Calendar No. 502

103D CONGRESS
2d Session

SENATE

REPORT
103–296

THE COUNTERINTELLIGENCE AND SECURITY ENHANCEMENTS ACT OF 1994

JUNE 30 (legislative day, JUNE 7), 1994.—Ordered to be printed

Mr. DECONCINI, from the Select Committee on Intelligence, submitted the following

REPORT

[To accompany S. 2056, as amended]

The Select Committee on Intelligence, having considered S. 2056, a bill to amend the National Security Act of 1947 to improve the counterintelligence and security posture of the United States, and for other purposes, reports favorably with an amendment in the form of a substitute and recommends that the bill as amended do pass.

PURPOSE

The purpose of S. 2056 is to improve the ability of the United States Government to deter persons with access to classified information from turning to the crime of espionage, to facilitate the detection of persons who commit espionage, and to provide additional authority to prosecute and redress espionage activities.

AMENDMENT

Strike all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Counterintelligence and Security Enhancements Act of 1994".

SEC. 2. ACCESS TO CLASSIFIED INFORMATION.

(a) AMENDMENT OF THE NATIONAL SECURITY ACT OF 1947.—The National Security Act of 1947 (50 U.S.C. 401 et seq.) is amended by adding at the end the following new title:

"TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

"PROCEDURES

"SEC. 801. Not later than 180 days after the date of enactment of this title, the President shall, by Executive order or regulation, establish procedures to govern access to classified information which shall be binding upon all departments, agencies, and offices of the executive branch of Government. Such procedures shall, at a minimum—

"(1) provide that, except as may be permitted by the President, no employee in the executive branch of Government may be given access to classified information by any department, agency, or office of the executive branch of Government unless, based upon an appropriate background investigation, such access is determined to be clearly consistent with the national security interests of the United States;

"(2) establish uniform minimum requirements governing the scope and frequency of background investigations and reinvestigations for all employees in the executive branch of Government who require access to classified information as part of their official responsibilities;

"(3) provide that all employees in the executive branch of Government who require access to classified information shall be required as a condition of such access to provide written consent to the employing department or agency which permits access by an authorized investigative agency to relevant financial records, other financial information, consumer reports, and travel records, as determined by the President, in accordance with section 802 of this title, during the period of access to classified information and for a period of five years thereafter;

"(4) provide that all employees in the executive branch of Government who require access to particularly sensitive classified information, as determined by the President, shall be required, as a condition of maintaining access to such information, to submit to the employing department or agency, during the period of such access, relevant information concerning their financial conditions and foreign travel, as determined by the President, as may be necessary to ensure appropriate security; and

"(5) establish uniform minimum standards to ensure that employees whose access to classified information is being denied or terminated under this title are appropriately advised of the reasons for such denial or termination and are provided an adequate opportunity to respond to all adverse information which forms the basis for such denial or termination before final action by the department or agency concerned, except that, wherever such information is derived from a classified source, appropriate measures shall be taken to conceal the identity of such source from the employee concerned.

"REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

"SEC. 802. (a)(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding agency, or from any consumer credit reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by a person outside the United States.

"(2) Requests may be made under this section where—

"(A) the records sought pertain to a person who is or was an employee required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than 5 years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

"(B)(i) there is information or allegations indicating that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

"(ii) information comes to the attention of the employing agency indicating the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

"(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

"(3) Each such request—

"(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that—

"(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

"(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

"(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

"(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

"(C) shall identify specifically or by category the records or information to be reviewed; and

"(D) shall inform the recipient of the request of the prohibition described in subsection (b).

"(b) Notwithstanding any other provision of law, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person, other than those officers, employees, or agents of such entity necessary to satisfy a request made under this section, that such entity has received or satisfied a request made by an authorized investigative agency under this section.

"(c)(1) Notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) shall, if the request satisfies the requirements of this section, make available such records or information within 30 days for inspection or copying, as may be appropriate, by the agency requesting such records or information.

"(2) Any entity (including any officer, employee, or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the certifications made by an agency pursuant to this section shall not be liable for any such disclosure to any person under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

"(d) Any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

"(e) An agency receiving records or information pursuant to a request under this section may disseminate the records or information obtained pursuant to such request outside the agency only—

"(1) to the agency employing the employee who is the subject of the records or information;

"(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

"(3) with respect to dissemination to an agency of the United States, if such information is clearly relevant to the authorized responsibilities of such agency.

"(f) Nothing in this section may be construed to affect the authority of an investigative agency to obtain information pursuant to the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

"EXCEPTIONS

"SEC. 803. Except as otherwise specifically provided, the provisions of this title shall not apply to the President and Vice President, Members of the Congress, Justices of the Supreme Court, and Federal judges appointed by the President.

"DEFINITIONS

"SEC. 804. For purposes of this title—

"(1) the term 'authorized investigative agency' means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information;

"(2) the term 'classified information' means any information that has been determined pursuant to Executive Order No. 12356 of April 2, 1982, or successive orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated;

"(3) the term 'consumer credit reporting agency' has the meaning given such term in section 603 of the Consumer Credit Protection Act (15 U.S.C. 1681a);

"(4) the term 'employee' includes any person who receives a salary or compensation of any kind from the United States Government, is a contractor of the United States Government or an employee thereof, is an unpaid consultant of the United States Government, or otherwise acts for or on behalf of the United States Government;

"(5) the terms 'financial agency' and 'financial institution' have the meanings given to such terms in section 5312(a) of title 31, United States Code, and the term 'holding agency' has the meaning given to such term in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

"(6) the terms 'foreign power' and 'agent of a foreign power' have the same meanings as set forth in sections 101 (a) and (b), respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

"(7) the term 'State' means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau (until such time as the Compact of Free Association is ratified), and any other possession of the United States.".

(b) CLERICAL AMENDMENT.—The table of contents of the National Security Act of 1947 is amended by adding at the end the following:

"TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

"Sec. 801. Procedures.
"Sec. 802. Requests by authorized investigative agencies.
"Sec. 803. Exceptions.
"Sec. 804. Definitions.".

(c) EFFECTIVE DATE.—The amendments made by subsections (a) and (b) shall take effect 180 days after the date of enactment of this Act.

SEC. 3. COORDINATION OF COUNTERINTELLIGENCE ACTIVITIES.

(a) ESTABLISHMENT OF COUNTERINTELLIGENCE POLICY BOARD.—(1) There is established within the executive branch of Government a National Counterintelligence Policy Board (in this section referred to as the "Board"). The Board shall report to the President through the National Security Council.

(2) The Board shall consist of the following individuals:

(A) The Attorney General, who shall serve as Chair.

(B) The Secretary of Defense.

(C) The Director of Central Intelligence.

(D) The Director of the Federal Bureau of Investigation.

(E) The Assistant to the President for National Security Affairs.

(b) FUNCTION OF THE BOARD.—The Board shall serve as the principal mechanism for—

(1) developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and

(2) resolving conflicts, as directed by the President, which may arise between elements of the Government which carry out such activities.

(c) COORDINATION OF COUNTERINTELLIGENCE MATTERS WITH THE FEDERAL BUREAU OF INVESTIGATION.—(1) The head of each department or agency within the executive branch of Government shall ensure that—

(A) the Federal Bureau of Investigation is advised immediately of any information, regardless of its source, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power;

(B) following a report made pursuant to subparagraph (A), the Federal Bureau of Investigation is consulted with respect to all subsequent actions which may be undertaken by the department or agency concerned to determine the source of such loss or compromise; and

(C) where, after appropriate consultation with the department or agency concerned, the Federal Bureau of Investigation undertakes investigative activities to determine the source of the loss or compromise, the Bureau is given complete and timely access to its employees and records for purposes of such investigative activities.

(2) Beginning on February 1, 1995, and each year thereafter, the Director of the Federal Bureau of Investigation shall, in consultation with the Director of Central Intelligence and the Secretary of Defense, submit a report to the Select Committee on Intelligence of the Senate and to the Permanent Select Committee on Intelligence

of the House of Representatives with respect to compliance with paragraph (1) during the preceding calendar year.

(3) Nothing in this subsection may be construed to alter the existing jurisdictional arrangements between the Federal Bureau of Investigation and the Department of Defense with respect to investigations of persons subject to the Uniform Code of Military Justice, nor to impose additional reporting requirements upon the Department of Defense with respect to such investigations other than those required by existing law and executive branch policy.

(4) As used in this subsection, the terms "foreign power" and "agent of a foreign power" have the same meanings as set forth in sections 101 (a) and (b), respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

SEC. 4. DISCLOSURE OF CONSUMER CREDIT REPORTS FOR COUNTERINTELLIGENCE PURPOSES.

Section 608 of the Fair Credit Reporting Act (15 U.S.C. 1681f) is amended—

(1) by striking "Notwithstanding" and inserting "(a) DISCLOSURE OF CERTAIN IDENTIFYING INFORMATION.—Notwithstanding"; and

(2) by adding at the end the following new subsection:

"(b) DISCLOSURES TO THE FBI FOR COUNTERINTELLIGENCE PURPOSES.—

"(1) CONSUMER REPORTS.—Notwithstanding the provisions of section 604, a consumer reporting agency shall furnish a consumer report to the Federal Bureau of Investigation when presented with a written request for a consumer report, signed by the Director or Deputy Director of the Federal Bureau of Investigation who certifies compliance with this subsection. The Director or Deputy Director may make such a certification only if he has determined in writing that—

"(A) such records are necessary for the conduct of an authorized foreign counterintelligence investigation; and

"(B) there are specific and articulable facts giving reason to believe that the consumer whose consumer report is sought is a foreign power or an agent of a foreign power, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(2) IDENTIFYING INFORMATION.—Notwithstanding the provisions of section 604, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or Deputy Director, which certifies compliance with this subsection. The Director or Deputy Director may make such certification only if the Director or Deputy Director has determined in writing that—

"(A) such information is necessary to the conduct of an authorized foreign counterintelligence investigation; and

"(B) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power, as so defined.

"(3) CONFIDENTIALITY.—No consumer reporting agency or officer, employee, or agent of such consumer reporting agency may disclose to any person, other than those officers, employees, or agents of such agency necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this subsection, that the Federal Bureau of Investigation has sought or obtained a consumer report or identifying information respecting any consumer under paragraph (1) or (2), nor shall such agency, officer, employee, or agent include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such a consumer report or identifying information.

"(4) PAYMENT OF FEES.—The Federal Bureau of Investigation may, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing credit reports or identifying information in accordance with this title, a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this subsection.

"(5) LIMIT ON DISSEMINATION.—The Federal Bureau of Investigation may not disseminate information obtained pursuant to this subsection outside of the Federal Bureau of Investigation, except to the Department of Justice or as may be necessary for the conduct of a foreign counterintelligence investigation.

"(6) RULES OF CONSTRUCTION.—Nothing in this subsection shall be construed to prohibit information from being furnished by the Federal Bureau of Inves-

tigation pursuant to a subpoena or court order, or in connection with a judicial or administrative proceeding to enforce the provisions of this Act. Nothing in this subsection shall be construed to authorize or permit the withholding of information from Congress.

"(7) REPORTS TO CONGRESS.—On an annual basis, the Attorney General of the United States shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to paragraphs (1) and (2).

"(8) DAMAGES.—Any agency or department of the United States obtaining or disclosing credit reports, records, or information contained therein in violation of this subsection is liable to the consumer to whom such records relate in an amount equal to the sum of—

"(A) $100, without regard to the volume of records involved;

"(B) any actual damages sustained by the consumer as a result of the disclosure;

"(C) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

"(D) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney's fees, as determined by the court.

"(9) GOOD FAITH EXCEPTION.—Any credit reporting agency or agent or employee thereof making disclosure of credit reports or identifying information pursuant to this subsection in good faith reliance upon a certificate of the Federal Bureau of Investigation pursuant to this subsection shall not be liable to any person for such disclosure under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State. As used in this subsection, the term '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.

"(10) LIMITATION OF REMEDIES.—The remedies set forth in this subsection shall be the only judicial remedies for violation of this subsection.

"(11) INJUNCTIVE RELIEF.—In addition to any other remedy contained in this subsection, injunctive relief shall be available to require compliance with the procedures of this subsection. In the event of any successful action under this subsection, costs of the action, together with reasonable attorney's fees, as determined by the court, may be recovered.".

SEC. 5. REWARDS FOR INFORMATION CONCERNING ESPIONAGE.

(a) REWARDS.—Section 3071 of title 18, United States Code, is amended—

(1) by inserting "(a)" before "With respect to"; and

(2) by adding at the end the following new subsection:

"(b) With respect to acts of espionage involving or directed at the United States, the Attorney General may reward any individual who furnishes information—

"(1) leading to the arrest or conviction, in any country, of any individual or individuals for commission of an act of espionage against the United States;

"(2) leading to the arrest or conviction, in any country, of any individual or individuals for conspiring or attempting to commit an act of espionage against the United States; or

"(3) leading to the prevention or frustration of an act of espionage against the United States.".

(b) DEFINITIONS.—Section 3077 of such title is amended by adding at the end the following new paragraph:

"(8) 'act of espionage' means an activity that is a violation of—

"(A) section 793, 794, or 798 of title 18, United States Code; or

"(B) section 783(b) of title 50, United States Code.".

(c) CLERICAL AMENDMENTS.—The items relating to chapter 24 in the table of chapters at the beginning of such title, and in the table of chapters at the beginning of part II of such title, are each amended by adding at the end the following: "and espionage.".

SEC. 6. ESPIONAGE NOT COMMITTED IN ANY DISTRICT.

(a) IN GENERAL.—Chapter 211 of title 18, United States Code, is amended by inserting after section 3238 the following new section:

"§ 3239. Espionage and related offenses not committed in any district

"The trial for any offense involving a violation of—

"(1) section 793, 794, 798, 952, or 1030(a)(1) of this title,

"(2) section 601 of the National Security Act of 1947 (50 U.S.C. 421), or

"(3) subsection (b) or (c) of section 4 of the Subversive Activities Control Act of 1950 (50 U.S.C. 783 (b) or (c)), begun or committed upon the high seas or elsewhere out of the jurisdiction of any particular State or district,

may be in the District of Columbia or in any other district authorized by law.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 211 of such title is amended by inserting after the item relating to section 3238 the following:

"3239. Espionage and related offenses not committed in any district.".

SEC. 7. CRIMINAL FORFEITURE FOR VIOLATION OF CERTAIN ESPIONAGE LAWS.

