

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

# H. R. 5825

---

## AN ACT

To update the Foreign Intelligence Surveillance Act of 1978.

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Electronic Surveillance  
3 Modernization Act”.

4 **SEC. 2. FISA DEFINITIONS.**

5 (a) **AGENT OF A FOREIGN POWER.**—Subsection  
6 (b)(1) of section 101 of the Foreign Intelligence Surveil-  
7 lance Act of 1978 (50 U.S.C. 1801) is amended—

8 (1) in subparagraph (B), by striking “; or” and  
9 inserting “;”; and

10 (2) by adding at the end the following:

11 “(D) is reasonably expected to possess,  
12 control, transmit, or receive foreign intelligence  
13 information while such person is in the United  
14 States, provided that the official making the  
15 certification required by section 104(a)(7)  
16 deems such foreign intelligence information to  
17 be significant; or”.

18 (b) **ELECTRONIC SURVEILLANCE.**—Subsection (f) of  
19 such section is amended to read as follows:

20 “(f) ‘Electronic surveillance’ means—

21 “(1) the installation or use of an electronic, me-  
22 chanical, or other surveillance device for acquiring  
23 information by intentionally directing surveillance at  
24 a particular known person who is reasonably believed  
25 to be in the United States under circumstances in  
26 which that person has a reasonable expectation of

1 privacy and a warrant would be required for law en-  
2 forcement purposes; or

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

10 (c) MINIMIZATION PROCEDURES.—Subsection (h) of  
11 such section is amended—

12 (1) in paragraph (2), by striking “importance;”  
13 and inserting “importance; and”;

14 (2) in paragraph (3), by striking “; and” and  
15 inserting “.”; and

16 (3) by striking paragraph (4).

17 (d) WIRE COMMUNICATION AND SURVEILLANCE DE-  
18 VICE.—Subsection (l) of such section is amended to read  
19 as follows:

20 “(l) ‘Surveillance device’ is a device that allows sur-  
21 veillance by the Federal Government, but excludes any de-  
22 vice that extracts or analyzes information from data that  
23 has already been acquired by the Federal Government by  
24 lawful means.”.

1 (e) CONTENTS.—Subsection (n) of such section is  
2 amended to read as follows:

3 “(n) ‘Contents’, when used with respect to a commu-  
4 nication, includes any information concerning the sub-  
5 stance, purport, or meaning of that communication.”.

6 **SEC. 3. AUTHORIZATION FOR ELECTRONIC SURVEILLANCE**  
7 **AND OTHER ACQUISITIONS FOR FOREIGN IN-**  
8 **TELLIGENCE PURPOSES.**

9 (a) IN GENERAL.—The Foreign Intelligence Surveil-  
10 lance Act of 1978 (50 U.S.C. 1801 et seq.) is further  
11 amended by striking section 102 and inserting the fol-  
12 lowing:

13 “AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR  
14 FOREIGN INTELLIGENCE PURPOSES

15 “SEC. 102. (a) IN GENERAL.—Notwithstanding any  
16 other law, the President, acting through the Attorney Gen-  
17 eral, may authorize electronic surveillance without a court  
18 order under this title to acquire foreign intelligence infor-  
19 mation for periods of up to one year if the Attorney Gen-  
20 eral certifies in writing under oath that—

21 “(1) the electronic surveillance is directed at—

22 “(A) the acquisition of the contents of  
23 communications of foreign powers, as defined in  
24 paragraph (1), (2), or (3) of section 101(a), or  
25 an agent of a foreign power, as defined in sub-  
26 paragraph (A) or (B) of section 101(b)(1); or

1           “(B) the acquisition of technical intel-  
2           ligence, other than the spoken communications  
3           of individuals, from property or premises under  
4           the open and exclusive control of a foreign  
5           power, as defined in paragraph (1), (2), or (3)  
6           of section 101(a); and

7           “(2) the proposed minimization procedures with  
8           respect to such surveillance meet the definition of  
9           minimization procedures under section 101(h);  
10 if the Attorney General reports such minimization proce-  
11 dures and any changes thereto to the Permanent Select  
12 Committee on Intelligence of the House of Representatives  
13 and the Select Committee on Intelligence of the Senate  
14 at least 30 days prior to the effective date of such mini-  
15 mization procedures, unless the Attorney General deter-  
16 mines immediate action is required and notifies the com-  
17 mittees immediately of such minimization procedures and  
18 the reason for their becoming effective immediately.

19           “(b) MINIMIZATION PROCEDURES.—An electronic  
20 surveillance authorized by this subsection may be con-  
21 ducted only in accordance with the Attorney General’s cer-  
22 tification and the minimization procedures. The Attorney  
23 General shall assess compliance with such procedures and  
24 shall report such assessments to the Permanent Select  
25 Committee on Intelligence of the House of Representatives

1 and the Select Committee on Intelligence of the Senate  
2 under the provisions of section 108(a).

3 “(c) SUBMISSION OF CERTIFICATION.—The Attorney  
4 General shall immediately transmit under seal to the court  
5 established under section 103(a) a copy of his certifi-  
6 cation. Such certification shall be maintained under secu-  
7 rity measures established by the Chief Justice with the  
8 concurrence of the Attorney General, in consultation with  
9 the Director of National Intelligence, and shall remain  
10 sealed unless—

11 “(1) an application for a court order with respect to  
12 the surveillance is made under section 104; or

13 “(2) the certification is necessary to determine the  
14 legality of the surveillance under section 106(f).

