer of signs, signals, writing, images,  
5 sounds, data, or intelligence of any nature trans-  
6 mitted, in whole or in part, by a wire, radio, electro-  
7 magnetic, photo electronic or photo optical system,  
8 cable, or other like connection furnished or operated  
9 by any person engaged as a common carrier in pro-  
10 viding or operating such facilities for the trans-  
11 mission of communications;

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

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

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

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

7           “(C) where effective gathering of foreign  
8 intelligence information requires the flexibility  
9 to begin electronic surveillance immediately  
10 after learning of suspect activity; and

11           “(D) where effective gathering of foreign  
12 intelligence information requires an extended  
13 period of electronic surveillance;

14           “(6) the term ‘foreign intelligence information’  
15 has the same meaning as in section 101 and in-  
16 cludes information necessary to protect against  
17 international terrorism;

18           “(7) the term ‘Foreign Intelligence Surveillance  
19 Court’ means the court established under section  
20 103(a);

21           “(8) the term ‘Foreign Intelligence Surveillance  
22 Court of Review’ means the court established under  
23 section 103(b);

24           “(9) the term ‘intercept’ means the acquisition  
25 of the substance of any electronic communication by

1 a person through the use of any electronic, mechan-  
2 ical, or other device; and

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

7 **SEC. 4. FOREIGN INTELLIGENCE SURVEILLANCE COURT**  
8 **JURISDICTION TO REVIEW ELECTRONIC SUR-**  
9 **VEILLANCE PROGRAMS.**

10 (a) IN GENERAL.—Title VII of the Foreign Intel-  
11 ligence Surveillance Act of 1978, as amended by section  
12 3, is amended by adding at the end the following:

13 **“SEC. 702. FOREIGN INTELLIGENCE SURVEILLANCE COURT**  
14 **JURISDICTION TO REVIEW ELECTRONIC SUR-**  
15 **VEILLANCE PROGRAMS.**

16 “(a) AUTHORIZATION OF REVIEW.—

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

24 “(2) REAUTHORIZATION.—The Foreign Intel-  
25 ligence Surveillance Court shall have jurisdiction to

1 reauthorize an electronic surveillance program for a  
2 period of time not longer than such court determines  
3 to be reasonable.

4 “(3) RESUBMISSION OR APPEAL.—In the event  
5 that the Foreign Intelligence Surveillance Court re-  
6 fuses to approve an application under this sub-  
7 section, the Attorney General may submit a new ap-  
8 plication. There shall be no limit on the number of  
9 times the Attorney General may seek approval of an  
10 electronic surveillance program. Alternatively, the  
11 Attorney General may appeal the decision of the  
12 Foreign Intelligence Surveillance Court to the For-  
13 eign Intelligence Surveillance Court of Review.

14 “(b) MANDATORY TRANSFER FOR REVIEW.—

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

1 to the Foreign Intelligence Surveillance Court of Re-  
2 view for further proceedings under this subsection.

3 “(2) RETRANSFER TO ORIGINATING COURT.—

4 Upon completion of review pursuant to this sub-  
5 section, the Foreign Intelligence Surveillance Court  
6 of Review shall remand the case to the originating  
7 court for further proceedings consistent with its  
8 opinion.

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

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

20 “(5) DISMISSAL.—The Foreign Intelligence  
21 Surveillance Court of Review or a court that is an  
22 originating court under paragraph (1) may dismiss  
23 a challenge to the legality of an electronic surveil-  
24 lance program for any reason provided for under  
25 law.



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

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

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

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

15           “(7) include an explanation of how the elec-  
16 tronic surveillance program is reasonably designed to  
17 ensure that the communications that are intercepted  
18 are communications of or with—

19           “(A) a foreign power that is engaged in  
20 international terrorism activities or in prepara-  
21 tion therefor;

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

1           “(C) a person reasonably believed to have  
2           communication with or be associated with a for-  
3           foreign power that is engaged in international ter-  
4           rorism activities or in preparation therefor or  
5           an agent of a foreign power that is engaged in  
6           international terrorism activities or in prepara-  
7           tion therefor;

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

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

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

20          “(11) include a statement of facts concerning  
21          the implementation of the electronic surveillance pro-  
22          gram described in the application, including, for any  
23          period of operation of the program authorized not  
24          less than 90 days prior to the date of submission of  
25          the application—

1           “(A) the minimization procedures imple-  
2           mented; and

3           “(B) the means and operational procedures  
4           by which the electronic tracking was executed  
5           and effected.

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

10 **SEC. 6. APPROVAL OF ELECTRONIC SURVEILLANCE PRO-**  
11 **GRAMS.**

12           Title VII of the Foreign Intelligence Surveillance Act  
13           18 of 1978, as amended by section 5, is amended by add-  
14           ing at the end the following:

15 **“SEC. 704. APPROVAL OF ELECTRONIC SURVEILLANCE**  
16 **PROGRAMS.**

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

22           “(1) the President has authorized the Attorney  
23           General to make the application for electronic sur-  
24           veillance for foreign intelligence information or to  
25           protect against international terrorism;

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

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

8                   “(A) a foreign power that is engaged in  
9                   international terrorism activities or in prepara-  
10                  tion therefor;

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

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

21           “(4) the proposed minimization procedures  
22           meet the definition of minimization procedures  
23           under section 101(h); and

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

1       “(b) CONSIDERATIONS.—In considering the constitu-  
2   tionality of the electronic surveillance program under sub-  
3   section (a), the Foreign Intelligence Surveillance Court  
4   may consider—

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

8           “(A) the minimization procedures proposed  
9   with the minimization procedures actually im-  
10   plemented;

11           “(B) the nature of the information sought  
12   with the nature of the information actually ob-  
13   tained; and

14           “(C) the means and operational procedures  
15   proposed with the means and operational proce-  
16   dures actually implemented; and

17           “(2) whether foreign intelligence information  
18   has been obtained through the electronic surveillance  
19   program.