(a) IN GENERAL.—Section 798 of title 18, United States Code, is amended by adding at the end the following new subsections:

"(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

"(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

"(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

"(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

"(A) property subject to forfeiture under this subsection;

"(B) any seizure or disposition of such property; and

"(C) any administrative or judicial proceeding in relation to such property if not inconsistent with this subsection.

"(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

"(e) As used in subsection (d) of this section, the term 'State' means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau (until such time as the Compact of Free Association is ratified), and any other possession of the United States.".

(b) AMENDMENTS FOR CONSISTENCY IN APPLICATION OF FORFEITURE UNDER TITLE 18.—(1) Section 793(h)(3) of such title is amended in the matter above subparagraph (A) by striking out "(o)" each place it appears and inserting in lieu thereof "(p)".

(2) Section 794(d)(3) of such title is amended in the matter above subparagraph (A) by striking out "(o)" each place it appears and inserting in lieu thereof "(p)".

(c) SUBVERSIVE ACTIVITIES CONTROL ACT.—Section 4 of the Subversive Activities Control Act of 1950 (50 U.S.C. 783) is amended by adding at the end the following new subsection:

"(g)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

"(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

"(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

"(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

"(A) property subject to forfeiture under this subsection;

"(B) any seizure or disposition of such property; and

"(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

"(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this sub-

section remaining after the payment of expenses for forfeiture and sale authorized by law.".

SEC. 8. DENIAL OF ANNUITIES OR RETIRED PAY TO PERSONS CONVICTED OF ESPIONAGE IN FOREIGN COURTS INVOLVING UNITED STATES INFORMATION.

Section 8312 of title 5, United States Code, is amended by adding at the end thereof the following new subsection:

"(d) For purposes of subsections (b)(1) and (c)(1), an offense within the meaning of such subsections is established if the Attorney General certifies to the agency administering the annuity or retired pay concerned—

"(1) that an individual subject to this chapter has been convicted by an impartial court of appropriate jurisdiction within a foreign country in circumstances in which the conduct violates the provisions of law enumerated in subsections (b)(1) and (c)(1), or would violate such provisions had such conduct taken place with the United States, and that such conviction is not being appealed or that final action has been taken on such appeal;

"(2) that such conviction was obtained in accordance with procedures that provided the defendant due process rights comparable to such rights provided by the United States Constitution, and such conviction was based upon evidence which would have been admissible in the courts of the United States; and

"(3) that such conviction occurred after the date of enactment of this subsection.".

SEC. 9. PROVIDING A COURT ORDER PROCESS FOR PHYSICAL SEARCHES UNDERTAKEN FOR FOREIGN INTELLIGENCE PURPOSES.

(a) AMENDMENT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by redesignating title III as title IV and section 301 as section 401, respectively;

(2) in section 401 (as redesignated) by inserting "(other than title III)" after "provisions of this Act"; and

(3) by inserting after title II the following new title:

"TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

"AUTHORIZATION OF PHYSICAL SEARCHES FOR FOREIGN INTELLIGENCE PURPOSES

"SEC. 301. (a) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the Foreign Intelligence Surveillance Court. Notwithstanding any other law, a judge of the court to whom application is made may grant an order in accordance with section 303 approving a physical search in the United States of the premises, property, information, or material of a foreign power or an agent of a foreign power for the purpose of collecting foreign intelligence information.

"(b) The Foreign Intelligence Surveillance Court shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence information anywhere within the United States under the procedures set forth in this title, except that no judge shall hear the same application which has been denied previously by another judge designated under section 103(a) of the Act. If any judge so designated denies an application for an order authorizing a physical search under this title, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established under section 103(b).

"(c) The court of review established under section 103(b) shall have jurisdiction to review the denial of any application made under this title. 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.

"(d) Judicial proceedings under this title shall be concluded as expeditiously as possible. The record of proceedings under this title, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Director of Central Intelligence.

"APPLICATION FOR AN ORDER

"SEC. 302. (a) Each application for an order approving a physical search under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this title. Each application shall include—

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

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

"(3) the identity, if known, or a description of the target of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;

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

"(A) the target of the physical search is a foreign power or an agent of a foreign power;

"(B) the premises or property to be searched contains foreign intelligence information; and

"(C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;

"(5) a statement of the proposed minimization procedures;

"(6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;

"(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 branch officers employed in the area of national security or defense and appointed by the President, by and 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 search 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 101(e); and

"(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D); and

"(8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

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

"(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 303.

"ISSUANCE OF AN ORDER

"SEC. 303. (a) Upon an application made pursuant to section 302, the judge shall enter an ex parte order as requested or as modified approving the physical search if the judge finds that—

"(1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;

"(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 physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States;

"(B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power; and

"(C) physical search of such premises or property can reasonably be expected to yield foreign intelligence information which cannot reasonably be obtained by normal investigative means;

"(4) the proposed minimization procedures meet the definition of minimization contained in this title; and

"(5) the application which has been filed contains all statements and certifications required by section 302, 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 302(a)(7)(E) and any other information furnished under section 302(c).

"(b) An order approving a physical search under this section shall—

"(1) specify—

"(A) the identity, if known, or a description of the target of the physical search;

"(B) the nature and location of each of the premises or property to be searched;

"(C) the type of information, material, or property to be seized, altered, or reproduced;

"(D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and

"(E) the period of time during which physical searches are approved; and

"(2) direct—

"(A) that the minimization procedures be followed;

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

"(C) that such landlord, custodian or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the search or the aid furnished that such person wishes to retain;

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

"(E) that the Federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.

"(c)(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a), for the period specified in the application or for one year, whichever is less.

"(2) Extensions of an order issued under this title may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a) (5) or (6), or against a foreign power, as defined in section 101(a)(4), 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 property 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 a physical search is approved by an order or an extension, or at any time after a physical search is carried out, 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.

"(d)(1) Notwithstanding any other provision of this title, whenever the Attorney General reasonably determines that—

"(A) an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an order authorizing such search can with due diligence be obtained, and

"(B) the factual basis for issuance of an order under this title to approve such a search exists,

the Attorney General may authorize the execution of an emergency physical search if—

"(i) a judge having jurisdiction under section 103 is informed by the Attorney General or the Attorney General's designee at the time of such authorization that the decision has been made to execute an emergency search, and

"(ii) an application in accordance with this title is made to that judge as soon as practicable but not more than 24 hours after the Attorney General authorizes such search.

"(2) If the Attorney General authorizes an emergency search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

"(3) In the absence of a judicial order approving such a physical search, the search shall terminate the earlier of—

"(A) the date on which the information sought is obtained;

"(B) the date on which the application for the order is denied; or

"(C) the expiration of 24 hours from the time of authorization by the Attorney General.

"(4) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the search, no information obtained or evidence derived from such search 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 search 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 301.

"(e) Applications made and orders granted under this title shall be retained for a period of at least 10 years from the date of the application.

"USE OF INFORMATION

"SEC. 304. (a) Information acquired from a physical search conducted pursuant to this title 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 title. No information acquired from a physical search pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

"(b) No information acquired pursuant to this title 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) Whenever the United States 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 a physical search of the premises or property of that aggrieved person pursuant to the authority of this title, the United States shall, prior to the trial, hearing, or the 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 United States intends to so disclose or so use such information.

"(d) 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 a physical search of the premises or property of that aggrieved person pursuant to the authority of this title, 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)(1) Any person against whom evidence obtained or derived from a physical search 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 search on the grounds that—

"(A) the information was unlawfully acquired; or

"(B) the physical search was not made in conformity with an order of authorization or approval.

"(2) 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) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), 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 a physical search authorized by this title or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this title, 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 any 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 physical search as may be necessary to determine whether the physical search 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 physical search only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

"(g) If the United States district court pursuant to subsection (f) determines that the physical search 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 the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

"(h) Orders granting motions or requests under subsection (g), decisions under this section that a physical search 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 the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

"(i) If an emergency execution of a physical search is authorized under section 303(d) and a subsequent order approving the search 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 the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of—

"(1) the fact of the application;

"(2) the period of the search; 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 90 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.

"CONGRESSIONAL OVERSIGHT

"SEC. 305. (a) On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all physical searches conducted pursuant to this title. On an annual basis the Attorney General shall also provide to those committees a report setting forth with respect to the preceding calendar year—

"(1) the total number of applications made for orders approving physical searches under this title; and

"(2) the total number of such orders either granted, modified, or denied.

"PENALTIES

"SEC. 306. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

"(1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute; or

"(2) discloses or uses information obtained under color of law by physical search within the United States, knowing or having reason to know that the information was obtained through physical search not authorized by statute, for the purpose of obtaining intelligence information.

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

"(c) PENALTY.—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) 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.

"CIVIL LIABILITY

"SEC. 307. CIVIL ACTION.—An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, of this Act, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 306 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

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

"(2) punitive damages; and

"(3) reasonable attorney's fees and other investigative and litigation costs reasonably incurred.

"AUTHORIZATION DURING TIME OF WAR

"SEC. 308. Notwithstanding any other law, the President, through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress.

"DEFINITIONS

"SEC. 309. As used in this title:

"(1) The terms 'foreign power', 'agent of a foreign power', 'international terrorism', 'sabotage', 'foreign intelligence information', 'Attorney General', 'United States person', 'United States', 'person', and 'State' shall have the same meanings as in section 101 of this Act.

"(2) 'Aggrieved person' means a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search.

"(3) 'Foreign Intelligence Surveillance Court' means the court established by section 103(a) of this Act.

"(4) 'Minimization procedures' with respect to physical search, means—

"(A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, 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;

"(B) procedures that require that non-publicly available information, which is not foreign intelligence information, as defined in section 101(e)(1) of this Act, 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 such foreign intelligence information or assess its importance; and

"(C) notwithstanding subparagraphs (A) and (B), 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.

"(5) 'Physical search' means any physical intrusion into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforce-

ment purposes, but does not include 'electronic surveillance', as defined in section 101(f) of this Act.".

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended by striking the items relating to title III and inserting the following:

"TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

"Sec. 301. Authorization of physical searches for foreign intelligence purposes.
"Sec. 302. Application for an order.
"Sec. 303. Issuance of an order.
"Sec. 304. Use of information.
"Sec. 305. Congressional oversight.
"Sec. 306. Penalties.
"Sec. 307. Civil liability.
"Sec. 308. Authorization during time of war.
"Sec. 309. Definitions.

"TITLE IV—EFFECTIVE DATE

"Sec. 401. Effective Date.".

(c) EFFECTIVE DATE.—The amendments made by subsections (a) and (b) shall take effect 90 days after the date of enactment of this Act, except that any physical search approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of title III of the Foreign Intelligence Surveillance Act of 1978 (as added by this Act), if that search is conducted within 180 days after the date of enactment of this Act pursuant to regulations issued by the Attorney General, which were in the possession of the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives before the date of enactment of this Act.

SEC. 10. LESSER CRIMINAL OFFENSE FOR UNAUTHORIZED REMOVAL OF CLASSIFIED DOCUMENTS.

(a) IN GENERAL.—Chapter 93 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 1924. Unauthorized removal and retention of classified documents or material

"(a) IN GENERAL.—Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than 1 year, or both.

"(b) DEFINITION.—In this section, the term 'classified information of the United States' means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following:

"1924. Unauthorized removal and retention of classified documents or material.".

BACKGROUND OF THE LEGISLATION

Prior actions of the committee

Since its creation in 1976, the Select Committee on Intelligence (SSCI) has made the problem of espionage a focus of its interest. Both through its annual actions on the foreign counterintelligence budgets of the CIA, the FBI, and the DOD, and in legislation, the Committee has attempted to strengthen the ability of the Government to deal with this seemingly intractable problem.

The Committee was instrumental in the development and passage of the Foreign Intelligence Surveillance Act of 1978 which established a new court to hear applications and grant orders authorizing electronic surveillances for foreign intelligence and counter-

intelligence purposes. Not only did this legislation provide protection to the civil liberties of those involved—subjecting such activities to court review—it also provided clear statutory authority for the Government to engage in such activity, thereby enhancing its use for counterintelligence purposes.

In 1978, the Committee also authorized the FBI to undertake certain undercover operations as part of its counterintelligence efforts.

In 1979, the Committee began to require reports from the Executive branch with respect to foreign nationals who were admitted into the United States over the objections of counterintelligence agencies who were concerned that such persons posed counterintelligence threats.

In 1982, the Committee took a leading role in the development of the Foreign Missions Act, establishing the Office of Foreign Missions at the Department of State, to regulate the activities of foreign missions within the United States consistent with the controls and limitations placed upon U.S. missions abroad.

In 1984, the Committee began requiring reports from the Executive branch with respect to the numbers, privileges, immunities, and travel restrictions of diplomatic personnel within the United States whose countries were known to be engaged in intelligence activities against the United States.

1985 witnessed numerous spy cases including the Walker-Whitworth spy ring, Jonathan Pollard, Ronald Pelton, and Edward Lee Howard. After these cases were made public, formal agreements between the CIA and the FBI were concluded, ostensibly to improve cooperation between the two agencies on CI and security matters.

In 1986, in the wake of the "Year of the Spy," the Committee issued a voluminous report entitled "Meeting the Espionage Challenge" (S. Rept. 99–522, 99th Cong. 2d Sess.), which was a comprehensive review of all U.S. counterintelligence and security programs. In all, the report contained 95 recommendations for action by the Congress and the Executive branch to improve the U.S. counterintelligence and security posture. Concurrent with the preparation of the Committee's 1986 report, Congress directed the President to undertake an Executive branch review of the same area, which resulted in an extensive classified report to the Committee which detailed the President's views on dealing with the espionage problem and on the Committee's recommendations.

In the same year, in its action on the FY 1987 Intelligence Authorization bill, the Committee provided authority to the FBI to obtain copies of financial records of persons suspected of being agents of foreign powers. During the same year, the Committee was instrumental in development of additional legislation authorizing the FBI to obtain telephone toll records of persons suspected of being agents of foreign powers based upon the certification of the Director.

In 1987, the Committee, in its action on the 1988 Intelligence Authorization bill, established a policy of substantial equivalence in terms of the numbers of Soviet diplomats allowed in the United States and the number of U.S. diplomats permitted in the Soviet

Union, and required reports of changes in the established personnel levels.