15 “AUTHORIZATION FOR ACQUISITION OF FOREIGN  
16 INTELLIGENCE INFORMATION

17 “SEC. 102A. (a) IN GENERAL.—Notwithstanding  
18 any other law, the President, acting through the Attorney  
19 General may, for periods of up to one year, authorize the  
20 acquisition of foreign intelligence information concerning  
21 a person reasonably believed to be outside the United  
22 States if the Attorney General certifies in writing under  
23 oath that—

24 “(1) the acquisition does not constitute elec-  
25 tronic surveillance;

1           “(2) the acquisition involves obtaining the for-  
2           foreign intelligence information from or with the assist-  
3           ance of a wire or electronic communications service  
4           provider, custodian, or other person (including any  
5           officer, employee, agent, or other specified person of  
6           such service provider, custodian, or other person)  
7           who has access to wire or electronic communications,  
8           either as they are transmitted or while they are  
9           stored, or equipment that is being or may be used  
10          to transmit or store such communications;

11           “(3) a significant purpose of the acquisition is  
12          to obtain foreign intelligence information; and

13           “(4) the proposed minimization procedures with  
14          respect to such acquisition activity meet the defini-  
15          tion of minimization procedures under section  
16          101(h).

17          “(b) SPECIFIC PLACE NOT REQUIRED.—A certifi-  
18          cation under subsection (a) is not required to identify the  
19          specific facilities, places, premises, or property at which  
20          the acquisition of foreign intelligence information will be  
21          directed.

22          “(c) SUBMISSION OF CERTIFICATION.—The Attorney  
23          General shall immediately transmit under seal to the court  
24          established under section 103(a) a copy of a certification  
25          made under subsection (a). Such certification shall be

1 maintained under security measures established by the  
2 Chief Justice of the United States and the Attorney Gen-  
3 eral, in consultation with the Director of National Intel-  
4 ligence, and shall remain sealed unless the certification is  
5 necessary to determine the legality of the acquisition  
6 under section 102B.

7 “(d) MINIMIZATION PROCEDURES.—An acquisition  
8 under this section may be conducted only in accordance  
9 with the certification of the Attorney General and the  
10 minimization procedures adopted by the Attorney General.  
11 The Attorney General shall assess compliance with such  
12 procedures and shall report such assessments to the Per-  
13 manent Select Committee on Intelligence of the House of  
14 Representatives and the Select Committee on Intelligence  
15 of the Senate under section 108(a).

16 “DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE  
17 AND OTHER ACQUISITIONS OF FOREIGN INTEL-  
18 LIGENCE INFORMATION

19 “SEC. 102B. (a) DIRECTIVE.—With respect to an au-  
20 thorization of electronic surveillance under section 102 or  
21 an authorization of an acquisition under section 102A, the  
22 Attorney General may direct a person to—

23 “(1) immediately provide the Government with  
24 all information, facilities, and assistance necessary  
25 to accomplish the acquisition of foreign intelligence  
26 information in such a manner as will protect the se-



1       crecy of the electronic surveillance or acquisition and  
2       produce a minimum of interference with the services  
3       that such person is providing to the target; and

4               “(2) maintain under security procedures ap-  
5       proved by the Attorney General and the Director of  
6       National Intelligence any records concerning the  
7       electronic surveillance or acquisition or the aid fur-  
8       nished that such person wishes to maintain.

9       “(b) COMPENSATION.—The Government shall com-  
10      pensate, at the prevailing rate, a person for providing in-  
11      formation, facilities, or assistance pursuant to subsection  
12      (a).

13       “(c) FAILURE TO COMPLY.—In the case of a failure  
14      to comply with a directive issued pursuant to subsection  
15      (a), the Attorney General may petition the court estab-  
16      lished under section 103(a) to compel compliance with the  
17      directive. The court shall issue an order requiring the per-  
18      son or entity to comply with the directive if it finds that  
19      the directive was issued in accordance with section 102(a)  
20      or 102A(a) and is otherwise lawful. Failure to obey an  
21      order of the court may be punished by the court as con-  
22      tempt of court. Any process under this section may be  
23      served in any judicial district in which the person or entity  
24      may be found.

1       “(d) REVIEW OF PETITIONS.—(1) IN GENERAL.—  
2 (A) CHALLENGE.—A person receiving a directive issued  
3 pursuant to subsection (a) may challenge the legality of  
4 that directive by filing a petition with the pool established  
5 under section 103(e)(1).

6       “(B) ASSIGNMENT OF JUDGE.—The presiding judge  
7 designated pursuant to section 103(b) shall assign a peti-  
8 tion filed under subparagraph (A) to one of the judges  
9 serving in the pool established by section 103(e)(1). Not  
10 later than 24 hours after the assignment of such petition,  
11 the assigned judge shall conduct an initial review of the  
12 directive. If the assigned judge determines that the peti-  
13 tion is frivolous, the assigned judge shall deny the petition  
14 and affirm the directive or any part of the directive that  
15 is the subject of the petition. If the assigned judge deter-  
16 mines the petition is not frivolous, the assigned judge  
17 shall, within 72 hours, consider the petition in accordance  
18 with the procedures established under section 103(e)(2)  
19 and provide a written statement for the record of the rea-  
20 sons for any determination under this subsection.

21       “(2) STANDARD OF REVIEW.—A judge considering a  
22 petition to modify or set aside a directive may grant such  
23 petition only if the judge finds that such directive does  
24 not meet the requirements of this section or is otherwise  
25 unlawful. If the judge does not modify or set aside the

1 directive, the judge shall affirm such directive, and order  
2 the recipient to comply with such directive.

3 “(3) DIRECTIVES NOT MODIFIED.—Any directive not  
4 explicitly modified or set aside under this subsection shall  
5 remain in full effect.

6 “(e) APPEALS.—The Government or a person receiv-  
7 ing a directive reviewed pursuant to subsection (d) may  
8 file a petition with the court of review established under  
9 section 103(b) for review of the decision issued pursuant  
10 to subsection (d) not later than 7 days after the issuance  
11 of such decision. Such court of review shall have jurisdic-  
12 tion to consider such petitions and shall provide for the  
13 record a written statement of the reasons for its decision.  
14 On petition by the Government or any person receiving  
15 such directive for a writ of certiorari, the record shall be  
16 transmitted under seal to the Supreme Court, which shall  
17 have jurisdiction to review such decision.