20       “(c) CONTENTS OF ORDER.—An order approving an  
21   electronic surveillance program under this section shall di-  
22   rect—

23           “(1) that the minimization procedures be fol-  
24   lowed;

1           “(2) that, upon the request of the applicant,  
2           specified communication or other common carriers,  
3           landlords, custodians, or other specified person, fur-  
4           nish the applicant forthwith with all information, fa-  
5           cilities, or technical assistance necessary to under-  
6           take the electronic surveillance program in such a  
7           manner as will protect its secrecy and produce a  
8           minimum of interference with the services that such  
9           carriers, landlords, custodians, or other persons are  
10          providing potential targets of the electronic surveil-  
11          lance program;

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

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

21 **SEC. 7. CONGRESSIONAL OVERSIGHT.**

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

1 **“SEC. 705. CONGRESSIONAL OVERSIGHT.**

2       “(a) IN GENERAL.—Not less often than every 180  
3 days, the Attorney General shall submit to the congres-  
4 sional intelligence committees a report in classified form  
5 on the activities during the previous 180-day period under  
6 any electronic surveillance program authorized under this  
7 title.

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

11               “(1) the minimization procedures implemented;

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

14               “(3) significant decisions of the Foreign Intel-  
15 ligence Surveillance Court on applications made  
16 under section 703;

17               “(4) the total number of applications made for  
18 orders approving electronic surveillance pursuant to  
19 this title; and

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

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

1 **SEC. 8. CLARIFICATION OF THE FOREIGN INTELLIGENCE**  
2 **SURVEILLANCE ACT OF 1978.**

3 (a) IN GENERAL.—The Foreign Intelligence Surveil-  
4 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended  
5 by inserting after title VII, as amended by this Act, the  
6 following:

7 **“TITLE VIII—EXECUTIVE**  
8 **AUTHORITY**

9 **“SEC. 801. EXECUTIVE AUTHORITY.**

10 “Nothing in this Act shall be construed to limit the  
11 constitutional authority of the President to collect intel-  
12 ligence with respect to foreign powers and agents of for-  
13 eign powers.”.

14 (b) REPEAL.—Sections 111, 309, and 404 of the  
15 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.  
16 1811, 1829, and 1844) are repealed.

17 (c) CONFORMING AMENDMENTS.—

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

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

15 (II) by striking “or” at the end;

16 (ii) in paragraph (2)—

17 (I) by inserting “or under the  
18 Constitution” after “authorized by  
19 statute”; 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) knowingly discloses or uses information ob-  
25 tained under color of law by electronic surveillance

1 in a manner or for a purpose not authorized by  
2 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. OTHER CONFORMING 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 (B), by striking “or”  
16 after the semicolon; and

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

18 “(D) otherwise possesses or is expected to  
19 transmit or receive foreign intelligence informa-  
20 tion within the United States; or”;

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

23 “(f) ‘Electronic surveillance’ means—

24 “(1) the installation or use of an electronic, me-  
25 chanical, or other surveillance device for the inten-

1 tional collection of information concerning a par-  
2 ticular known person who is reasonably believed to  
3 be in the United States by intentionally targeting  
4 that person under circumstances in which that per-  
5 son has a reasonable expectation of privacy and a  
6 warrant would be required for law enforcement pur-  
7 poses; or

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

14 (3) in subsection (g), by inserting before the pe-  
15 riod the following: “or a person or persons des-  
16 ignated by the Attorney General or Acting Attorney  
17 General”;

18 (4) in subsection (h)—

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

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

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

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

1 “(n) ‘contents’ has the meaning set forth in section  
2 2510(8) of title 18, United States Code.”.

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

6 “ELECTRONIC SURVEILLANCE AUTHORIZATION WITHOUT  
7 COURT ORDER; CERTIFICATION BY ATTORNEY GEN-  
8 ERAL; REPORTS TO CONGRESSIONAL COMMITTEES;  
9 TRANSMITTAL UNDER SEAL; DUTIES AND COM-  
10 PENSATION OF COMMUNICATION COMMON CARRIER;  
11 APPLICATIONS; JURISDICTION OF COURT

12 “SEC. 102. (a)(1) Notwithstanding any other law, the  
13 President through the Attorney General, may authorize  
14 electronic surveillance without a court order under this  
15 title to acquire foreign intelligence information for periods  
16 of up to 1 year if the Attorney General certifies in writing  
17 under oath that—

18 “(A)(i) the acquisition of the contents of com-  
19 munications of foreign powers, as defined in section  
20 101(a), an agent of a foreign power as defined in  
21 section 101(b)(1); or

22 “(ii) the acquisition of technical intelligence,  
23 other than the spoken communications of individ-  
24 uals, from property or premises under the open and  
25 exclusive control of a foreign power, as defined in  
26 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.”.

Calendar No. 599

109<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

**S. 3876**

**A BILL**

Entitled The National Security Surveillance Act.

SEPTEMBER 8, 2006

Read the second time and placed on the calendar