In late 1989, at the request of the Committee leadership, a panel of unpaid consultants was assembled by businessman Eli Jacobs to examine the desirability of further statutory changes to improve the ability of government to cope with espionage. Consisting of Admiral Bobby R. Inman, former Director of the National Security Agency and Deputy Director of Central Intelligence; Lloyd Cutler, Counsel to President Carter; A.B. Culvahouse, Counsel to President Reagan; Warren Christopher, former UnderSecretary of State and Deputy Attorney General; Sol Linowitz, former Ambassador to the Organization of American States; Richard Helms, former Director of Central Intelligence and Ambassador to Iran; Seymour Weiss, former Ambassador and currently Chairman of the Defense Policy Board; and Harold Edgar, professor of law at Columbia University and a recognized authority on espionage laws, the panel produced a lengthy report recommending thirteen statutory changes, to include:

Uniform security requirements for everyone with access to TOP SECRET information. These requirements included obtaining an employee's consent permitting the government access to their financial, credit, and travel records while the TOP SECRET clearance was in effect and for 5 years thereafter;

An amendment to the Right to Financial Privacy Act to permit employees with TOP SECRET clearances to consent to having the Government gain access to their financial records (i.e., primarily bank account records). Under existing law, such consent could only be provided every three months and was revocable by the employee;

All government employees with routine access to codes and coding/decoding equipment be subject to a polygraph examination limited to counterintelligence questions;

The NSA Director have authority to provide assistance to problem employees who were terminated from their jobs to preclude a security problem from developing;

A new federal criminal offense for the mere possession of "espionage devices" whether or not the government could prove the passage of classified information to a foreign agent;

A new federal criminal offense for any government employee who sold material marked as TOP SECRET to a foreign government without the Government having to prove in court that the material was properly classified as TOP SECRET;

A new misdemeanor offense for anyone who removed TOP SECRET documents to an unauthorized location (regardless of whether they were also disclosed to an unauthorized person);

Extension of the "Son of Sam" statute providing for the forfeiture of profits derived from certain crimes to several espionage statutes not otherwise included in the existing statute;

Amendment of the federal retirement statute to deny annuities or retired pay to U.S. employees who had been convicted of espionage involving U.S. information in foreign courts;

New authority for the FBI to obtain consumer credit reports in counterintelligence investigations;

The FBI be granted authority to obtain certain telephone subscriber information in counterintelligence cases;

Providing authority to the Attorney General to provide rewards for information leading to espionage arrests; and

Amendment of the Foreign Intelligence Surveillance Act (FISA) to require court orders for physical searches for intelligence purposes.

The Jacobs panel presented their recommendations to the Committee in a public hearing on May 23, 1990. On June 13, 1990, Senators Boren and Cohen introduced a bill, S. 2726, incorporating the recommendations made by the Jacobs panel without substantive change.

On July 12, 1990, the Committee held a public hearing on S. 2726, receiving testimony from Administration witnesses, the ACLU, and private witnesses. On the basis of the hearing and ensuing consultations with the Executive branch, a revised bill was prepared and introduced by Senators Boren and Cohen on October 26, 1990 as S. 3251. The bill, however, was not reported out of Committee prior to the *sine die* adjournment of the 101st Congress.

The Boren-Cohen bill was reintroduced with amendments in January, 1991 as S. 394, but again was not reported out by the Committee.

Two of the Jacobs panel recommendations were subsequently enacted in modified form in later legislation. The recommendation pertaining to the NSA Director's authority to provide after-employment assistance was enacted as part of the Intelligence Authorization Act for Fiscal Year 1990, and the recommendation pertaining to the FBI's access to certain telephone subscriber information was enacted as separate legislation in 1993.

There was no further consideration of the remaining recommendations until 1994.

The Ames case: 1994

On February 21, 1994, agents from the FBI's Washington Metropolitan Field Office (WMFO) arrested CIA employee Aldrich Hazen ("Rick") Ames and his wife Maria Del Rosario Casas Ames on charges of having committed espionage, first for the Soviet Union beginning in 1985, and later for Russia, continuing until the time of their arrest. It was clear, given Ames's 31-year career in the Directorate of Operations and the highly sensitive information to which he had access during this period, that this case was an extremely serious breach of security, perhaps the most serious ever experienced by the CIA.

At the time of the Ameses' arrest, it was reported that Ames had paid $540,000 in cash for his home in Arlington, Virginia, in 1989, and that he drove a new Jaguar automobile, apparently without arousing suspicion.

On February 23, 1994, SSCI Chairman DeConcini and Vice Chairman Warner sent a letter to the CIA Inspector General expressing concern with the apparent security deficiencies at the CIA and noting that while "* * * we recognize the need to refrain from investigative actions which would complicate or interfere with the ongoing criminal investigation, we strongly believe that an Inspec-

tor General inquiry is needed to address these concerns." Such an inquiry was instituted several days later.

In the weeks that followed, the Committee held a series of closed hearings to determine how Ames had been able to avoid detection for such a long period. While the Committee refrained from calling witnesses who might be called during the criminal trial and otherwise sought to avoid testimony on topics which might become issues of proof at trial, it explored the effectiveness of CIA security policies and procedures, examined the conduct of the counterintelligence investigation which eventually identified Ames,s and conducted a review of Ames's polygraph examinations.

On April 28, 1994, Aldrich Ames and his wife Rosario pled guilty to charges of conspiracy to commit espionage and tax fraud. At the time the pleas were entered, a "Statement of Facts," agreed to by Ames, was filed with the court which among other things acknowledged that Ames had begun spying for the Soviet Union in April, 1985, and that he had since been paid over $2.5 million.

The indictment filed the same day charged that since 1985 Ames had provided to the KGB information about CIA's operations in the Soviet Union, including the names of human sources in the Soviet Union who were secretly cooperating with the CIA. (Virtually all of these individuals were reportedly executed or incarcerated.) He also provided the names of "double agents" under the control of U.S. intelligence, whom the Soviet Union had believed they were controlling. In addition, Ames provided a substantial amount of information regarding the CIA and other intelligence agencies, including information regarding their budgets, personnel, strategy, and organization. Specific evidence was also developed showing that Ames had passed 10 TOP SECRET documents, including one which related to U.S. capabilities to detect Russian nuclear submarines.

Ames was sentenced to life imprisonment without parole, to undergo extensive debriefings about his espionage activities, and to forfeit all his proceeds of espionage (e.g., foreign and domestic bank accounts, his home in Arlington, Virginia, automobiles and pension). The plea agreement also requires him to assign to the United States the proceeds of any book, movie, or interview contract he might sign. The agreement also provides that the Government may seek release from its obligations under the plea agreement with Ames or his wife if Ames does not fulfill his obligations under the plea agreement, primarily by cooperating in the debriefings.

Rosario Ames is scheduled to be sentenced on August 26 of this year. But the Government and her attorneys agreed to recommend to the court that she be sentenced to between 63 months and 72 months in prison without parole. She also agreed to a complete debriefing, complete forfeiture of assets and assignment of proceeds, like her husband.

The Committee's inquiry into the Ames case is far from complete. Additional hearings are contemplated, and the results of the CIA Inspector General investigation must be considered and evaluated. The results of the Government's debriefings of the Ameses must also be taken into account. It is the intention of the Committee to issue a comprehensive public report on its inquiry before the end of the 103rd Congress.

Action in the 103rd Congress

The Ames case served as a considerable impetus for new legislation. Six bills to improve the counterintelligence posture of the United States were introduced in the Senate alone following the arrest of the Ameses: S. 1866 by Senator Metzenbaum; S. 1869 by Senators Cohen and Boren; S. 1890 by Senator Heflin; S. 1948 by Senators DeConcini and Warner; S. 2056 by Senators DeConcini and Warner (at the request of the Administration); and S. 2063 by Senator Gorton. All of these bills were the subject of a public hearing held by the Committee on May 3, 1994.

Testifying were former SSCI Chairman and Vice Chairman, Senators Boren and Cohen; Deputy Attorney General Jamie Gorelick; Director of Central Intelligence R. James Woolsey; Director of the Federal Bureau of Investigation, Louis J. Freeh; Robert Kohler, Vice President, TRW Aeronautics and Space Surveillance Group; Kate Martin, Director for National Security Studies, American Civil Liberties Union; and David Whipple, Executive Director, Association for Former Intelligence Officers.

Following the public hearing on May 3rd, the Committee held a series of discussions with representatives of the Administration involving possible amendments to the Administration proposal. Agreement in principle was reached on several amendments, which were offered and approved at the Committee's markup on May 24, 1994. Two additional amendments offered by members of the Committee were also approved. The bill, as amended, is explained in what follows.

RATIONALE FOR S. 2056, AS AMENDED

General

S. 2056, as amended by the Committee, contains nine separate substantive provisions, which fall generally into three categories: strengthening security requirements for government employees with access to classified information; improvements with respect to the conduct of counterintelligence investigations; and improvements in the laws pertaining to the prosecution of espionage. The background and rationale for each selection are explained below.

In general, the Committee sought to identify measures that would have practical utility with respect to deterring, detecting, and prosecuting espionage but would not constitute unreasonable intrusions into the privacy of the American people, including federal employees. In making its assessment, the Committee considered and ultimately rejected several proposals pending before the Committee on the grounds that their perceived value for counterintelligence purposes was seen as insufficient to overcome the civil liberties concerns which had been raised with the Committee.

Although the bill does contemplate new requirements on federal employees with access to classified information to provide access to certain personal data, the Committee believes that such persons should be prepared to yield a measure of their personal privacy to the Government. After all, the Government is entrusting them with information whose disclosure could have serious repercussions for the United States and for persons who cooperate with the United States.

The Committee does not anticipate that the enactment of S. 2056, as amended, will spell the end of espionage. Espionage has posed a threat to the United States since the early days of the Republic, and no law is apt to change this. The Committee does believe, however, that the enactment of S. 2056 will significantly assist the Government in coping with this intractable problem by providing greater deterrence to those who might contemplate betraying their country, by improving the government's ability to detect such activity once it occurs, and by facilitating the prosecution of such conduct and punishing it appropriately once detected.

The United States should have in place an optimal statutory framework to deal with this problem. If there are improvements that can be made consistent with the rights and values shared by all Americans, Congress should enact them. S. 2056, as amended, provides such an opportunity.

Section 2: Access to classified information

Section 2 of the bill requires that the President within 180 days of enactment issue regulations to govern access to classified information binding upon all elements of the Executive branch.

There is currently no law or Executive order which establishes minimum uniform requirements for the federal government as a whole. The Director of Central Intelligence is charged by law with the protection of intelligence sources and methods, and, pursuant to this authority, establishes government-wide standards for access to Sensitive Compartmented Information (i.e. information revealing intelligence sources or methods). But requirements for ordinary security clearances and background investigations, as well as the standards and procedures for granting such clearances, are left largely to departmental and agency regulation. In practice, they vary substantially.

These disparities were explored at length in extensive hearings before the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee held in 1985 (see Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, "Federal Government Security Clearance Programs", 99th Cong., 1st Sess.), which resulted in the subcommittee recommending that the President issue an Executive order which would establish uniform policy in this area for the Executive branch as a whole.

This Committee, after an extensive review of federal personnel security programs in its 1986 report on "Meeting the Espionage Challenge," reached the same conclusion.

Indeed, both the Reagan and Bush Administrations attempted to develop uniform policy governing access to classified information. Due largely to bureaucratic concerns for preserving agency prerogatives, however, these efforts failed to produce the desired policy.

Meanwhile, the absence of uniform minimum requirements for access to classified information remains a problem. Security clearances are awarded on the basis of investigative requirements and adjudicative standards that can differ from agency to agency. Similarly, persons who are denied clearances by one agency may be entitled to certain due process rights which they would not be entitled to at other agencies.

What is required of persons as a condition of access to classified information itself needs thorough review. It appears to the Committee that much of the government's investigative effort is spent gathering information with little or no consequence to national security concerns, while information which potentially could be the most helpful in identifying security problems is not collected. For example, relatively little information of a financial nature, or information regarding foreign travel, which may be the most likely to provide an indication of espionage or the vulnerability to espionage, is now required of cleared federal employees in any agency.

The Committee was sensitive to the concerns expressed by the Executive with regard to legislating such requirements. Given the need to allow for the needs of various departments and agencies, and the need to leave sufficient flexibility in the administration of the personnel security system, the Committee opted to require the President to issue procedures which address the principal shortcomings perceived with the current system, rather than legislating such requirements.

In addition to mandating Executive regulations governing access to classified information, section 2 of the bill also provides procedures to govern requests by authorized investigative agencies of the federal government to request certain financial and travel records of cleared federal employees who have previously provided written consent to the government permitting such access.

In general, the bill provides specific criteria under which access may be sought and requires a written determination of a senior official of the employing agency certifying that the requirements of the statute have been met.

Once the request is made, the recipient of the request—whether a governmental or private entity—is prohibited from disclosing that such a request was made to other persons.

This provision is needed in order to obtain the cooperation of the private institutions involved as well as to preclude them from divulging such information to others (including the subject of the request). It is also needed because, in some cases, the government's access to such records (even based upon consent of the subject) is restricted by other laws. For example, under the Right to Financial Privacy Act of 1978, a government agency may obtain access to bank accounts, credit card accounts, mortgage accounts, etc., based the consent of the individual concerned, but the Act limits the period for which such consent may be provided to a period of 90 days and such consent may be revoked.

The Committee believes that the requirement for written consent, the criteria governing requests for access, and the certification required of a senior official of the employing agency constitute adequate safeguards against misuse of this authority.

Section 3: Coordination of counterintelligence activities

Section 3 of the bill establishes a national-level mechanism for the development of policy and resolution of conflicts involving U.S. counterintelligence activities and establishes procedures to ensure that such activities are appropriately coordinated by affected departments and agencies with the Federal Bureau of Investigation.

In the course of the Committee's review of the Ames investigation, it became apparent that there were serious shortcomings in the existing framework and coordination process.

The existing bureaucratic mechanisms for resolving problems between agencies—the Advisory Group for Counterintelligence (AG/CI)—was organizationally placed under the Director of Central Intelligence, who was often not in a position to act as disinterested arbiter, and was too large a mechanism to discuss extremely sensitive cases. Thus, where conflict resolution was concerned, the AG/CI was not structured to function effectively.

The Committee also found that counterintelligence matters had often not been effectively coordinated between the CIA and the FBI, which has the principal responsibility under Executive Order 12333 for counterintelligence activities undertaken within the United States, and, pursuant to section 603 of the Intelligence Authorization Act for Fiscal Year 1990, for espionage investigations undertaken at U.S. diplomatic establishments abroad. Conversely, the Committee found indications that the FBI had not always coordinated counterintelligence activities undertaken abroad with the Central Intelligence Agency, as required by Executive Order 12333.