18 “(f) PROCEEDINGS.—Judicial proceedings under this  
19 section shall be concluded as expeditiously as possible. The  
20 record of proceedings, including petitions filed, orders  
21 granted, and statements of reasons for decision, shall be  
22 maintained under security measures established by the  
23 Chief Justice of the United States, in consultation with  
24 the Attorney General and the Director of National Intel-  
25 ligence.

1       “(g) SEALED PETITIONS.—All petitions under this  
2 section shall be filed under seal. In any proceedings under  
3 this section, the court shall, upon request of the Govern-  
4 ment, review ex parte and in camera any Government sub-  
5 mission, or portions of a submission, which may include  
6 classified information.

7       “(h) LIABILITY.—No cause of action shall lie in any  
8 court against any person for providing any information,  
9 facilities, or assistance in accordance with a directive  
10 under this section.

11       “(i) USE OF INFORMATION.—Information acquired  
12 pursuant to a directive by the Attorney General under this  
13 section concerning any United States person may be used  
14 and disclosed by Federal officers and employees without  
15 the consent of the United States person only in accordance  
16 with the minimization procedures required by section  
17 102(a) or 102A(a). No otherwise privileged communica-  
18 tion obtained in accordance with, or in violation of, the  
19 provisions of this section shall lose its privileged character.  
20 No information from an electronic surveillance under sec-  
21 tion 102 or an acquisition pursuant to section 102A may  
22 be used or disclosed by Federal officers or employees ex-  
23 cept for lawful purposes.

24       “(j) USE IN LAW ENFORCEMENT.—No information  
25 acquired pursuant to this section shall be disclosed for law

1 enforcement purposes unless such disclosure is accom-  
2 panied by a statement that such information, or any infor-  
3 mation derived from such information, may only be used  
4 in a criminal proceeding with the advance authorization  
5 of the Attorney General.

6       “(k) DISCLOSURE IN TRIAL.—If the Government in-  
7 tends to enter into evidence or otherwise use or disclose  
8 in any trial, hearing, or other proceeding in or before any  
9 court, department, officer, agency, regulatory body, or  
10 other authority of the United States, against an aggrieved  
11 person, any information obtained or derived from an elec-  
12 tronic surveillance conducted under section 102 or an ac-  
13 quisition authorized pursuant to section 102A, the Gov-  
14 ernment shall, prior to the trial, hearing, or other pro-  
15 ceeding or at a reasonable time prior to an effort to dis-  
16 close or use that information or submit it in evidence, no-  
17 tify the aggrieved person and the court or other authority  
18 in which the information is to be disclosed or used that  
19 the Government intends to disclose or use such informa-  
20 tion.

21       “(l) DISCLOSURE IN STATE TRIALS.—If a State or  
22 political subdivision of a State intends to enter into evi-  
23 dence or otherwise use or disclose in any trial, hearing,  
24 or other proceeding in or before any court, department,  
25 officer, agency, regulatory body, or other authority of a

1 State or a political subdivision of a State, against an ag-  
2 grieved person, any information obtained or derived from  
3 an electronic surveillance authorized pursuant to section  
4 102 or an acquisition authorized pursuant to section  
5 102A, the State or political subdivision of such State shall  
6 notify the aggrieved person, the court, or other authority  
7 in which the information is to be disclosed or used and  
8 the Attorney General that the State or political subdivision  
9 intends to disclose or use such information.

10       “(m) MOTION TO EXCLUDE EVIDENCE.—(1) IN  
11 GENERAL.—Any person against whom evidence obtained  
12 or derived from an electronic surveillance authorized pur-  
13 suant to section 102 or an acquisition authorized pursuant  
14 to section 102A is to be, or has been, used or disclosed  
15 in any trial, hearing, or other proceeding in or before any  
16 court, department, officer, agency, regulatory body, or  
17 other authority of the United States, a State, or a political  
18 subdivision thereof, may move to suppress the evidence ob-  
19 tained or derived from such electronic surveillance or such  
20 acquisition on the grounds that—

21               “(A) the information was unlawfully acquired;

22       or

23               “(B) the electronic surveillance or acquisition  
24 was not properly made in conformity with an au-  
25 thorization under section 102(a) or 102A(a).

1       “(2) TIMING.—A person moving to suppress evidence  
2 under paragraph (1) shall make the motion to suppress  
3 the evidence before the trial, hearing, or other proceeding  
4 unless there was no opportunity to make such a motion  
5 or the person was not aware of the grounds of the motion.

6       “(n) REVIEW OF MOTIONS.—If a court or other au-  
7 thority is notified pursuant to subsection (k) or (l), a mo-  
8 tion is made pursuant to subsection (m), or a motion or  
9 request is made by an aggrieved person pursuant to any  
10 other statute or rule of the United States or any State  
11 before any court or other authority of the United States  
12 or any State—

13               “(1) to discover or obtain an Attorney General  
14 directive or other materials relating to an electronic  
15 surveillance authorized pursuant to section 102 or  
16 an acquisition authorized pursuant to section 102A,  
17 or

18               “(2) to discover, obtain, or suppress evidence or  
19 information obtained or derived from an electronic  
20 surveillance authorized pursuant to section 102 or  
21 an acquisition authorized pursuant to section 102A,  
22 the United States district court or, where the motion is  
23 made before another authority, the United States district  
24 court in the same district as the authority, shall, notwith-  
25 standing any other law, if the Attorney General files an

1 affidavit under oath that disclosure or an adversary hear-  
2 ing would harm the national security of the United States,  
3 review in camera and ex parte the application, order, and  
4 such other materials relating to such electronic surveil-  
5 lance or such acquisition as may be necessary to determine  
6 whether such electronic surveillance or such acquisition  
7 authorized under this section was lawfully authorized and  
8 conducted. In making this determination, the court may  
9 disclose to the aggrieved person, under appropriate secu-  
10 rity procedures and protective orders, portions of the di-  
11 rective or other materials relating to the acquisition only  
12 where such disclosure is necessary to make an accurate  
13 determination of the legality of the acquisition.

