

shall, upon conviction, be fined not more than \$50,000, or, if a natural person, may be imprisoned for not more than ten years, or both; and any officer, director, or agent of any corporation who knowingly participates in such violation may be punished by a like fine, imprisonment, or both.

(Pub. L. 95-223, title II, § 206, Dec. 28, 1977, 91 Stat. 1628.)

§ 1706. Savings provisions

(a) Termination of national emergencies pursuant to National Emergencies Act

(1) Except as provided in subsection (b) of this section, notwithstanding the termination pursuant to the National Emergencies Act [50 U.S.C. 1601 et seq.] of a national emergency declared for purposes of this chapter, any authorities granted by this chapter, which are exercised on the date of such termination on the basis of such national emergency to prohibit transactions involving property in which a foreign country or national thereof has any interest, may continue to be so exercised to prohibit transactions involving that property if the President determines that the continuation of such prohibition with respect to that property is necessary on account of claims involving such country or its nationals.

(2) Notwithstanding the termination of the authorities described in section 101(b) of this Act, any such authorities, which are exercised with respect to a country on the date of such termination to prohibit transactions involving any property in which such country or any national thereof has any interest, may continue to be exercised to prohibit transactions involving that property if the President determines that the continuation of such prohibition with respect to that property is necessary on account of claims involving such country or its nationals.

(b) Congressional termination of national emergencies by concurrent resolution

The authorities described in subsection (a)(1) of this section may not continue to be exercised under this section if the national emergency is terminated by the Congress by concurrent resolution pursuant to section 202 of the National Emergencies Act [50 U.S.C. 1622] and if the Congress specifies in such concurrent resolution that such authorities may not continue to be exercised under this section.

(c) Supplemental savings provisions; supersedure of inconsistent provisions

(1) The provisions of this section are supplemental to the savings provisions of paragraphs (1), (2), and (3) of section 101(a) [50 U.S.C. 1601(a)(1), (2), (3)] and of paragraphs (A), (B), and (C) of section 202(a) [50 U.S.C. 1622(a)(A), (B), and (C)] of the National Emergencies Act.

(2) The provisions of this section supersede the termination provisions of section 101(a) [50 U.S.C. 1601(a)] and of title II [50 U.S.C. 1621 et seq.] of the National Emergencies Act to the extent that the provisions of this section are inconsistent with these provisions.

(d) Periodic reports to Congress

If the President uses the authority of this section to continue prohibitions on transactions involving foreign property interests, he shall report to the Congress every six months on the use of such authority.

(Pub. L. 95-223, title II, § 207, Dec. 28, 1977, 91 Stat. 1628.)

REFERENCES IN TEXT

The National Emergencies Act, referred to in subsecs. (a)(1) and (c)(2), is Pub. L. 94-412, Sept. 14, 1976, 90 Stat. 1255, as amended, which is classified principally to chapter 34 (§ 1601 et seq.) of this title. Title II of the National Emergencies Act is classified generally to subchapter II (§ 1621 et seq.) of chapter 34 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

Section 101(b) of this Act, referred to in subsec. (a)(2), is section 101(b) of Pub. L. 95-223, which is set out as a note under section 5 of the Appendix to this title.

CHAPTER 36—FOREIGN INTELLIGENCE SURVEILLANCE

| | |
|-------|--|
| Sec. | |
| 1801. | Definitions. |
| 1802. | Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction of court. |
| 1803. | Designation of judges. <ul style="list-style-type: none"> (a) Court to hear applications and grant orders; record of denial; transmittal to court of review. (b) Court of review; record, transmittal to Supreme Court. (c) Expeditious conduct of proceedings; security measures for maintenance of records. (d) Tenure. |
| 1804. | Applications for court orders. <ul style="list-style-type: none"> (a) Submission by Federal officer; approval of Attorney General; contents. (b) Exclusion of certain information respecting foreign power targets. (c) Additional affidavits or certifications. (d) Additional information. |
| 1805. | Issuance or order. <ul style="list-style-type: none"> (a) Necessary findings. (b) Specifications and directions of orders. (c) Exclusion of certain information respecting foreign power targets. (d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated. (e) Emergency orders. (f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel. (g) Retention of certifications, applications and orders. |
| 1806. | Use of information. <ul style="list-style-type: none"> (a) Compliance with minimization procedures; privileged communications; lawful purposes. (b) Statement for disclosure. (c) Notification by United States. |

- Sec.
- (d) Notification by States or political subdivisions.
 - (e) Motion to suppress.
 - (f) In camera and ex parte review by district court.
 - (g) Suppression of evidence; denial of motion.
 - (h) Finality of orders.
 - (i) Destruction of unintentionally acquired information.
 - (j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination.
1807. Report to Administrative Office of the United States Court and to Congress.
1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress.
1809. Criminal sanctions.
- (a) Prohibited activities.
 - (b) Defense.
 - (c) Penalties.
 - (d) Federal jurisdiction.
1810. Civil liability.
1811. Authorization during time of war.