The failure to coordinate such matters effectively has in some cases resulted in the inability of the Government to prosecute possible criminal violations; or in considerable delay in the investigation and arrest of subsequently-convicted spies; and in some cases appears to have harmed the relationship of U.S. agencies with foreign liaison services.

Moreover, the Committee found that the coordination problems between the CIA and the FBI evident in the recent past are, in fact, longstanding problems which have proven immutable of solution by the Executive branch.

In October, 1986, the Committee issued a report entitled "Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs," which, among other things, highlighted the need, in the wake of the Howard and Pollard cases, in particular, for improving coordination with the FBI:

> In the Edward Lee Howard case, CIA security officials failed to alert and involve the FBI in a timely fashion. The CIA has taken steps recently to guard against a recurrence of this problem. The FBI should continue to work closely with security officials of all FBI Government agencies to ensure they understand its requirements and guidelines. * * * The lessons of the Howard and Pollard cases should be extended to all departments and agencies that handle highly sensitive information. Interagency procedures for reporting suspicious conduct to the FBI should be strengthened. * * * The decision as to whether the circumstances justify investigation in varying degrees should be made by the FBI, in light of its counterintelligence experience, not by the employing agency.

In 1988, responding to the express direction of President Reagan to "fix" the coordination problems evident in the Howard case, the FBI and CIA negotiated a new Memorandum of Understanding to govern the CIA's reporting of counterintelligence information to the

FBI. Although the text of the memorandum remains classified, the Committee finds the criteria for reporting counterintelligence matters to the FBI reasonably clear. They appear broad and encompassing.

Yet, despite this agreement—which remains in force today—coordination difficulties have continued. In the Ames case, it was not until 1991, five years after the CIA realized that it had a serious and unresolved security problem, that it formed a joint task force with the FBI to deal with it. Relevant information bearing upon Ames in particular appears not to have been turned over to the FBI until considerably later.

Given the lack of success of previous non-legislative attempts to minimize or eliminate those problems, a provision (section 807) was added to S. 1948, introduced by Senators DeConcini and Warner, which gave the FBI "overall responsibility for the conduct of counterintelligence and law enforcement investigations" involving persons in particularly sensitive positions, as explained elsewhere in the bill.

At the public hearing held by the Committee on May 3, 1994, Administration witnesses objected strenuously to the proposed language. While both the Director of Central Intelligence and the Director of the FBI conceded that coordination between the two agencies has been and remained "a problem," they objected to the language as giving the FBI Director too much control in the counterintelligence area to the detriment of other interests, principally the DCI's foreign intelligence-gathering function.

The Administration witnesses instead urged the Committee to rely upon a new bureaucratic arrangement, approved by President Clinton the morning of the public hearing as Presidential Decision Directive (PDD) 24, to ensure that appropriate coordination took place. Under the PDD—

> A National Counterintelligence Policy Board was established to report to the President through the Assistant to the President for National Security Affairs. The Board would be chaired alternately for two-year periods by representatives of the CIA, FBI, and Department of Defense, as designated by the Director of Central Intelligence. The Board would be principally responsible for developing policy recommendations for the President and resolving conflicts between agencies;
>
> The existing DCI Counterintelligence Center was split into two parts: one part would become the National Counterintelligence Center, to serve as the interagency forum for national-level CI activities, e.g., threat assessments or security evaluations of diplomatic establishments; and the other would become the CIA Counterintelligence Center, responsible for providing counterintelligence support to the CIA and to execute the CIA Director's responsibilities for coordinating counterintelligence activities outside the United States; and, finally,
>
> The Chief of the Counterespionage Group within the CIA Counterintelligence Center would be permanently staffed by a senior FBI official; and, conversely, CIA counterintelligence officers would be assigned to FBI headquarters and field elements involved in counterintelligence work.

It was this latter arrangement—making a senior FBI official chief of the CIA's counterespionage group—which Administration witnesses told the oversight committees was key to resolving the coordination problem:

DIRECTOR OF CENTRAL INTELLIGENCE WOOLSEY

> The key thing from the point of view of the hand-off [coordination with the FBI] is that the Chief in the Center of the CIA that does counterespionage will be permanently staffed * * * by a senior executive from the FBI * * *. [The counterespionage group] is the focal point within the CIA for managing research and investigation of all counterintelligence leads. This is where all leads come to, whether they come from our own espionage overseas, or from defectors, or from liaison work with foreign intelligence services, or from technical operations, or from volunteers * * *. [W]hether it is from a polygraph of a CIA employee, a foreign intelligence agent's report about what may be known in some foreign country that could have come from a leak in our own government—as soon as it appears to have any counterespionage implications, I can't conceive of any lead like that that does not come to the counterespionage group.

[Before the SSCI, 5/3/94]

DEPUTY ATTORNEY GENERAL GORELICK

> What that [the FBI official heading the counterespionage group at CIA] means is that all leads, all evidence that comes into the CIA for investigation will be directed to, handled by, a group headed by the FBI * * *. The purpose here is to move the FBI into a position where it can follow up on all leads, all relevant leads.

[Before the House Permanent Select Committee on Intelligence, 5/4/94]

The Committee believes these new bureaucratic arrangements should, as a practical matter, help to resolve the coordination problem which has long existed between the two agencies. At the same time, the Committee believes, given the failure of previous efforts by the Executive branch to cope with the problem, that legislation to complement the Administration's initiatives is necessary and desirable.

Accordingly, in its action on S. 2056, the Administration bill, the Committee added a new section 3 which deals with the coordination of counterintelligence activities.

This section would create a new National Counterintelligence Policy Board, chaired by the Attorney General, to provide a focus for the development of policy in the counterintelligence area and to resolve disputes between agencies. While the Board is similar to that recently created by presidential directive, the Committee believes that the two-year rotational chairmanship of the board created under the directive would necessarily limit its effectiveness. The Committee also believes that a permanent chair would provide

better leadership and continuity, and that, in view of the Attorney General's responsibility for the enforcement of espionage and criminal statutes and for the largest and predominant counterintelligence agency—the FBI—that this cabinet officer is best positioned to bear this responsibility. The Committee expects the Attorney General, in performing this function, to take a broader view than that of any one investigative agency, including the FBI.

Section 3 also would establish a clear policy to ensure that departments and agencies within the Executive branch advise the FBI immediately when information indicating a counterintelligence problem comes to their attention, and consult with the FBI with respect to follow-on actions. In the view of the Committee, this mandate is entirely consistent with what Administration witnesses have testified are the objectives of the new bureaucratic arrangements. With continuing oversight by the intelligence committees, the Committee believes combining the Administration's new counterintelligence structure with the statutory mandate contained in section 3 offers the best chance to resolve this intractable problem.

In mandating coordination with the FBI, the intent of the Committee is not to suggest that the investigative interest in these situations will always predominate. That will depend upon the particular circumstances involved. The intent of section 3 is to ensure that departments and agencies do not unilaterally take actions, in the interests of preserving the identity of a source or in the interests of limiting damage to their own operations, which would delay, hamper, or preclude a potential criminal prosecution.

Section 4: Disclosure of consumer credit reports for counterintelligence purposes

Section 4 would amend section 608 of the Fair Credit Reporting Act (15 U.S.C. 1681f) to grant the Federal Bureau of Investigation (FBI) access to consumer credit records in counterintelligence investigations.

This provision would provide a limited expansion of the FBI's authority in counterintelligence investigations (including terrorism investigations) to use a "National Security Letter," i.e., a written certification by the FBI Director or the Deputy Director, to obtain information without a court order. FBI presently has authority to use the National Security Letter mechanism to obtain two types of records: financial institution records (under the Right to Financial Privacy Act, 12 U.S.C. 3414(a)(5)); and telephone subscriber and toll billing information (under the Electronic Communications Privacy Act, 18 U.S.C. 2709). Expansion of this extraordinary authority is not taken lightly by the Committee, but the Committee has concluded that in this instance the need is genuine, the threshold for use is sufficiently rigorous, and, given the safeguards built in to the legislation, the threat to privacy is minimized.

Under the provision of the Right to Financial Privacy Act (RFPA) cited above, the FBI is entitled to obtain financial records from financial institutions, such as banks and credit card companies, by means of a National Security Letter when the Director or the Director's designee certifies in writing to the financial institution that such records are sought for foreign counterintelligence purposes and that there are specific and articulable facts giving reason to be-

lieve that the customer or entity whose records are sought is a foreign power or an agent of a foreign power, as those terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

The FBI considers such access to financial records crucial to trace the activities of suspected spies or terrorists. The need to follow financial dealings in counterintelligence investigations has grown as foreign intelligence services increasingly operate under non-official cover, i.e., pose as business entities or executives, and as foreign intelligence service activity has relied increasingly upon economic incentives to U.S. agents.

The FBI's right of access under the Right to Financial Privacy Act cannot be effectively used, however, until the FBI discovers which financial institutions are being utilized by the subject of a counterintelligence investigation. Consumer reports maintained by credit bureaus are a ready source of such information, but, although such reports are readily available to the private sector, they are not available to FBI counterintelligence investigators. Under the existing section 608 of the Fair Credit Reporting Act (FCRA), without a court order, FBI counterintelligence officials, like other government agencies, are entitled to obtain only limited information from credit reporting agencies—the name, address, former addresses, places of employment, and former places of employment of a person—and this information can be obtained only with the consent of the credit bureau.

When appropriate legal standards are met, the FBI is able to obtain broader and mandatory access to credit records by means of a court order or grand jury subpoena (see the FCRA, 15 U.S.C. 1681b(1)), but such an option is available to the FBI only after a counterintelligence investigation has been formally converted to a criminal investigation or proceeding. Many counterintelligence investigations never reach the criminal stage but proceed for intelligence purposes or are handled in diplomatic channels.

The FBI has made a specific showing to the Committee that the effort to identify financial institutions in order to make use of FBI authority under the Right to Financial Privacy Act can not only be time-consuming and resource-intensive, but can also require the use of investigative techniques—such as physical and electronic surveillance, review of mail covers, and canvassing of all banks in an area—that would appear to be more intrusive than the review of credit reports. The FBI has offered a number of specific examples in which lengthy, intensive and intrusive surveillance activity was required to identify financial institutions doing business with a suspected spy or terrorist.

FBI officials have informed the Committee that the FBI's only interest in the credit reports is to identify relevant financial institutions so that it may make use of its authority under the Right to Financial Privacy Act. The provision adopted by the Committee is intended to limit FBI access and use of its authority to that access and use required to fulfill this interest. This should alleviate any concern that the FBI might rely upon inaccurate information in a credit report regarding a person's financial status.

Section 5: Rewards for information concerning espionage

Existing law (18 U.S.C. 3071 et seq.) permits the Attorney General to pay rewards of up to $500,000 for information leading to the arrest or conviction of persons who commit acts of terrorism against the United States, or for information which enables the Government to frustrate such acts. Government officials are not eligible for such rewards, and provision is made for the identity of recipients to be kept confidential if they wish.

The Committee believes that this discretionary authority should be extended to the area of espionage, to grant the Attorney General similar authority to pay rewards. The family members, former spouses, or associates of those engaged in espionage are frequently the first to become aware of, or to suspect, such activities. Such persons may be more apt to come forward if the Government is in a position to pay rewards for such information and if such persons can be guaranteed anonymity. Given the extraordinary costs to the Government of serious espionage cases, the Committee believes that providing discretion to the Attorney General to pay rewards up to $500,000 for information leading to espionage arrests is justified.

Section 6. Espionage not committed in any district

Section 6 would give the U.S. District Court for the District of Columbia and other federal district courts authorized by law jurisdiction over trials of offenses involving violations of U.S. espionage statutes and related statutes where the alleged misconduct took place outside the United States.

According to Justice Department representatives, the lack of such jurisdiction in U.S. courts has posed, from time to time, a substantial problem in terms of trying U.S. citizens in U.S. courts even through their conduct allegedly violated U.S. law, e.g., passing classified U.S. information to a foreign agent. This has led to prosecutions in foreign courts even though the United States had the predominant interest in prosecution. Section 6 is intended to provide an alternative in such circumstances.

Section 7: Criminal forfeiture for violation of certain espionage laws

Section 7 expands the criminal forfeiture provisions of 18 U.S.C. 794 to allow a court, where it can be demonstrated that a person convicted of espionage has deliberately removed the proceeds of his espionage activities beyond the reach of the court, to subject other property of the defendant, where available, to such forfeiture. This provision is identical to subsection 413(p) of the Comprehensive Drug Abuse Prevention and Control Act of 1970, as it applies to the proceeds of narcotics trafficking.

Section 7 also adds the criminal forfeiture provisions, as amended, to two additional espionage statutes: 18 U.S.C. 798, which applies to disclosures of communications intelligence, and 50 U.S.C. 783, which prohibits government employees from making unauthorized disclosures of classified information to representatives of foreign governments.

Section 8: Denial of annuities or retired pay to persons convicted in foreign courts of espionage involving United States information

Current law (5 U.S.C. 8312) provides that an annuity or retired pay may be denied on the basis of a conviction in U.S. civil or military courts for a wide range of offenses involving espionage. However, there is no provision in existing law which would permit the U.S. Government to deny retirement benefits to U.S. retirees convicted in foreign courts for espionage involving the communication of U.S. information to a foreign government.

There have been several cases in the recent past involving foreign convictions of U.S. military retirees for espionage involving United States classified information. Given the fact that many if not most espionage cases involve conduct which takes place outside the United States, prosecution in foreign courts is not an uncommon result. In at least one of these cases, the U.S. Government was obliged to provide retirement pay to a retired civilian employee who had been sentenced to prison in a foreign country for espionage involving U.S. information, because the law provided no basis for denying such pay in these circumstances. The Committee believes that foreign convictions for espionage involving U.S. information which are obtained in courts of competent jurisdiction, which provide due process and other procedural guarantees comparable to those in U.S. courts, should provide a basis for the Attorney General to deny annuities or retired pay to such persons.

Section 9. Providing a court order process for physical searches undertaken for foreign intelligence purposes

Section 9 would amend the Foreign Intelligence Surveillance Act of 1978, which established a court order procedure to govern electronic surveillances conducted in the United States for foreign intelligence purposes, to add a new title establishing similar but separate procedures for physical searches for intelligence purposes (hereinafter referred to as "intelligence searches"). To understand the need for this legislation it is necessary to review the U.S. Government's experience with intelligence searches.