14       “(o) DETERMINATIONS.—If, pursuant to subsection  
15 (n), a United States district court determines that the ac-  
16 quisition authorized under this section was not lawfully  
17 authorized or conducted, it shall, in accordance with the  
18 requirements of law, suppress the evidence which was un-  
19 lawfully obtained or derived or otherwise grant the motion  
20 of the aggrieved person. If the court determines that such  
21 acquisition was lawfully authorized and conducted, it shall  
22 deny the motion of the aggrieved person except to the ex-  
23 tent that due process requires discovery or disclosure.

24       “(p) BINDING ORDERS.—Orders granting motions or  
25 requests under subsection (m), decisions under this section



1 that an electronic surveillance or an acquisition was not  
2 lawfully authorized or conducted, and orders of the United  
3 States district court requiring review or granting disclo-  
4 sure of directives, orders, or other materials relating to  
5 such acquisition shall be final orders and binding upon  
6 all courts of the United States and the several States ex-  
7 cept a United States court of appeals and the Supreme  
8 Court.

9 “(q) COORDINATION.—(1) IN GENERAL.—Federal  
10 officers who acquire foreign intelligence information may  
11 consult with Federal law enforcement officers or law en-  
12 forcement personnel of a State or political subdivision of  
13 a State, including the chief executive officer of that State  
14 or political subdivision who has the authority to appoint  
15 or direct the chief law enforcement officer of that State  
16 or political subdivision, to coordinate efforts to investigate  
17 or protect against—

18 “(A) actual or potential attack or other grave  
19 hostile acts of a foreign power or an agent of a for-  
20 eign power;

21 “(B) sabotage, international terrorism, or the  
22 development or proliferation of weapons of mass de-  
23 struction by a foreign power or an agent of a foreign  
24 power; or

1           “(C) clandestine intelligence activities by an in-  
2           telligence service or network of a foreign power or by  
3           an agent of a foreign power.

4           “(2) CERTIFICATION REQUIRED.—Coordination au-  
5           thorized under paragraph (1) shall not preclude the cer-  
6           tification required by section 102(a) or 102A(a).

7           “(r) RETENTION OF DIRECTIVES AND ORDERS.—A  
8           directive made or an order granted under this section shall  
9           be retained for a period of not less than 10 years from  
10          the date on which such directive or such order is made.”.

11          (b) TABLE OF CONTENTS.—The table of contents in  
12          the first section of the Foreign Intelligence Surveillance  
13          Act of 1978 (50 U.S.C. 1801 et seq.) is amended by in-  
14          serting after the item relating to section 102 the following:

          “102A. Authorization for acquisition of foreign intelligence information.

          “102B. Directives relating to electronic surveillance and other acquisitions of  
          foreign intelligence information.”.

15          **SEC. 4. JURISDICTION OF FISA COURT.**

16          Section 103 of the Foreign Intelligence Surveillance  
17          Act of 1978 (50 U.S.C. 1803) is amended by adding at  
18          the end the following new subsection:

19          “(g) Applications for a court order under this title  
20          are authorized if the President has, by written authoriza-  
21          tion, empowered the Attorney General to approve applica-  
22          tions to the court having jurisdiction under this section,  
23          and a judge to whom an application is made may, notwith-  
24          standing any other law, grant an order, in conformity with

1 section 105, approving electronic surveillance of a foreign  
2 power or an agent of a foreign power for the purpose of  
3 obtaining foreign intelligence information.”.

4 **SEC. 5. APPLICATIONS FOR COURT ORDERS.**

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

7 (1) in subsection (a)—

8 (A) in paragraph (6), by striking “detailed  
9 description” and inserting “summary descrip-  
10 tion”;

11 (B) in paragraph (7)—

12 (i) in the matter preceding subpara-  
13 graph (A), by striking “or officials des-  
14 ignated” and all that follows through “con-  
15 sent of the Senate” and inserting “des-  
16 ignated by the President to authorize elec-  
17 tronic surveillance for foreign intelligence  
18 purposes”;

19 (ii) in subparagraph (C), by striking  
20 “techniques;” and inserting “techniques;  
21 and”;

22 (iii) by striking subparagraph (D);  
23 and

24 (iv) by redesignating subparagraph  
25 (E) as subparagraph (D);

1 (C) in paragraph (8), by striking “a state-  
2 ment of the means” and inserting “a summary  
3 statement of the means”;

4 (D) in paragraph (9)—

5 (i) by striking “a statement” and in-  
6 serting “a summary statement”; and

7 (ii) by striking “application;” and in-  
8 serting “application; and”;

9 (E) in paragraph (10), by striking “there-  
10 after; and” and inserting “thereafter.”; and

11 (F) by striking paragraph (11).

12 (2) by striking subsection (b);

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

15 (4) in paragraph (1)(A) of subsection (d), as re-  
16 designated by paragraph (3), by striking “or the Di-  
17 rector of National Intelligence” and inserting “the  
18 Director of National Intelligence, or the Director of  
19 the Central Intelligence Agency”.