CHAPTER REFERRED TO IN OTHER SECTIONS

This chapter is referred to in title 18 section 2511.

§ 1801. Definitions

As used in this chapter:

(a) "Foreign power" means—

- (1) a foreign government or any component thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation therefor;
- (5) a foreign-based political organization, not substantially composed of United States persons; or
- (6) an entity that is directed and controlled by a foreign government or governments.

(b) "Agent of a foreign power" means—

- (1) any person other than a United States person, who—
 - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
 - (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
- (2) any person who—

- (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

- (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

- (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

- (D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that—

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

- (2) appear to be intended—

- (A) to intimidate or coerce a civilian population;

- (B) to influence the policy of a government by intimidation or coercion; or

- (C) to affect the conduct of a government by assassination or kidnapping; and

- (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of title 18, or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means—

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

- (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

- (2) information with respect to a foreign power or foreign territory that relates to,

and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

(h) "Minimization procedures", with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is

evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(Pub. L. 95-511, title I, § 101, Oct. 25, 1978, 92 Stat. 1783.)

EFFECTIVE DATE; EXCEPTION

Section 301 of Pub. L. 95-511 provided that: "The provisions of this Act [enacting this chapter, amending sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacting provision set out as a note below] and the amendments made hereby shall become effective upon the date of enactment of this Act [Oct. 25, 1978], except that any elec-

tronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of this Act, if that surveillance is terminated or an order approving that surveillance is obtained under title I of this Act [enacting this chapter] within ninety days following the designation of the first judge pursuant to section 103 of this Act [section 1803 of this title]."

SHORT TITLE

Section 1 of Pub. L. 95-511 provided: "That this Act [enacting this chapter, amending sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacting provision set out as a note above] may be cited as the 'Foreign Intelligence Surveillance Act of 1978.'"

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1802, 1804, 1805, 1810 of this title; title 18 section 2511.

§ 1802. Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction of court

(a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this chapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and

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

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report

such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.

(3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or

(B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title.

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this chapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

(Pub. L. 95-511, title I, § 102, Oct. 25, 1978, 92 Stat. 1786.)

EX. ORD. NO. 12139. EXERCISE OF CERTAIN AUTHORITY RESPECTING ELECTRONIC SURVEILLANCE

Ex. Ord. No. 12139, May 23, 1979, 44 F.R. 30311, provided:

By the authority vested in me as President by Sections 102 and 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802 and 1804), in order to provide as set forth in that Act [this chapter] for the authorization of electronic surveillance for foreign intelligence purposes, it is hereby ordered as follows:

1-101. Pursuant to Section 102(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.

1802(a)), the Attorney General is authorized to approve electronic surveillance to acquire foreign intelligence information without a court order, but only if the Attorney General makes the certifications required by that Section.

1-102. Pursuant to Section 102(b) of the Foreign Intelligence Act of 1978 (50 U.S.C. 1802(b)), the Attorney General is authorized to approve applications to the court having jurisdiction under Section 103 of that Act [50 U.S.C. 1803] to obtain orders for electronic surveillance for the purpose of obtaining foreign intelligence information.

1-103. Pursuant to Section 104(a)(7) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804(a)(7)), the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by Section 104(a)(7) of the Act in support of applications to conduct electronic surveillance:

- (a) Secretary of State.
- (b) Secretary of Defense.
- (c) Director of Central Intelligence.
- (d) Director of the Federal Bureau of Investigation.
- (e) Deputy Secretary of State.
- (f) Deputy Secretary of Defense.
- (g) Deputy Director of Central Intelligence.

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate.

1-104. Section 2-202 of Executive Order No. 12036 [set out under section 401 of this title] is amended by inserting the following at the end of that section: "Any electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act as well as this Order."

1-105. Section 2-203 of Executive Order No. 12036 [set out under section 401 of this title] is amended by inserting the following at the end of that section: "Any monitoring which constitutes electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978 shall be conducted in accordance with that Act as well as this Order."

JIMMY CARTER.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1801, 1805 of this title.