The historical background

The policy and practice of the U.S. Government for conducting intelligence searches within the United States has had an unusual history. The Supreme Court has never directly addressed the issue—indeed, few cases have reached the federal courts—and the position of the Executive branch with respect to such searches has fluctuated over time. The basic issues are similar to those relating to electronic surveillance for "national security" purposes, which Congress addressed in the Foreign Intelligence Surveillance Act of 1978. These issues involve the competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the Nation and the constitutional protections for personal privacy in the Fourth Amendment. Intelligence searches, however, raise different concerns than electronic surveillance because the Fourth Amendment was so clearly understood from the earliest days of the Nation to require judicial warrants for searches of private homes.

The practices of U.S. intelligence agencies for conducting warrantless physical searches within the United States remained secret until the Watergate-related disclosures in the 1970s. By contrast, the Executive branch publicly acknowledged in the 1950s and 1960s that electronic surveillance was conducted for "national security" purposes. The policy of the Department of Justice for electronic surveillance was stated publicly in 1966 by the Solicitor General in a supplemental brief to the Supreme Court in *Black* v. *United States*, 385 U.S. 26 (1966). Pursuant to directives from Presidents Roosevelt and Truman, interception of wire communications had been "limited to matters involving national security or danger to human life" and had "required the specific authorization of the Attorney General in each instance." Pursuant to a directive from President Johnson in 1965, the requirement for specific authorization of the Attorney General had been extended to the installation and use of "listening devices," and the authority was confined to "the collection of intelligence affecting the national security." (See H. Rept. 95–1283, p. 17.) Nothing was said publicly by the Executive branch in this period with regard to warrantless physical searches for intelligence purposes.

The Supreme Court considered the issue of electronic surveillance for "national security" purposes in two leading cases in 1967 and 1972. The Court held in *Katz* v. *United States*, 389 U.S. 347 (1967), that the Fourth Amendment applied to electronic surveillance, but explicitly declined to extend its holding that the Fourth Amendment required a warrant for electronic surveillance to cases "involving the national security" (389 U.S., at 358, n. 23). The Supreme Court subsequently narrowed the scope of any "national security" exception to the warrant requirement for electronic surveillance in *United States* v. *United States District Court* (the "Keith case"), 407 U.S. 297 (1972). The Court rejected the claim of Presidential power to authorize warrantless electronic surveillance in "internal security matters." However, the Court emphasized that "this case involved only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to "activities of foreign powers or their agents" (407 U.S., at 321–322).

After the Keith case, lower federal courts generally upheld the legality of electronic surveillance of foreign powers and foreign agents. The fifth circuit in *United States* v. *Brown,* 484 F.2d 418 (5th Cir. 1973), *cert. denied,* 415 U.S. 960 (1974) upheld the legality of a surveillance in which the defendant, an American citizen, was overheard as a result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. In *United States* v. *Butenko,* 494 F.2d 593 (3rd Cir. 1974) (en banc), *cert. denied sub. nom. Ivanov* v. *United States,* 419 U.S. 881 (1974), the third circuit similarly held that electronic surveillance conducted without a warrant would be lawful so long as the primary purpose was to obtain foreign intelligence information.

The FBI's warrantless intelligence search practices first came to light in 1973, when the Watergate investigation uncovered a proposal approved and then withdrawn by President Nixon in 1970, directing the FBI to conduct "surreptitious entries" for both domestic security and foreign intelligence purposes. The so-called

"Huston Plan" reflected dissatisfaction with FBI Director J. Edgar Hoover's apparent decision to discontinue long-standing FBI "surreptitious entry" practices in 1965–66, after President Johnson's directive on electronic surveillance was issued. The proposal that reached President Nixon in 1970 described "surreptitious entry" practices as "clearly illegal," and President Nixon withdrew his approval upon the advice of Attorney General John Mitchell, who had not been consulted in the development of the plan. FBI Director Hoover advised Mitchell that the FBI would resume "surreptitious entries" only with the Attorney General's specific authorization in each case (S. Rept. No. 94–755, Book III, pp. 921–986).

More information about the FBI's intelligence search practices was disclosed during the congressional investigations of U.S. intelligence activities in 1975–76. An internal FBI memorandum from 1966 discussed the policy as follows:

> We do not obtain authorization for 'black bag' jobs from outside the Bureau. Such a technique involves trespassing and is clearly illegal; therefore, it would be impossible to obtain any legal sanction for it. Despite this, 'black bag' jobs have been used because they represent an invaluable technique in combating subversive activities of a clandestine nature aimed directly at undermining and destroying our nation.

The FBI also provided to Congress the following description of the procedure for authorization of "surreptitious entries" that were conducted before 1966:

> When a Special Agent in Charge (SAC) of a field office considered surreptitious entry necessary to the conduct of an investigation, he would make his request to the appropriate Assistant Director at FBIHQ, justifying the need for an entry and assuring it could be accomplished safely with full security. In accordance with instructions of Director J. Edgar Hoover, a memorandum was written outlining the facts of the request for approval of Mr. Hoover, or Mr. Tolson, the Associate Director. Subsequently, the memorandum was filed in the Assistant Director's office under a 'Do Not File' procedure, and thereafter destroyed. In the field office, the SAC maintained a record of approval as a control device in his office safe. At the next yearly field office inspection, a review of these records would be made by the Inspection to insure that the SAC was not acting without prior FBIHQ approval in conducting surreptitious entries. Upon completion of this review, surreptitious entries. Upon completion of this review, these records were destroyed.

The FBI advised congressional investigators that, because of this procedure, it was "unable to retrieve an accurate accounting" of the number of warrantless surreptitious entries (S. Rept. 94–755, Book III, pp. 358–361).

The Department of Justice did not take a public position on the legality of "surreptitious entries" or intelligence searches generally, apart from electronic surveillance, until 1975 when the Department

filed a statement distinguishing its position from that of the Watergate Special Prosecutor in the appeal of the conviction of Nixon White House aide John Ehrlichman. In 1974, Ehrlichman was convicted under the federal civil rights statutes for authorizing the White House "plumbers" (a unit formed to stop leaks of classified information) to break into and search the office of the psychiatrist of former Defense Department official Daniel Ellsberg, who had provided the "Pentagon Papers," a study of U.S. policy in Vietnam, to the press in 1971. The District Court opinion by Judge Gerhard Gesell found the search "clearly illegal under the unambiguous mandate of the Fourth Amendment" because no search warrant was obtained: "the Government must comply with the strict constitutional and statutory limitations on trespassory searches and arrests even when known foreign agents are involved." *United States* v. *Ehrlichman,* 376 F. Supp. 29, 33 (D.D.C. 1974) Judge Gesell distinguished this case from the precedents that has upheld warrantless wiretapping for foreign intelligence purposes. In particular, he cited a passage in the Supreme Court's 1972 pinion in the Keith case to emphasize that the type of search in the *Ehrlichman* case should be viewed as more intrusive than wiretapping. The Supreme Court had stated that "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed" (407 U.S., at 313).

The Watergate Special Prosecutor took the same position as the District Court on appeal. Submitting a separate statement to the Court of Appeals, the Department of Justice declared:

> The physical entry here was plainly unlawful * * * because the search was not controlled as we have suggested it must be, there was no proper authorization, there was no delegation to a proper officer, and there was no sufficient predicate for the choice of the particular premises invaded.

The Department went on, however, to defend the power of the President to authorize this type of warrantless intelligence search technique on the same basis as wiretaps:

> It is the position of the Department that such activities must be very carefully controlled. There must be solid reason to believe that foreign espionage or intelligence is involved. In addition, the intrusion into any zone of expected privacy must be kept to the minimum and there must be personal authorization by the President or the Attorney General. The Department believes that activities so controlled are lawful under the Fourth Amendment.
>
> In regard to warrantless searches related to foreign espionage or intelligence, the Department does not believe there is a constitutional difference between searches conducted by wiretapping and those involving physical entries into private premises. One form of search is no less serious than another.

(Letter from Acting Assistant Attorney General John C. Keeney to Hugh E. Kline, Clerk of U.S. Court of Appeals for the District of

Columbia, May 9, 1975, cited in S. Rept. 94–755, Book III, pp. 369–370.)

In considering the *Ehrlichman* case, the Court of Appeals for the District of Columbia found it unnecessary to rule on whether there was an exception to the warrant requirement for searches of the property of foreign agents, because neither Ellsberg nor his psychiatrist was a foreign agent. Nevertheless, two of the three judges filed a concurring opinion which declared that "physical entry of the home was the 'chief evil' appreciated by the framers of the Constitution" and that national security electronic surveillance precedents may not apply to such intrusive searches. (*United States* v. *Ehrlichman,* 546 F.2d 910 (D.C.Cir. 1976), opinion of Judge Leventhal).

Another panel of the Court of Appeals for the District of Columbia dealt to a limited extent with intelligence searches in the Barker and Martinez case involving two persons convicted of assisting with the break-in into the office of Ellsberg's psychiatrist. Two judges of the panel voted to reverse the convictions. Judge Wilkey argued, in part, that because warrantless foreign intelligence-gathering activities were reasonable under some circumstances, Barker and Martinez could have reasonably believed the statements of a White House aide that the search was lawful. Judge Wilkey observed that the Justice Department had acknowledged that it could identify no "constitutional difference" between wiretapping and "physical entries into private premises" and that warrantless physical searches were permissible "under the proper circumstances when related to foreign espionage or intelligence" (*United States* v. *Barker,* 546 F.2d 940 (D.C.Cir. 1976), at 949–954). Judge Mehrige voted to reverse on different grounds and declined to concur in the Attorney General's position that there was a "national security" exception permitting warrantless intrusions into a citizen's home or office because that issue was not before the court (546 F.2d, at 957 n. 6). Judge Leventhal, who stated his position on intelligence searches in the *Ehrlichman* case, dissented, in part because Barker and Martinez had not asserted a belief that either the President or the Attorney General had personally authorized the search (546 F.2d, at 961–963).

In 1976 President Ford issued the first public Executive order on U.S. intelligence activities. Section 5(b)(3) of the order prohibited U.S. foreign intelligence agencies from engaging in "unconsented physical searches within the United States * * * except lawful searches under procedures approved by the Attorney General" (Executive Order 11905, February 18, 1976). The order did not expressly delegate authority to the Attorney General to approve physical searches. Nor did the order provide substantive standards for the exercise of that authority, other than a general mandate to conduct foreign intelligence activities "in a manner which preserves and respects our established concepts of privacy and civil liberties."

The Carter Administration issued a revised Executive order containing a provision on "unconsented physical searches within the United States." Sections 2–201 and 2–204 of the 1978 Carter order stated that such activities "for which a warrant would be required if undertaken for law enforcement rather than intelligence purposes shall not be undertaken against a United States person with-

out a judicial warrant, unless the President has authorized the type of activity involved and the Attorney General has both approved the particular activity and determined that there is probable cause to believe that the United States person is an agent of a foreign power" (Executive Order 12036, January 26, 1978).

The extent and conditions of President Carter's subsequent authorization of warrantless physical search activity were not made public. In the Truong-Humphrey espionage case, however, President Carter personally authorized warrantless physical searches by the FBI, reportedly "because of the limited nature of the delegations then in effect under Executive Order 12036" (Brown and Cinquegrana, "Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment," 35 *Catholic U. L. Rev.* 97, 140 (1985)).

The Truong-Humphrey case resulted in the only court decisions directly addressing the legality of warrantless intelligence searches of foreign agents. The case involved both warrantless electronic surveillance and warrantless searches that involved opening three packages transmitted by a Vietnamese intelligence officer to a courier for delivery abroad. The courier was an FBI asset who allowed the FBI to open and examine the packages. The District Court and the Court of Appeals for the Fourth Circuit disposed of the physical search issue summarily in opinions that dealt almost entirely with warrantless electronic surveillance. The District Court stated in a footnote:

> The Court is unpersuaded that there is any constitutional significance to the fact that this was a physical seizure and search and not an electronic search. It would be incongruous indeed were a court to find the opening of an envelope more intrusive than a wiretap or bug that runs for weeks at a time.

(*United States* v. *Humphrey,* 456 F. Supp. 51, 63 n. 13 (E.D.Va. 1978)).

The Court of Appeals opinion did not discuss the relative intrusiveness of different techniques and simply applied its warrantless electronic surveillance ruling to the searches. It accepted the rationale that the President's constitutional powers for the conduct of foreign policy gave him "the principal responsibility * * * for foreign intelligence surveillance" and took into account the practical difficulties that would "unduly frustrate" the President in attempting to get a warrant under normal procedures. (*United States* v. *Truong,* 629 F.2d 908 (4th Cir. 1980), *cert. denied,* 454 U.S. 1144 (1982)).

Significantly, the Truong-Humphrey decisions declared unconstitutional one of the three physical searches and a portion of the electronic surveillance conducted in the investigation. The third search, as well as electronic surveillance during the final stages of the investigation, violated the Fourth Amendment despite having been approved by the President and the Attorney General based on information establishing that the target was a foreign agent. The District Court found that, because the primary purpose of the investigation had shifted from foreign intelligence gathering to gathering criminal evidence, the foreign intelligence exception to the

warrant requirement could not be applied (*United States* v. *Humphrey,* 456 F.2d 51 (E.D.Va. 1978), at 63).

The Court of Appeals agreed with the "primary purpose" test:

> We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis of a criminal prosecution.

The Court of Appeals recognized that the evidence obtained from warrantless foreign intelligence gathering activities could be used in a criminal prosecution, so long as the government's primary purpose was to collect foreign intelligence rather than to prosecute the target (*United States* v. *Truong,* 629 F.2d, at 915–916).

While the *Truong-Humphrey* case was pending in the courts, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA) which established a special court to issue orders approving electronic surveillance for foreign intelligence purposes. FISAL regulated a wide variety of investigative techniques that fall within its definition of "electronic surveillance." Congress expressly declined, however, to apply the FISA procedures to physical searches. The legislative history in the House Intelligence Committee report on FISA stated:

> The committee does not intend to term "surveillance device" as used in paragraph [1801(f)](4) to include devices which are used incidentally as part of a physical search, or the opening of mail, but which do not constitute a device for monitoring. Lock picks, still cameras, and similar devices can be used to acquire information, or to assist in the acquisition of information, by means of physical search. So-called chamfering devices can be used to open mail. This bill does not bring these activities within the purview. Although it may be desirable to develop legislative controls over physical search techniques, the committee has concluded that these practices are sufficiently different from electronic surveillance so as to require separate consideration by the Congress. The fact that the bill does not cover physical searches for intelligence purposes should not be viewed as congressional authorization for such activities. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of activity.