20 **SEC. 6. ISSUANCE OF AN ORDER.**

21 Section 105 of the Foreign Intelligence Surveillance  
22 Act of 1978 (50 U.S.C. 1805) is amended—

23 (1) in subsection (a)—

24 (A) by striking paragraph (1); and

1 (B) by redesignating paragraphs (2)  
2 through (5) as paragraphs (1) through (4), re-  
3 spectively;

4 (2) in subsection (c)(1)—

5 (A) in subparagraph (D), by striking “sur-  
6 veillance;” and inserting “surveillance; and”;

7 (B) in subparagraph (E), by striking “ap-  
8 proved; and” and inserting “approved.”; and

9 (C) by striking subparagraph (F);

10 (3) by striking subsection (d);

11 (4) by redesignating subsections (e) through (i)  
12 as subsections (d) through (h), respectively;

13 (5) in subsection (d), as redesignated by para-  
14 graph (4), by amending paragraph (2) to read as  
15 follows:

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

21 (6) in subsection (e), as redesignated by para-  
22 graph (4), to read as follows:

23 “(e) Notwithstanding any other provision of this title,  
24 the Attorney General may authorize the emergency em-

1 ployment of electronic surveillance if the Attorney Gen-  
2 eral—

3           “(1) determines that an emergency situation ex-  
4           ists with respect to the employment of electronic  
5           surveillance to obtain foreign intelligence informa-  
6           tion before an order authorizing such surveillance  
7           can with due diligence be obtained;

8           “(2) determines that the factual basis for  
9           issuance of an order under this title to approve such  
10          electronic surveillance exists;

11          “(3) informs a judge having jurisdiction under  
12          section 103 at the time of such authorization that  
13          the decision has been made to employ emergency  
14          electronic surveillance; and

15          “(4) makes an application in accordance with  
16          this title to a judge having jurisdiction under section  
17          103 as soon as practicable, but not more than 168  
18          hours after the Attorney General authorizes such  
19          surveillance.

20 If the Attorney General authorizes such emergency em-  
21 ployment of electronic surveillance, the Attorney General  
22 shall require that the minimization procedures required by  
23 this title for the issuance of a judicial order be followed.  
24 In the absence of a judicial order approving such electronic  
25 surveillance, the surveillance shall terminate when the in-

1 formation sought is obtained, when the application for the  
2 order is denied, or after the expiration of 168 hours from  
3 the time of authorization by the Attorney General, which-  
4 ever is earliest. In the event that such application for ap-  
5 proval is denied, or in any other case where the electronic  
6 surveillance is terminated and no order is issued approving  
7 the surveillance, no information obtained or evidence de-  
8 rived from such surveillance shall be received in evidence  
9 or otherwise disclosed in any trial, hearing, or other pro-  
10 ceeding in or before any court, grand jury, department,  
11 office, agency, regulatory body, legislative committee, or  
12 other authority of the United States, a State, or political  
13 subdivision thereof, and no information concerning any  
14 United States person acquired from such surveillance shall  
15 subsequently be used or disclosed in any other manner by  
16 Federal officers or employees without the consent of such  
17 person, except with the approval of the Attorney General  
18 if the information indicates a threat of death or serious  
19 bodily harm to any person. A denial of the application  
20 made under this subsection may be reviewed as provided  
21 in section 103.”;

22 (7) in subsection (h), as redesignated by para-  
23 graph (4)—

24 (A) by striking “a wire or” and inserting  
25 “an”; and

1 (B) by striking “physical search” and in-  
2 serting “physical search or in response to a cer-  
3 tification by the Attorney General or a designee  
4 of the Attorney General seeking information,  
5 facilities, or technical assistance from such per-  
6 son under section 102B”; and

7 (8) by adding at the end the following new sub-  
8 section:

9 “(i) In any case in which the Government makes an  
10 application to a judge under this title to conduct electronic  
11 surveillance involving communications and the judge  
12 grants such application, the judge shall also authorize the  
13 installation and use of pen registers and trap and trace  
14 devices to acquire dialing, routing, addressing, and sig-  
15 naling information related to such communications and  
16 such dialing, routing, addressing, and signaling informa-  
17 tion shall not be subject to minimization procedures.”.

18 **SEC. 7. USE OF INFORMATION.**

19 Section 106(i) of the Foreign Intelligence Surveil-  
20 lance Act of 1978 (50 U.S.C. 1806(i)) is amended—

21 (1) by striking “radio communication” and in-  
22 serting “communication”; and

23 (2) by striking “contents indicates” and insert-  
24 ing “contents contain significant foreign intelligence  
25 information or indicate”.



1 **SEC. 8. CONGRESSIONAL OVERSIGHT.**

2 (a) **ELECTRONIC SURVEILLANCE UNDER FISA.**—

3 Section 108 of the Foreign Intelligence Surveillance Act  
4 of 1978 (50 U.S.C. 1808) is amended—

5 (1) in subsection (a)(2)—

6 (A) in subparagraph (B), by striking  
7 “and” at the end;

8 (B) in subparagraph (C), by striking the  
9 period and inserting “; and”; and

10 (C) by adding at the end the following new  
11 subparagraph:

12 “(D) the authority under which the elec-  
13 tronic surveillance is conducted.”; and

14 (2) by striking subsection (b) and inserting the  
15 following:

16 “(b) On a semiannual basis, the Attorney General ad-  
17 ditionally shall fully inform the Permanent Select Com-  
18 mittee on Intelligence of the House of Representatives and  
19 the Select Committee on Intelligence of the Senate on elec-  
20 tronic surveillance conducted without a court order.”.