§ 1803. Designation of judges

- (a) Court to bear applications and grant orders; record of denial; transmittal to court of review

The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason of his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section.

- (b) Court of review; record, transmittal to Supreme Court

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

- (c) Expeditious conduct of proceedings; security measures for maintenance of records

Proceedings under this Act shall be conducted as expeditiously as possible. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

- (d) Tenure

Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

(Pub. L. 95-511, title I, § 103, Oct. 25, 1978, 92 Stat. 1788.)

REFERENCES IN TEXT

This Act, referred to in subsecs. (a), (b), and (c), means Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, known as the Foreign Intelligence Surveillance Act of 1978, which enacted this chapter, amended sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacted provisions set out as notes under section 1801 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1802, 1804, 1805 of this title.

§ 1804. Applications for court orders

- (a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving electronic surveillance under this chapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this chapter. It shall include—

(1) the identity of the Federal officer making the application;

(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate—

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

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

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

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this chapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this chapter should not automatically terminate when the described type of information

has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

(b) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a) of this section, but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title.

(Pub. L. 95-511, title I, § 104, Oct. 25, 1978, 92 Stat. 1788.)

DESIGNATION OF CERTAIN OFFICIALS TO MAKE CERTIFICATIONS

For designation of certain officials to make certifications required by subsec. (a)(7) of this section, see Ex. Ord. No. 12139, May 23, 1979, 44 F.R. 30311, set out under section 1802 of this title.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1802, 1805 of this title.

§ 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1804(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(h) Specifications and directions of orders

An order approving an electronic surveillance under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the electronic surveillance;

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

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security

procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1) of this section, but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less.

(2) Extensions of an order issued under this chapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that an extension of an order under this Act for a surveillance targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Emergency orders

Notwithstanding any other provision of this chapter, when the Attorney General reasonably determines that—

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this chapter to approve such surveillance exists;

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this chapter is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this chapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel

Notwithstanding any other provision of this chapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test

personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided*, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, or section 605 of title 47, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this chapter; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Retention of certifications, applications and orders

Certifications made by the Attorney General pursuant to section 1802(a) of this title and applications made and orders granted under this chapter shall be retained for a period of at least ten years from the date of the certification or application.

(Pub. L. 95-511, title I, § 105, Oct. 25, 1978, 92 Stat. 1790.)

REFERENCES IN TEXT

This Act, referred to in subsec. (d)(2), means Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, known as the Foreign Intelligence Surveillance Act of 1978, which enacted this chapter, amended sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacted provisions set out as notes under section 1801 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 1801, 1802, 1804, 1806 of this title.

§ 1806. Use of information**(a) Compliance with minimization procedures; privileged communications; lawful purposes**

Information acquired from an electronic surveillance conducted pursuant to this chapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this chapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this chapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this chapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this chapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this chapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency,

regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

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

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(b) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of

the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(Pub. L. 95-511, title I, § 106, Oct. 25, 1978, 92 Stat. 1793.)

REFERENCES IN TEXT

This Act, referred to in subsec. (f), means Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, known as the Foreign Intelligence Surveillance Act of 1978, which enacted this chapter, amended sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacted provisions set out as notes under section 1801 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 1802 of this title.

§ 1807. Report to Administrative Office of the United States Court and to Congress

In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this chapter; and

(b) the total number of such orders and extensions either granted, modified, or denied.

(Pub. L. 95-511, title I, § 107, Oct. 25, 1978, 92 Stat. 1795.)

§ 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

(a) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this chapter. Nothing in this chapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

(Pub. L. 95-511, title I, § 108, Oct. 25, 1978, 92 Stat. 1795.)

REFERENCES IN TEXT

This Act, referred to in subsec. (b), means Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, known as the Foreign Intelligence Surveillance Act of 1978, which enacted this chapter, amended sections 2511, 2518, and 2519 of Title 18, Crimes and Criminal Procedure, and enacted provisions set out as notes under section 1801 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 1802 of this title.

§ 1809. Criminal sanctions

(a) Prohibited activities

A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by statute; or

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

(b) Defense

It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) Penalties

An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

(d) Federal jurisdiction

There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

(Pub. L. 95-511, title I, § 109, Oct. 25, 1978, 92 Stat. 1796.)

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 1810 of this title.

§ 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as de-

finied in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(a) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

(Pub. L. 95-511, title I, § 110, Oct. 25, 1978, 92 Stat. 1796.)

§ 1811. Authorization during time of war

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this chapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

(Pub. L. 95-511, title I, § 111, Oct. 25, 1978, 92 Stat. 1796.)