The Committee report noted that Executive Order 12036 placed limits on physical searches (H. Rept. 95–1283, p. 53). The Senate Intelligence Committee report included an identical statement and also observed that proposed intelligence charter legislation would address the problem of physical searches for intelligence purposes. (S. Rept. 95–701, p. 38, citing S. 2525, the National Intelligence Reorganization and Reform Act of 1978.)

Subsequently, the Carter Administration endorsed provisions in a revised intelligence charter bill that would have amended the Foreign Intelligence Surveillance Act to incorporate physical searches. At Senate hearings on the National Intelligence Act of 1980, FBI Director William H. Webster testified:

> Title VIII amends the Foreign Intelligence Surveillance Act to subject physical searches to the same review and certification procedures, plus the same criminal standard for U.S. persons, as was carefully designed for wiretaps by this Congress in late 1978. The same compelling reasons of security that led to the foreign intelligence wiretap process apply to physical searches of foreign powers and their agents. Judicial review exists except in that limited number of searches that do not affect U.S. persons, property, or premises. I am confident that with the Foreign Intelligence Surveillance Court having the expanded role regarding physical search, plus Congressional oversight, the American public can be assured of the lawfulness of the process, while affording necessary security to the activity.

(*National Intelligence Act of 1980,* Hearings before the Select Committee on Intelligence, United States Senate, 96th Cong., 2d Sess. on S. 2284 (1980), p. 60.)

Although the Carter Administration proposed several minor amendments to the FISA procedures, it supported the basic court order requirement for intelligence searches. Legislation on physical search was not reported, as the comprehensive intelligence charter bill was set aside in favor of what became the Intelligence Oversight Act of 1980.

In the absence of legislation, the Department of Justice under the Carter Administration sought and obtained orders from the Foreign Intelligence Surveillance Court approving physical search for intelligence purposes in three cases, although Attorney General Benjamin Civiletti continued to state that the President retained independent authority to approve warrantless intelligence searches. The Justice Department advised the intelligence committees:

> The Attorney General has, as a matter of policy, decided that he will, whenever possible submit physical search issues to the FISA Court for judicial review. He believes this proposal provides maximum protection for individual rights and is consistent with national security interests. In submitting such applications, the Attorney General does not intend to alter the existing Executive policy regarding physical searches as set forth in the internal, classified documents which have previously been made available to you.

(*Letter from Kenneth C. Bass III, Counsel for Intelligence Policy, U.S. Department of Justice, to the Senate Select Committee on Intelligence, October 27, 1980, S. Rept. 96–1017, p. 11.)*

In a legal memorandum on the jurisdiction of the Foreign Intelligence Surveillance Court to issue search orders, the Justice Department explained why it was willing to accept a greater degree of judicial review:

> Prior to the creation of the Foreign Intelligence Surveillance Court, there was no established judicial procedure available which could be utilized without frustrating the Executive Branch's ability to carry out its intelligence activities. Accordingly, prior judicial approval was not required by the Fourth Amendment for warrantless foreign intelligence searches * * *.
>
> The creation of the Foreign Intelligence Surveillance Court (FISC) in 1978 with its pertinent protections against compromise and foreign penetration and its establishment of a special group of judges who have expertise in examining questions of law pertaining to foreign intelligence, diplomacy and military affairs eliminated the "frustration" previously existing with regard to judicial review of "electronic surveillance" as defined in the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. Sec. 1801(f). While the regular federal judicial system lacks the physical and personnel security structure used by the Executive to protect the national security, the FISC and its judges have secure facilities, personnel and procedures compatible with the Executive's foreign affairs and national security obligations. Also, intelligence searches are frequently based on information derived from intelligence surveillances, as has been the case in some of the applications already submitted. At least in the absence of contested litigation, only the FISC judges can review the files concerning these surveillances. FISC judges, therefore, are in a position to review applications for foreign intelligence searches without jeopardizing the Executive's requirements for security and expertise.

(Memorandum from Kenneth C. Bass III, Counsel for Intelligence Policy, to William H. Webster, Director, Federal Bureau of Investigation, in S. Rept. 96–1017 (1980), pp. 18–19.)

Although the Foreign Intelligence Surveillance Court approved three physical searches submitted by the Justice Department, the court directed its legal advisor to prepare a legal memorandum on the court's jurisdiction which concluded that the court had no authority to approve activities beyond "electronic surveillance" as defined in FISA (H. Rept. 96–1466, pp. 17–24).

Under the Reagan Administration in 1981, Attorney General William French Smith reversed the policy of his predecessor. In an extraordinary proceeding, the Justice Department submitted both an application to the Foreign Intelligence Surveillance Court for an order approving an intelligence search and a memorandum requesting the court to deny the application on the grounds that the court lacked jurisdiction. The memorandum stated that "there is no constitutional necessity to obtain a judicial warrant for the government to engage in a properly authorized intelligence physical search" and that "the Constitution does not require prior judicial review of intelligence physical searches of foreign powers or their agents when properly authorized by the President or the Attorney General." (See S. Rept. 97–280 (1981), pp. 10–16.)

Thereafter, Foreign Intelligence Surveillance Court Chief Judge George L. Hart, Jr., issued an opinion on behalf of the court con-

cluding that it had no authority over intelligence searches (*In re* the Application of the United States for an Order Authorizing Physical Search of Nonresidential Premises and Personal Property (U.S.F.I.S.C., June 11, 1981), in S. Rept. 97–280, pp. 16–19). The opinion of the Court focused on the intent of Congress in establishing the Foreign Intelligence Surveillance Court for the sole purpose of considering electronic surveillance applications. The opinion did not address the issue of Executive branch authority to conduct warrantless intelligence searches.

The Reagan Administration also revised the Executive order restrictions on warrantless physical searches. The new order eliminated the requirement in the Carter order for a separate Presidential delegation of authority to the Attorney General to approve particular types of activity (under which President Carter reportedly reserved certain matters for approval only by the President, as noted above). President Reagan's order stated:

> The Attorney General is hereby delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

(Sec. 2.5, Executive Order 12333, December 4, 1981).

Intelligence search practices after 1981 were discussed in a report by the Senate Intelligence Committee on the first five years' experience under the Foreign Intelligence Surveillance Act. This report stated that, in 1983, the FBI's guidelines incorporated definitions of "foreign power" and "agent of a foreign power" comparable to those in FISA for intelligence searches within the United States. The Justice Department's Counsel for Intelligence Policy testified that the Attorney General approved FBI intelligence searches "sparingly" and that each case received "extremely close scrutiny within the FBI and the Department to ensure that the rights and interests of U.S. persons are fully protected." According to the Counsel and FBI Director Webster, the approval procedures were almost identical to the Executive branch review procedures for FISA surveillances. (S. Rept. 98–660, p. 17.)

The Justice Department submitted an opinion on the applicability of a federal statute which makes it a crime for a federal law enforcement officer to search a private dwelling without a judicial warrant, except as incident to an arrest or with the consent of the occupant (18 United States Code Sec. 2236). The Department's opinion concluded that this statute "is not an impediment to properly approved warrantless physical searches for national security purposes," but the opinion also stated that "the issue is not free from doubt." The question is whether legislation passed in 1921 in response to reports of overly aggressive conduct by prohibition enforcement agents should be considered "an anachronism" because its original purpose does not apply, as the Department's opinion argued, or should be read literally to apply the FBI Agents who act

as both law enforcement and counterintelligence officers. (S. Rept. 98–660, p. 18.)

The Justice Department also provided a classified analysis of the constitutionality of warrantless intelligence searches. This analysis explained why ordinary judicial warrant procedures are not suitable for intelligence searches and discussed the problem of inadequate security arrangements for district courts and magistrates. Citing the experience under the Foreign Intelligence Surveillance Act, the Department's analysis stated:

> There is no comparable modified provision or procedure by which to obtain warrants authorizing physical searches conducted for foreign intelligence purposes. * * * The operation of the United States Foreign Intelligence Surveillance Court demonstrates that a properly structured and specialized court can achieve the expertise and security to consider these issues, and a properly drawn statute can prevent judicial intrusion into policy decisions legitimately left to the Executive Branch.

FBI Director Webster also testified with respect to the risks of possible civil or criminal liability by FBI employees involved in such searches in the absence of a court order:

> Well, we are fortified by considerable advice and opinion of the Attorney General as to the inherent authority of the President delegated to him to authorize searches in national security matters. That convinces me that the good faith defense is clearly available to us * * * in relying on the advice of our chief law enforcement officer. But I am also mindful of course that the *Keith* opinion in 1972 left open the questions of whether searches required a warrant in national security matters. I am sure our agents can withstand the lawsuits, but I naturally prefer not to have them at all.

(S. Rept. 98–660, p. 18.)

This Committee's 1984 report on the implementation of the FISA characterized the legal position of Congress regarding warrantless physical search practices as "comparable to its position before FISA in the field of electronic surveillance, which was described in the *Keith* case as 'essentially neutral.' Congress has done nothing to authorize such actions by the Executive branch; any determination of the validity of Executive branch assertions of inherent powers to conduct warrantless physical searches is up to the courts" (S. Rept. 98–660). The Committee went on to urge the adoption of a court order procedure for intelligence searches:

> The Committee is persuaded that a court order procedure for physical searches in the United States using either the FISA procedure or a procedure comparable to FISA, ought to be established. Based on the FISA experience, we are now confident that such a court order procedure would remove the legal and constitutional ambiguities inherent in current Executive branch practice regarding physical searches for foreign intelligence purposes. We also note that Executive branch approval standards for

> such physical searches are already very similar to FISA standards, and that previous use of the FISA Court (which was stopped when the Court ruled that it lacked authority in such cases) did not appear to have caused any practical difficulties. The Committee intends to develop a legislative proposal for amendment of FISA or for a court order procedure comparable to FISA, in consultation with the Attorney General.

(S. Rept. 98–660, *The Foreign Intelligence Surveillance Act of 1978: The First Five Years* (1984), p. 19.)

Two years later, in its report on *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs,* the Committee reiterated its view: "Congress should enact legislation comparable to FISA to authorize physical search for intelligence purposes, so as to reduce legal uncertainties in counterintelligence investigations that have prosecution as one of their objectives." The report stated that the Committee was "prepared to develop and introduce such legislation in cooperation with the Executive branch" (S. Rept. 99–522, pp. 54, 56.) Given the lack of interest in the Reagan Administration for pursuing the matter, no such legislation was developed.

Four years later, in 1990, a panel of outside consultants to the Senate Intelligence Committee, the so-called "Jacobs panel" (see the background provided earlier in the report) chartered to look at statutory changes to improve the counterintelligence posture of the federal government, recommended legislation—introduced by Senators Boren and Cohen as S. 2726—to bring intelligence searches under the FISA. Testifying on behalf of the Jacobs panel, Columbia Law Professor Harold Edgar advised the Committee on May 23, 1990:

> We think subjecting such searches to a court order process not only would be an important safeguard for the civil liberties of Americans, but would serve as a protection for employees of the Executive agencies who are asked to engage in such searches. The Panel has been told that the FISA has worked exceedingly well over the last ten years where electronic surveillances are concerned. We are persuaded that it should be applied to physical searches as well.

(Testimony of Harold Edgar, *Hearings before the Senate Select Committee on Intelligence,* on "S. 2726 to Improve U.S. Counterintelligence Measures," May 23, 1990, p. 18.)

Justice Department witnesses testified in response that the Department was "fully satisfied the President's authority in this area is adequate to meet our intelligence needs," but said the Administration maintained "an open mind on the question of whether legislation which supplements this authority would be useful" (testimony of Mary C. Lawton, in *Hearings before the Select Committee on Intelligence*, on "S. 2726 to Improve U.S. Counterintelligence Measures," July 12, 1990, p. 129). The legislative provision contained in S. 2726 was not, however, acceptable to the Administration as written.

Somewhat revised legislation was introduced later in the session by Senators Boren and Cohen which incorporated revised language pertaining to intelligence searches (S. 3251), but no action was taken on the bill. The same language was included in a bill (S. 394) reintroduced in January, 1991 by Senators Boren and Murkowski, but it also was not reported by the Committee. The Bush Administration did not support either of these proposals.

In the fall of 1993, Attorney General Janet Reno approved a warrantless intelligence search of the residence of CIA employee Aldrich H. Ames, who was at the time the subject of a counterintelligence investigation carried out jointly by the FBI and the CIA. Evidence developed as a result of the search subsequently became part of the Government's indictment of Ames on charges of conspiracy to commit espionage and tax evasion. Since the defendants pled guilty to the charges, a trial was not held, and the legality of the intelligence search was not considered by the court.

Following the plea agreements in the Ames case, however, the Administration advised the Committee in May, 1994, that it was interested in reconsidering legislation to provide a court order procedure for intelligence searches. In concert with the Administration, new language was developed, set forth in section 9 of the bill.

Purpose of a court order procedure for intelligence searches

The Committee continues to believe there are compelling reasons to establish statutory procedures for the conduct of physical searches in the United States to collect foreign intelligence information, especially to include a court order procedure similar to that used for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978.

In the absence of legislation, the Executive branch will continue conducting physical searches without a judicial warrant based upon the approval of the Attorney General. The Committee does not believe this arrangement provides adequate protection for the constitutional rights of U.S. citizens. Searches carried out under a court order would provide such protection. The special court established under the Foreign Intelligence Surveillance Act of 1978 is comprised of seven federal district court judges appointed by the Chief Justice of the United States. The statutory requirements which must be met by the Government before an order approving an electronic surveillance can be issued by this court are detailed and comprehensive. The constitutionality of such orders has been upheld by every federal court which has considered the issue since 1978.

The constitutionality of warrantless intelligence searches, on the other hand, remains unresolved. There is no authoritative judicial opinion upholding the legality of such searches. Any defendant in an espionage case who is confronted with evidence obtained by an intelligence search can be expected to challenge the legality of such search. Should a court rule against the Government, a successful prosecution could be seriously jeopardized.

Such a ruling would also leave those federal officers in the Justice Department and FBI who approved and carried out such search potentially liable to civil suits by the defendant for violation of his or her civil rights. The Committee is advised that such offi-

cers routinely purchase personal liability insurance at their own expense to guard against such contingency.