21 (b) **INTELLIGENCE ACTIVITIES.**—The National Secu-  
22 rity Act of 1947 (50 U.S.C. 401 et seq.) is amended—

23 (1) in section 501 (50 U.S.C. 413)—

24 (A) by redesignating subsection (f) as sub-  
25 section (g); and

1 (B) by inserting after subsection (e) the  
2 following new subsection:

3 “(f) The Chair of each of the congressional intel-  
4 ligence committees, in consultation with the ranking mem-  
5 ber of the committee for which the person is Chair, may  
6 inform—

7 “(1) on a bipartisan basis, all members or any  
8 individual members of such committee, and

9 “(2) any essential staff of such committee,  
10 of a report submitted under subsection (a)(1) or sub-  
11 section (b) as such Chair considers necessary.”;

12 (2) in section 502 (50 U.S.C. 414), by adding  
13 at the end the following new subsection:

14 “(d) INFORMING OF COMMITTEE MEMBERS.—The  
15 Chair of each of the congressional intelligence committees,  
16 in consultation with the ranking member of the committee  
17 for which the person is Chair, may inform—

18 “(1) on a bipartisan basis, all members or any  
19 individual members of such committee, and

20 “(2) any essential staff of such committee,  
21 of a report submitted under subsection (a) as such Chair  
22 considers necessary.”; and

23 (3) in section 503 (50 U.S.C. 415), by adding  
24 at the end the following new subsection:

1           “(g) The Chair of each of the congressional intel-  
2           ligence committees, in consultation with the ranking mem-  
3           ber of the committee for which the person is Chair, may  
4           inform—

5                   “(1) on a bipartisan basis, all members or any  
6           individual members of such committee, and

7                   “(2) any essential staff of such committee,  
8           of a report submitted under subsection (b), (c), or (d) as  
9           such Chair considers necessary.”.

10 **SEC. 9. INTERNATIONAL MOVEMENT OF TARGETS.**

11           (a) **ELECTRONIC SURVEILLANCE.**—Section 105(d) of  
12           the Foreign Intelligence Surveillance Act of 1978 (50  
13           U.S.C. 1805(d)), as redesignated by section 6(4), is  
14           amended by adding at the end the following new para-  
15           graph:

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

21           (b) **PHYSICAL SEARCH.**—Section 304(d) of the For-  
22           eign Intelligence Surveillance Act of 1978 (50 U.S.C.  
23           1824(d)) is amended by adding at the end the following  
24           new paragraph:

1           “(4) An order issued under this section shall re-  
2           main in force during the authorized period of sur-  
3           veillance notwithstanding the absence of the target  
4           from the United States, unless the Government files  
5           a motion to extinguish the order and the court  
6           grants the motion.”.

7 **SEC. 10. COMPLIANCE WITH COURT ORDERS AND**  
8           **ANTITERRORISM PROGRAMS.**

9           (a) **IN GENERAL.**—Notwithstanding any other provi-  
10          sion of law, and in addition to the immunities, privileges,  
11          and defenses provided by any other provision of law, no  
12          action, claim, or proceeding shall lie or be maintained in  
13          any court, and no penalty, sanction, or other form of rem-  
14          edy or relief shall be imposed by any court or any other  
15          body, against any person for an activity arising from or  
16          relating to the provision to an element of the intelligence  
17          community of any information (including records or other  
18          information pertaining to a customer), facilities, or assist-  
19          ance during the period of time beginning on September  
20          11, 2001, and ending on the date that is 60 days after  
21          the date of the enactment of this Act, in connection with  
22          any alleged communications intelligence program that the  
23          Attorney General or a designee of the Attorney General  
24          certifies, in a manner consistent with the protection of  
25          State secrets, is, was, or would be intended to protect the

1 United States from a terrorist attack. This section shall  
2 apply to all actions, claims, or proceedings pending on or  
3 after the effective date of this Act.

4 (b) JURISDICTION.—Any action, claim, or proceeding  
5 described in subsection (a) that is brought in a State court  
6 shall be deemed to arise under the Constitution and laws  
7 of the United States and shall be removable pursuant to  
8 section 1441 of title 28, United States Code.

9 (c) DEFINITIONS.—In this section:

10 (1) INTELLIGENCE COMMUNITY.—The term  
11 “intelligence community” has the meaning given the  
12 term in section 3(4) of the National Security Act of  
13 1947 (50 U.S.C. 401a(4)).

14 (2) PERSON.—The term “person” has the  
15 meaning given the term in section 2510(6) of title  
16 18, United States Code.

17 **SEC. 11. REPORT ON MINIMIZATION PROCEDURES.**

18 (a) REPORT.—Not later than two years after the date  
19 of the enactment of this Act, and annually thereafter until  
20 December 31, 2009, the Director of the National Security  
21 Agency, in consultation with the Director of National In-  
22 telligence and the Attorney General, shall submit to the  
23 Permanent Select Committee on Intelligence of the House  
24 of Representatives and the Select Committee on Intel-  
25 ligence of the Senate a report on the effectiveness and use

1 of minimization procedures applied to information con-  
2 cerning United States persons acquired during the course  
3 of a communications activity conducted by the National  
4 Security Agency.

5 (b) REQUIREMENTS.—A report submitted under sub-  
6 section (a) shall include—

7 (1) a description of the implementation, during  
8 the course of communications intelligence activities  
9 conducted by the National Security Agency, of pro-  
10 cedures established to minimize the acquisition, re-  
11 tention, and dissemination of nonpublicly available  
12 information concerning United States persons;

13 (2) the number of significant violations, if any,  
14 of such minimization procedures during the 18  
15 months following the effective date of this Act; and

16 (3) summary descriptions of such violations.

17 (c) RETENTION OF INFORMATION.—Information con-  
18 cerning United States persons shall not be retained solely  
19 for the purpose of complying with the reporting require-  
20 ments of this section.

21 **SEC. 12. AUTHORIZATION AFTER AN ARMED ATTACK.**

22 (a) ELECTRONIC SURVEILLANCE.—Section 111 of  
23 the Foreign Intelligence Surveillance Act of 1978 (50  
24 U.S.C. 1811) is amended by striking “for a period not  
25 to exceed” and all that follows and inserting the following:

1 “for a period not to exceed 90 days following an armed  
2 attack against the territory of the United States if the  
3 President submits to the Permanent Select Committee on  
4 Intelligence of the House of Representatives and the Se-  
5 lect Committee on Intelligence of the Senate notification  
6 of the authorization under this section.”.

7 (b) PHYSICAL SEARCH.—Section 309 of such Act (50  
8 U.S.C. 1829) is amended by striking “for a period not  
9 to exceed” and all that follows and inserting the following:  
10 “for a period not to exceed 90 days following an armed  
11 attack against the territory of the United States if the  
12 President submits to the Permanent Select Committee on  
13 Intelligence of the House of Representatives and the Se-  
14 lect Committee on Intelligence of the Senate notification  
15 of the authorization under this section.”.

16 **SEC. 13. AUTHORIZATION OF ELECTRONIC SURVEILLANCE**  
17 **AFTER A TERRORIST ATTACK.**

18 The Foreign Intelligence Surveillance Act of 1978  
19 (50 U.S.C. 1801 et seq.) is further amended—

20 (1) by adding at the end of title I the following  
21 new section:

22 “AUTHORIZATION FOLLOWING A TERRORIST ATTACK  
23 UPON THE UNITED STATES

24 “SEC. 112. (a) IN GENERAL.—Notwithstanding any  
25 other provision of law, but subject to the provisions of this  
26 section, the President, acting through the Attorney Gen-

1 eral, may authorize electronic surveillance without an  
2 order under this title to acquire foreign intelligence infor-  
3 mation for a period not to exceed 90 days following a ter-  
4 rorist attack against the United States if the President  
5 submits a notification to the congressional intelligence  
6 committees and a judge having jurisdiction under section  
7 103 that—

8           “(1) the United States has been the subject of  
9           a terrorist attack; and

10           “(2) identifies the terrorist organizations or af-  
11           filiates of terrorist organizations believed to be re-  
12           sponsible for the terrorist attack.

13           “(b) SUBSEQUENT CERTIFICATIONS.—At the end of  
14 the 90-day period described in subsection (a), and every  
15 90 days thereafter, the President may submit a subse-  
16 quent certification to the congressional intelligence com-  
17 mittees and a judge having jurisdiction under section 103  
18 that the circumstances of the terrorist attack for which  
19 the President submitted a certification under subsection  
20 (a) require the President to continue the authorization of  
21 electronic surveillance under this section for an additional  
22 90 days. The President shall be authorized to conduct  
23 electronic surveillance under this section for an additional  
24 90 days after each such subsequent certification.



1       “(c) ELECTRONIC SURVEILLANCE OF INDIVID-  
2 UALS.—The President, or an official designated by the  
3 President to authorize electronic surveillance, may only  
4 conduct electronic surveillance of a person under this sec-  
5 tion if the President or such official determines that—

6               “(1) there is a reasonable belief that such per-  
7 son is communicating with a terrorist organization  
8 or an affiliate of a terrorist organization that is rea-  
9 sonably believed to be responsible for the terrorist  
10 attack; and

11               “(2) the information obtained from the elec-  
12 tronic surveillance may be foreign intelligence infor-  
13 mation.

14       “(d) MINIMIZATION PROCEDURES.—The President  
15 may not authorize electronic surveillance under this sec-  
16 tion until the Attorney General approves minimization  
17 procedures for electronic surveillance conducted under this  
18 section.

19       “(e) UNITED STATES PERSONS.—Notwithstanding  
20 subsection (a) or (b), the President may not authorize  
21 electronic surveillance of a United States person under  
22 this section without an order under this title for a period  
23 of more than 60 days unless the President, acting through  
24 the Attorney General, submits a certification to the con-  
25 gressional intelligence committees that—

1           “(1) the continued electronic surveillance of the  
2           United States person is vital to the national security  
3           of the United States;

4           “(2) describes the circumstances that have pre-  
5           vented the Attorney General from obtaining an order  
6           under this title for continued surveillance;

7           “(3) describes the reasons for believing the  
8           United States person is affiliated with or in commu-  
9           nication with a terrorist organization or affiliate of  
10          a terrorist organization that is reasonably believed to  
11          be responsible for the terrorist attack; and

12          “(4) describes the foreign intelligence informa-  
13          tion derived from the electronic surveillance con-  
14          ducted under this section.

15          “(f) USE OF INFORMATION.—Information obtained  
16          pursuant to electronic surveillance under this subsection  
17          may be used to obtain an order authorizing subsequent  
18          electronic surveillance under this title.

19          “(g) REPORTS.—Not later than 14 days after the  
20          date on which the President submits a certification under  
21          subsection (a), and every 30 days thereafter until the  
22          President ceases to authorize electronic surveillance under  
23          subsection (a) or (b), the President shall submit to the  
24          congressional intelligence committees a report on the elec-

1 tronic surveillance conducted under this section, includ-  
2 ing—

3 “(1) a description of each target of electronic  
4 surveillance under this section; and

5 “(2) the basis for believing that each target is  
6 in communication with a terrorist organization or an  
7 affiliate of a terrorist organization.

8 “(h) CONGRESSIONAL INTELLIGENCE COMMITTEES  
9 DEFINED.—In this section, the term ‘congressional intel-  
10 ligence committees’ means the Permanent Select Com-  
11 mittee on Intelligence of the House of Representatives and  
12 the Select Committee on Intelligence of the Senate.”; and

13 (2) in the table of contents in the first section,  
14 by inserting after the item relating to section 111  
15 the following new item:

“Sec. 112. Authorization following a terrorist attack upon the United States.”.