Thus, from the standpoint of protecting the constitutional rights of Americans, from the standpoint of bringing greater legal certainty to this area, from the standpoint of avoiding problems with future espionage prosecutions, and from the standpoint of protecting federal officers and employees from potential civil liability, the Committee believes this legislation is desirable and necessary.

Section 10: Lesser criminal offense for the unauthorized removal of classified documents

Section 10 of the bill would create a new misdemeanor offense applicable to federal employees who knowingly remove classified documents or materials without authority with the intent to retain them at an unauthorized location. Persons convicted of such offense could be fined up to $1,000 or imprisoned for up to a year, or both.

The Committee included this provision in the bill principally because it believes the unauthorized removal and retention of classified documents is a widespread problem within the Executive branch. Although Executive regulations currently prohibit such conduct, these regulations appear to provide little deterrence to federal employees. Making such conduct a criminal offense, albeit a misdemeanor, would in the view of the Committee have a far more effective impact.

The Committee sees no justification for federal employees to remove classified materials to unauthorized locations and retain them there. If there is a need for federal employees to take such materials to their residences to work on them, the Executive branch ought to provide authority for such removal under carefully limited conditions.

The unauthorized removal and retention of classified documents or materials at an unsecure location inherently increases the risk that such documents or materials will be disclosed to unauthorized persons. Indeed, some employees may "stockpile" such materials waiting for an opportunity, or possibly the motivation, to sell them.

The Committee believes this provision could be useful to the Government not only to deter such conduct, but also as a means of prosecuting cases where the passage of classified information to a foreign government cannot be proved. This lesser criminal offense might also be used by the Government in negotiating plea agreements with defendants in certain cases.

The Committee notes that under some circumstances the type of conduct contemplated by this section might be prosecuted under subsection 793(d) of title 18, United States Code, which provides, in pertinent part:

> Whoever, lawfully having possession of * * * any document, writing, code book, signal book, sketch, photograph * * * model, instrument, appliance * * * or information relating to the national defense which the possessor has reason to believe could be used to the injury of the United States or to the advantage of a foreign nation * * * *willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to re-*

ceive it * * * shall be fined not more than $10,000 or imprisoned not more than ten years, or both. (Italic added.)

Thus, where the Government discovered classified documents were being stored at an unauthorized location and made a demand for the documents which was refused by the officer or employee concerned, it would appear such officer or employee could be prosecuted under section 793(d). Conversely, any officer or employee who did cooperate and willingly returned the classified materials to Government control when asked to do so could not be prosecuted under section 793(d).

The Committee believes that where classified information is involved, the fact that a government officer or employee is willing to surrender such information when he or she has been discovered by the Government should not absolve such officer or employee from possible criminal liability, as now appears to be the case under section 793(d). If classified information is knowingly removed without authority with the intent to retain it for an indefinite period of time, such action necessarily creates a substantial risk of unauthorized disclosure and damage to the national security, regardless of whether such harm actually occurs. For a government officer or employee to have knowingly created such a risk is itself, in the view of the Committee, reprehensible conduct which should carry potential criminal liability.

The Committee is also mindful of the objection raised to this provision that it might be used to prosecute "whistleblowers," i.e., federal employees who remove classified documents or materials containing evidence of fraud, waste, or abuse in order to provide them to the press, Congress, or other oversight mechanisms within the Executive branch.

First, the Committee notes that the Whistleblower Act of 1989 (5 U.S.C. et seq.) does not provide protection to federal employees who disclose classified information indicating violation of laws, rules, or regulations, or gross mismanagement, or gross waste of funds, or abuse of authority, or a substantial and specific danger to public health and safety unless such information is disclosed to the Special Counsel appointed under the Act or the Inspector General of the agency concerned. It is the intent of the Committee that section 10 be interpreted consistent with the Whistleblower Act of 1989. In other words, disclosure of classified information to the Special Counsel or the Inspector General pursuant to the Whistleblower Act of 1989 would be an "authorized" disclosure provided for by law.

Furthermore, the misdemeanor offense created by section 10 would not be established without proof of the intent to retain such documents or materials at an unauthorized location. A "whistleblower" who removes classified documents or materials for the purpose of conveying them to the Special Counsel or relevant Inspector General under the Act presumably would have no need to retain such documents or materials at an unauthorized location.

In conclusion, the Committee believes the creation of this new misdemeanor offense would be useful both as a deterrent and as providing an additional ground for prosecution in particular circumstances.

THE NEED FOR ADDITIONAL ACTIONS BY THE EXECUTIVE BRANCH

In addition to the actions mandated by the bill, the Committee believes numerous actions are needed by the Executive branch to improve the counterintelligence and security posture of the Government. Foremost among them are:

The need for improved security awareness training to sensitize employees to security problems within their respective organizations;

The need for training which sensitizes intelligence employees to the needs of law enforcement, and, conversely, which sensitizes law enforcement officials to the need of intelligence;

The need to improve the control of classified information generally, to include more stringent measures to prevent classified materials from being removed without authority from government or government-approved facilities and to enforce compartmentation, particularly the control of sensitive information electronically available to cleared employees; and

The need to relate counterintelligence information more closely with routine security activities (e.g. background investigations, polygraph examinations, etc.) in order to make better use of existing administrative capabilities in dealing with counterintelligence problems.

Enactment of S. 2056 does not in any way relieve the Executive branch of the responsibility to take appropriate actions pursuant to its own authority to address the shortcomings and deficiencies evident in current system.

SECTION-BY-SECTION ANALYSIS

Section 1

Section 1 contains the title of the Act, "The Counterintelligence and Security Enhancement Act of 1994."

Section 2

Section 2 adds a new title VIII to the National Security Act of 1947 (50 U.S.C. 401 et seq.) to govern access to classified information.

Section 801 of the new title requires the President to issue within 180 days of the date of enactment an Executive order or regulation which establishes procedures to govern access to classified information which shall be binding upon all departments, agencies, and offices of the Executive branch. Section 801 provides that, at a minimum, this order or regulation shall satisfy certain requirements set forth in subsections (1)–(5) of this section.

Subsection (1) provides that no person may be given access to classified information by any department, agency, or office of the Executive branch unless, based upon an appropriate background investigation, such access is determined to be clearly consistent with the national security interests of the United States, except as may be determined by the President.

It is anticipated that all full-time Executive branch employees who may require access to classified information in the performance of their official duties will meet this standard. The latitude which the Committee provides the President to permit access to

other persons is intended to cover persons who are not full-time employees of the Executive branch but who require access for a particular purpose or are permitted access based upon a treaty or international agreement, and for other circumstances. Even in these circumstances, it is expected the President will require appropriate measures to ascertain the trustworthiness of the recipient or recipients in question and to protect against the unauthorized disclosure of any classified information provided pursuant to such arrangements.

Subsection (2) requires the Executive order or regulation issued by the President to establish uniform minimum requirements governing the scope and frequency of background investigations and reinvestigations for all persons who require access to information as part of their official responsibilities.

This subsection is not intended to preclude departments and agencies of the Executive branch which handle extremely sensitive classified information from imposing requirements in excess of those required by the Executive order or regulation. For example, some agencies require polygraph examinations or psychological testing as a condition of access to classified information in addition to a background investigation. In some cases, departments and agencies perform reinvestigations more frequently than other agencies. This subsection is not intended to preclude such practices unless the President determines that such limitation or regulation is warranted. It is the intent of this section to establish a minimum uniform baseline for security clearances generally. It is anticipated that once access to classified information is granted by one department or agency based upon the standards in the order or regulation, access will be granted by other departments and agencies without the need for separate security clearances from each department or agency concerned.

Subsection (3) provides that all employees who require access to classified information shall be required as a condition of such access to provide written consent to the employing department or agency which will permit access by an authorized investigative agency to relevant financial records, other financial information, consumer reports, and travel records, as determined in the order or regulation issued by the President, during the period of access to classified information and for a period of five years thereafter. Such consent is, indeed, required as a condition of any request for such records made pursuant to section 802 of this section (which must also meet additional criteria).

While the President retains the discretion to determine which types of financial and travel records may be relevant to assessing the security status of a cleared employee, the Committee intends that the President consider requiring consent for access to tax returns and tax return information, consistent with section 6103 of the Internal Revenue Code, as well as access to financial records or information covered by the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.); the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); and the Bank Secrecy Act of 1986. Relevant travel records include records maintained by travel entities in the United States concerning travel outside the United States.

Subsection (4) provides that all persons who occupy positions in the executive branch of the Government who require access to particularly sensitive classified information, as determined by the President, shall be required, as a condition of maintaining access to such information, to submit to the employing department or agency during the period of such access, relevant information concerning their financial conditions and foreign travel, as determined by the President, as may be necessary to ensure appropriate security.

This subsection leaves to the discretion of the President what employees will be required to submit financial and travel reports, consistent with the needs of security and the capabilities of departments and agencies to process and evaluate such reports. The President is also given discretion to establish the type of information which will be required and the frequency with which reporting will be required.

The Committee anticipates that the population covered by this requirement will be relatively small, limited to those with access to truly sensitive information, the unauthorized disclosure of which would likely result in significant costs to the United States or to other governments or persons who cooperate with the United States.

Subsection (5) required that uniform minimum standards be established to ensure that employees whose access to classified information is being denied or terminated under this title are appropriately advised of the reasons for such denial or termination and are provided an adequate opportunity to respond to all adverse information which forms the basis for such denial or termination before final action by the department or agency concerned. This subsection does provide, however, that where adverse information is derived from a classified source, appropriate measures may be taken to protect the identity of such source from the employee concerned.

It is the Committee's intent to require the President to establish by order or regulation uniform minimum due process rights applicable to all employees whose access to classified information is being denied or terminated so that such rights shall not vary depending upon the employing department or agency.

It is not the intent of the Committee to diminish in any way the due process procedures which are currently provided to contractor employees pursuant to the Department of Defense Industrial Security Program, e.g., formal hearings before administrative law judges, rights of appeal to a review board, etc. In other words, it is not intended that the rights and protections of contractor employees provided pursuant to Executive Order 10865 (25 Fed. Reg. 1583), dated February 20, 1960, be affected in any way by this provision.

It is the intent of the Committee that employees of the Executive branch are accorded sufficient due process rights to ensure that they understand why their security clearances are being denied or terminated and are given an adequate opportunity to respond to the adverse information at issue. While the Committee subscribes to the view that security clearances are a privilege granted by the Executive branch and are not a "right" of the individual employee,

it is also cognizant that mistakes can be made, and often are made, in the clearance process. As a practical matter, failure to obtain a security clearance can have an adverse impact on an employee's career and earning capacity. Thus, the Committee believes that basic fairness requires a process which ensures the affected employee an opportunity to challenge or supplement adverse information which forms the basis for a decision to deny or terminate his or her security clearance.

Section 802 provides policy and procedures to govern requests by authorized investigative agencies for access to financial records and travel information pertaining to employees of the executive branch of government who hold security clearances.

Subsection (a)(1) provides that any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer credit reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. The subsection also provides that such agency may request records maintained by any commercial entity in the United States pertaining to travel by a person outside the United States. The terms "financial agency," "financial institution," "holding agency," and "consumer credit reporting agency" are defined in section 804 of this title.

Subsection (a)(2) sets forth the criteria which must be met before a request may be made by an authorized investigative agency pursuant to this section.

Subsection (a)(2)(A) provides that the records sought must pertain to a person who is or was an employee required by the President in an Executive order or regulation, as a condition of having access to classified information, to provide consent, during the period of such access and for five years thereafter, to an authorized investigative agency having access to financial or travel records.

Subsection (a)(2)(B) provides that, in addition, one of three circumstances must exist before such records may be requested:

There are information or allegations indicating that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

Information comes to the attention of the employing agency indicating the person has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information known to the agency; or

Circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

In short, the Committee intends that a specific and articuable basis exist in order for an authorized investigative agency to request financial or travel records pursuant to this section. This basis need not necessarily indicate wrongdoing on the part of the employee concerned, but only that information known to the agency regarding such employee (who has already consented to such access as a condition of obtaining a security clearance) makes further inquiry prudent in the interests of maintaining security.

Subsection (a)(3) provides that each request by an authorized investigative agency pursuant to this section shall be accompanied by a written certification signed by the department or agency head, the deputy department or agency head, or by a senior official designated by the department or agency head for this purpose which shall be no lower than an Assistant Secretary or Assistant Director. This certification shall contain a statement that the person whose records are requested is a covered employee or former employee of the department or agency concerned; that the request is being made pursuant to an authorized inquiry or investigation and is authorized pursuant to this section; and that the records or information being requested are records or information which the employee previously agreed to make available for review by an authorized investigative agency. Subsection (a)(3) also provides that a copy of the employee's consent shall be furnished the recipient and that the request shall identify specifically or by category the records or information to be reviewed and advise the recipient of the prohibition in subsection (b), as explained immediately below.

Subsection (b) provides that notwithstanding any other provision of law, no governmental or private entity, officer, employee or agent of such entity, may disclose to any person, other than those officers, employees, or agents of such entity necessary to satisfy a request made under this section, that such entity has received or satisfied a request made by an authorized investigative agency under this section.

It is the Committee's intent, in order to preserve the confidentiality of the inquiry or investigation, to protect the privacy of the person concerned, and to prevent persons who may have violated the law from destroying evidence or evading detection, that requests made under this section not be disclosed by the recipients of such requests.

Subsection (c)(1) provides that notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) shall, if the request satisfies the requirements of this section, be made available within 30 days for inspection or copying by the authorized investigative agency concerned.

Section 6103 of the Internal Revenue Act of 1986 permits the Secretary of the Treasury to provide access to tax returns and tax return information to government agencies based upon the written request of the taxpayer but permits the Secretary not to disclose such information where the Secretary determines that "such disclosure would seriously impair Federal tax administration." By leaving intact this provision, it is the Committee's intent to leave this determination to the discretion of the Secretary. However, given the expectation of the Committee that requests for access to such information will be limited and subject to a high level of approval, it is the expectation that disclosure of tax returns and tax return information pursuant to this section would not "seriously impair Federal tax administration" pursuant to section 6103.

Section (c)(2) of the bill provides that any entity that discloses records of information for inspection or copying in good faith reliance upon the certifications made by an agency pursuant to this section shall not be liable for any disclosure to any person under

this title, the constitution of any State, or any law or regulation of any State or political subdivision of any State.