16 **SEC. 14. AUTHORIZATION OF ELECTRONIC SURVEILLANCE**  
17 **DUE TO IMMINENT THREAT.**

18 The Foreign Intelligence Surveillance Act of 1978  
19 (50 U.S.C. 1801 et seq.) is further amended—

20 (1) by adding at the end of title I the following  
21 new section:

22 “AUTHORIZATION DUE TO IMMINENT THREAT

23 “SEC. 113. (a) IN GENERAL.—Notwithstanding any  
24 other provision of law, but subject to the provisions of this  
25 section, the President, acting through the Attorney Gen-

1 eral, may authorize electronic surveillance without an  
2 order under this title to acquire foreign intelligence infor-  
3 mation for a period not to exceed 90 days if the President  
4 submits to the congressional leadership, the congressional  
5 intelligence committees, and the Foreign Intelligence Sur-  
6 veillance Court a written notification that the President  
7 has determined that there exists an imminent threat of  
8 attack likely to cause death, serious injury, or substantial  
9 economic damage to the United States. Such notifica-  
10 tion—

11           “(1) shall be submitted as soon as practicable,  
12           but in no case later than 5 days after the date on  
13           which the President authorizes electronic surveil-  
14           lance under this section;

15           “(2) shall specify the entity responsible for the  
16           threat and any affiliates of the entity;

17           “(3) shall state the reason to believe that the  
18           threat of imminent attack exists;

19           “(4) shall state the reason the President needs  
20           broader authority to conduct electronic surveillance  
21           in the United States as a result of the threat of im-  
22           minent attack;

23           “(5) shall include a description of the foreign  
24           intelligence information that will be collected and the

1 means that will be used to collect such foreign intel-  
2 ligence information; and

3 “(6) may be submitted in classified form.

4 “(b) SUBSEQUENT CERTIFICATIONS.—At the end of  
5 the 90-day period described in subsection (a), and every  
6 90 days thereafter, the President may submit a subse-  
7 quent written notification to the congressional leadership,  
8 the congressional intelligence committees, the other rel-  
9 evant committees, and the Foreign Intelligence Surveil-  
10 lance Court that the circumstances of the threat for which  
11 the President submitted a written notification under sub-  
12 section (a) require the President to continue the author-  
13 ization of electronic surveillance under this section for an  
14 additional 90 days. The President shall be authorized to  
15 conduct electronic surveillance under this section for an  
16 additional 90 days after each such subsequent written no-  
17 tification.

18 “(c) ELECTRONIC SURVEILLANCE OF INDIVID-  
19 UALS.—The President, or an official designated by the  
20 President to authorize electronic surveillance, may only  
21 conduct electronic surveillance of a person under this sec-  
22 tion if the President or such official determines that—

23 “(1) there is a reasonable belief that such per-  
24 son is communicating with an entity or an affiliate

1 of an entity that is reasonably believed to be respon-  
2 sible for imminent threat of attack; and

3 “(2) the information obtained from the elec-  
4 tronic surveillance may be foreign intelligence infor-  
5 mation.

6 “(d) MINIMIZATION PROCEDURES.—The President  
7 may not authorize electronic surveillance under this sec-  
8 tion until the Attorney General approves minimization  
9 procedures for electronic surveillance conducted under this  
10 section.

11 “(e) UNITED STATES PERSONS.—Notwithstanding  
12 subsections (a) and (b), the President may not authorize  
13 electronic surveillance of a United States person under  
14 this section without an order under this title for a period  
15 of more than 60 days unless the President, acting through  
16 the Attorney General, submits a certification to the con-  
17 gressional intelligence committees that—

18 “(1) the continued electronic surveillance of the  
19 United States person is vital to the national security  
20 of the United States;

21 “(2) describes the circumstances that have pre-  
22 vented the Attorney General from obtaining an order  
23 under this title for continued surveillance;

24 “(3) describes the reasons for believing the  
25 United States person is affiliated with or in commu-

1        nication with an entity or an affiliate of an entity  
2        that is reasonably believed to be responsible for im-  
3        minent threat of attack; and

4               “(4) describes the foreign intelligence informa-  
5        tion derived from the electronic surveillance con-  
6        ducted under this section.

7        “(f) USE OF INFORMATION.—Information obtained  
8        pursuant to electronic surveillance under this subsection  
9        may be used to obtain an order authorizing subsequent  
10       electronic surveillance under this title.

11       “(g) DEFINITIONS.—In this section:

12               “(1) CONGRESSIONAL INTELLIGENCE COMMIT-  
13        TEES.—The term ‘congressional intelligence commit-  
14        tees’ means the Permanent Select Committee on In-  
15        telligence of the House of Representatives and the  
16        Select Committee on Intelligence of the Senate.

17               “(2) CONGRESSIONAL LEADERSHIP.—The term  
18        ‘congressional leadership’ means the Speaker and  
19        minority leader of the House of Representatives and  
20        the majority leader and minority leader of the Sen-  
21        ate.

22               “(3) FOREIGN INTELLIGENCE SURVEILLANCE  
23        COURT.—The term ‘Foreign Intelligence Surveillance  
24        Court’ means the court established under section  
25        103(a).

1           “(4) OTHER RELEVANT COMMITTEES.—The  
2 term ‘other relevant committees’ means the Commit-  
3 tees on Appropriations, the Committees on Armed  
4 Services, and the Committees on the Judiciary of  
5 the House of Representatives and the Senate.”; and

6           (2) in the table of contents in the first section,  
7 by inserting after the item relating to section 112,  
8 as added by section 13(2), the following new item:

“Sec. 113. Authorization due to imminent threat.”.

9 **SEC. 15. TECHNICAL AND CONFORMING AMENDMENTS.**

10       The Foreign Intelligence Surveillance Act of 1978  
11 (50 U.S.C. 1801 et seq.) is further amended—

12           (1) in section 105(a)(4), as redesignated by sec-  
13 tion 6(1)(B)—

14               (A) by striking “104(a)(7)(E)” and insert-  
15 ing “104(a)(7)(D)”; and

16               (B) by striking “104(d)” and inserting  
17 “104(c)”;

18           (2) in section 106(j), in the matter preceding  
19 paragraph (1), by striking “105(e)” and inserting  
20 “105(d)”; and



1           (3) in section 108(a)(2)(C), by striking  
2           “105(f)” and inserting “105(e)”.

          Passed the House of Representatives September 28,  
2006.

Attest:

*Clerk.*

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

**H. R. 5825**

---

**AN ACT**

To update the Foreign Intelligence Surveillance Act  
of 1978.