Section (d) provides that any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for reasonable costs incurred in responding to such request.

Section (e) restricts agencies receiving records or information pursuant to a request under this section from disseminating such records or information outside the agency except to the employing department or agency; to the Department of Justice for law enforcement or counterintelligence purposes; or to another federal agency where the information is clearly relevant to the authorized responsibilities of such agency.

Section (f) clarifies that nothing in this section is intended to affect the authority of investigative agencies pursuant to the Right to Financial Privacy Act or the Fair Credit Reporting Act.

Section 803 provides that the provisions of this title shall not apply to the President and Vice President, Members of the Congress, Justices of the Supreme Court, and Federal judges appointed by the President.

While the provisions of sections 801 and 802 by their own terms apply only to employees of the Executive branch, the Executive branch itself may choose to condition access to classified information by the legislative and judicial branches based upon the same or similar standards. Section 803 makes clear that certain officials in the legislative and judicial branches, together with the President and Vice President, are exempted from the requirements of this statute or any regulations promulgated thereunder.

Section 804 contains the definitions of terms used in this title.

Subsection (1) defines the term "authorized investigative agency" as meaning any agency authorized by law or regulation to conduct a counterintelligence investigation or investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information.

Subsection (2) defines the term "classified information" as meaning any information that has been determined pursuant to Executive Order 12356, dated April 2, 1982, or successive orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated.

Subsection (3) provides that the term "consumer credit reporting agency" has the same meaning as given in section 603 of the Consumer Credit Protection Act (15 U.S.C. 1681a).

Subsection (4) defines the term "employee" as including any person who receives a salary or compensation of any kind from the United States Government, is a contractor of the United States Government or an employee thereof, is an unpaid consultant of the United States Government, or otherwise acts for or on behalf of the United States Government.

Subsection (5) provides that the terms "financial agency" and "financial institution" have the meanings given such terms in section 5312(a) of title 31, United States Code, and the term "holding agency" has the meaning given such term in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401).

Subsection (6) provides that the terms "foreign power" and "agent of a foreign power" have the same meanings set forth in subsections 101 (a) and (b), respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Subsection (7) defines the term "State" to mean each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau (until such time as the Compact of Free Association is ratified), and any other possession of the United States.

Section 2(b) amends the table of contents of the National Security Act of 1947 to include the new title VIII added by section 2(a).

Section 2(c) provides that the amendments made by sections 2 (a) and (b) shall take effect 180 days after the date of enactment. This period is necessary in order to allow time for the President to issue the implementing regulations required by section 801 prior to the effective date of this title.

Section 3

Section 3 of the bill establishes a national-level mechanism for the development of policy and resolution of conflicts involving U.S. counterintelligence activities and establishes procedures to ensure that such activities are appropriately coordinated by affected departments and agencies with the Federal Bureau of Investigation.

Subsection (a) provides for the establishment of a National Counterintelligence Policy Board which shall report to the President through the National Security Council. The Board would be chaired by the Attorney General and be composed of the Secretary of Defense, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation and the Advisor to the President for National Security Affairs.

This Board is similar to that created recently by presidential directive. However, under the presidential directive, the chair of the Board would rotate every two years between a representative of the Secretary of Defense, the Director of Central Intelligence, and the Director of the FBI. While the Committee understands that the two-year rotational chairmanship was intended to demonstrate evenhandedness among the principal agencies involved in counterintelligence, the Committee believes that this will at the same time limit its institutional effectiveness. The Committee believes a permanent chair would provide better continuity and leadership, and that the Attorney General, who has responsibility for the Federal Bureau of Investigation, the largest and predominant counterintelligence agency within the Government, is the appropriate official to bear this responsibility. It is also believed that the Attorney General would be the official, short of the President, best positioned to arbitrate disputes which may arise between agencies.

Subsection (b) provides that the Board shall serve as the principal mechanism for developing policies and procedures for the approval of the President in the counterintelligence area, and for resolving conflicts, as directed by the President, which may arise between counterintelligence agencies.

These functions are similar to those assigned to the Board by the recent presidential directive. In particular, the Committee believes it important, in light of the requirements contained in subsection (c) of this section, that the statute itself provide a mechanism whereby conflicts between agencies can be appealed and resolved.

Subsection (c) provides that the heads of departments and agencies within the Executive branch shall take appropriate actions to ensure that counterintelligence matters are coordinated with the Federal Bureau of Investigation, as specifically provided in this subsection.

By imposing such a requirement on department and agency heads, the Committee does not intend to interfere with communications between the heads of departments or agencies and the President. There is nothing in this section which precludes department or agency heads from bringing counterintelligence matters of concern to the attention of the President. Nor does this section restrict the President in the exercise of his constitutional functions. This subsection imposes no obligation on the President but rather upon department and agency heads to ensure appropriate coordination of counterintelligence matters with the FBI.

At the same time, the Committee believes that the President as well as department and agency heads must be accountable for breakdowns in the coordination process. If criminal prosecutions of potential spies are foreclosed, delayed, or hampered due to inadequate coordination in the Executive branch, the interests of the American people are not well served. Having said that, the Committee notes that subsection (c) contains no criminal penalties for failure to comply with its terms. Such failures will clearly be a matter of concern, however, to the oversight committees of the Congress, and, ultimately, to the American people.

Subsection (c) prescribes general requirements for departments and agencies to follow in dealing with counterintelligence cases. It is meant to allow considerable flexibility in terms of implementation. Thus, departments and agencies are given latitude to determine how and at what level in the FBI the required coordination will be achieved, depending upon the facts at hand. The Committee cannot realistically envision any circumstance which would justify failure to coordinate at some level within the FBI. But presuming that such a rare circumstance might arise, the Committee would consider coordination with the Attorney General, who is the chief law enforcement officer of the United States and who exercises overall authority over the FBI and serves as Chair of the National Counterintelligence Policy Board, as constituting compliance with subsection (c). The Committee would expect, however, that the rationale for coordinating with the Attorney General and not the FBI directly would be fully explained at the time of the annual report required by subsection (c)(2).

Subsection (c) is also not intended to interfere with communications between agencies which might be required by law or Executive branch policy. For example, nothing in this section affects the responsibilities of departments and agencies to keep chiefs of U.S. diplomatic missions abroad fully and currently informed of activities within their area of jurisdiction pursuant to Section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927). Nor does this section

affect the responsibility of departments and agencies to report possible violations of federal criminal statutes to the Attorney General pursuant to 28 U.S.C. 535. Nor does it affect the coordination requirements with respect to counterintelligence activities contained in Executive Order 12333.

Subsection (c)(1)(A) provides that the heads of departments and agencies will ensure the FBI is advised immediately of any information, regardless of its source, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, as those terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978.

The intent of the Committee is to require reports to the FBI of all cases where information comes to the attention of a department or agency which suggests that U.S. classified information may have been lost or compromised to a foreign government through the intentional act of an individual or through other clandestine means, e.g., electronic eavesdropping. It is not meant to require reports of security violations where classified information has been mishandled or is otherwise left vulnerable to compromise unless the information suggests that a loss or compromise to a foreign government has actually taken place. Nor is it intended to require reports to the FBI of leaks of classified information to the news media.

It is meant to require reports to the FBI of circumstances which indicate that classified information has been lost, e.g., an intelligence source has been compromised or a classified military or intelligence operation has been thwarted in the absence of strong evidence indicating another explanation, regardless of whether the department or agency concerned has direct evidence of the loss or compromise to the foreign government concerned.

Nothing in this subsection prevents departments or agencies, once such information has been received, from taking such immediate steps as may be required by applicable agency regulations to limit the extent of the damage or the effects of the loss or compromise in question before a report can be made to the FBI pursuant to this subsection.

Subsection (c)(1)(B) provides that once a report has been made to the FBI pursuant to subsection (c)(1)(A), the department or agency concerned shall consult with the FBI with respect to all subsequent actions which may be undertaken by the department or agency concerned to determine the source of such loss or compromise.

This obligation is intended to encompass use of extraordinary investigative techniques (e.g., interviews of fellow employees) as well as routine administrative measures (e.g., scheduled polygraph examinations) which are to be utilized to ascertain the source of the loss or compromise.

It is not intended to require prior consultation with the FBI with respect to passive administrative actions undertaken by the department or agency concerned, e.g., reviews of personnel records or security files, which may relate to the loss or compromise or identify persons who had access to the information which was lost or compromised. Nor is prior consultation required for routine administrative measures which are not to be utilized for the purposes of

ascertaining the source of the loss or compromise, e.g., routine background investigations or reinvestigations.

If there should be a disagreement between the FBI and the department or agency concerned regarding what follow-on actions are appropriate, which cannot be resolved between the two parties, it is the intent of the Committee that the matter be referred to the National Counterintelligence Policy Board established by section 3(a), or to a subcommittee thereof as may be appropriate, for resolution.

Subsection (c)(1)(C) provides that where, after appropriate consultation with the department or agency concerned, the FBI undertakes investigative activities of its own to determine the source of the loss or compromise, its investigators will be given complete and timely access to the employees and records of the department or agency concerned for purposes of its investigation.

It is the Committee's expectation that once the FBI determines to initiate an investigation, the department or agency concerned will work with the FBI in a cooperative manner to facilitate its investigation without undue delays or bureaucratic obstacles being imposed. At the same time, the Committee expects the FBI to respect the concerns of the department or agency involved and to avoid unreasonable demands upon its personnel and resources or risks to its operations.

Subsection (c)(2) provides that beginning on February 1, 1995, and for each year thereafter, the Director of the Federal Bureau of Investigation shall, in consultation with the Director of Central Intelligence and the Secretary of Defense, submit a report to the two congressional oversight committees with respect to compliance with subsection (c)(1) during the previous calendar year.

It is expected that this report shall describe any cases where reports required by (c)(1)(A) were delayed or not made at all; cases where actions were taken by departments or agencies without the consultation required by (c)(1)(B); and cases where departments or agencies did not provide timely and complete access to their employees or records as requested by the FBI. In any case in which coordination was achieved by reporting to the Attorney General rather than directly to the FBI, the Attorney General will be expected to describe that case and the basis which necessitated this action, either in the FBI report or in a separate report submitted at the same time.

Subsection (c)(3) provides that nothing in subsection (c) may be construed to alter the jurisdictional arrangements between the Federal Bureau of Investigation and the Department of Defense with respect to investigations of persons subject to the Uniform Code of Military Justice, nor to impose additional reporting requirements upon the Department of Defense with respect to such investigations other than those required by existing law or executive branch policy.

This provision recognizes that the Department of Defense retains independent investigative and and prosecutive authority over military personnel subject to the Uniform Code of Military Justice. The Committee believes that investigative activities by the military departments which involve such personnel should not be subject to additional coordination with the FBI beyond what is now required

by law and Executive order. Under section 603 of the FY 1990 Intelligence Authorization Act, DoD is required to report to the FBI information it may receive concerning violations of espionage statutes by military personnel assigned to U.S. diplomatic missions abroad. Under paragraph 1.12 of Executive Order 12333, the military departments are required to coordinate counterintelligence activities in the United States (including those involving military personnel) with the FBI.

This subsection is not intended, however, to exempt the Department of Defense from compliance with subsection (c)(1)(A) requiring reports of information which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power. Nor is it intended to exempt the Department of Defense from compliance with subsections (c)(1)(B) or (c)(1)(C) where the matter involves civilian employees who are not subject to the Uniform Code of Military Justice.

Subsection (c)(4) provides that the terms "foreign power" and "agent of a foreign power" shall have the same meaning as set forth as sections 101 (a) and (b), respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Section 4

Section 608 of the Fair Credit Reporting Act (FCRA) presently consists of only one paragraph which authorizes credit reporting agencies to provide government agencies with certain identifying information respecting a consumer. Section 4 of this bill would amend FCRA section 608 by designating the existing text as subsection 608(a) and adding a new subsection 608(b) consisting of eleven paragraphs.

Paragraph 608(b)(1) of the amended FCRA requires a consumer reporting agency to furnish a consumer report to the FBI when presented with a written request for a consumer report, signed by the FBI Director or Deputy Director, which certifies compliance with the subsection. The Director or Deputy Director may make such a certification only if the Director or the Deputy Director has determined in writing that such records are necessary for the conduct of an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person whose consumer report is sought is a foreign power or an agent of a foreign power, as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

The requirement that there be specific and articulable facts giving reason to believe that the person is an agent of a foreign power before the FBI can obtain access to a consumer report is consistent with the standards in the Right to Financial Privacy Act, 12 U.S.C. 3414(a)(5)(A), and the Electronic Communications Privacy Act, 18 U.S.C. 2709(b).

However, in contrast to those statutes, the Committee has drafted the FCRA certification requirement to provide that the FBI request submitted to the consumer reporting agency make reference to the statutory provision without providing the agency with a written certification that the subject of the consumer report is believed to be an agent of a foreign power. FBI would still be re-

quired to record in writing its determination regarding the subject, and the credit reporting agency would be able to draw the necessary conclusion, but the Committee believes that its approach would reduce the risk of harm from the certification process itself to the person under investigation. A similar approach is taken in paragraph 608(b)(2), described below.

Section 605 of the FCRA, 15 U.S.C. 1681c, defines "consumer report" in a manner that prohibits the dissemination by credit reporting agencies of certain older information except in limited circumstances. None of these excepted circumstances would apply to FBI access under the proposed FCRA paragraph 608(b)(1) (or proposed FCRA paragraph 608(b)(2)). Accordingly, FBI access would be limited to "consumer reports" as defined in section 605.

The term "an authorized foreign counterintelligence investigation" includes those FBI investigations conducted for the purpose of countering international terrorist activities as well as those FBI investigations conducted for the purpose of countering the intelligence activities of foreign powers. Both types of investigations are conducted under the auspices of the FBI's Intelligence Division, headed by an FBI Assistant Director.

Paragraph 608(b)(2) would give the FBI mandatory access to the consumer identifying information—name, address, former addresses, places of employment, or former places of employment—that it may obtain under current section 608 only with the consent of the credit reporting agency. A consumer reporting agency would be required to provide access to such information when presented with a written request signed by the FBI Director or Deputy Director, which certifies compliance with the subsection. The Director or Deputy Director may make such a certification only if the Director or the Deputy Director has determined in writing that such information is necessary to the conduct of an authorized foreign counterintelligence investigation and that there is information giving reason to believe that the person about whom the information is sought has been, or is about to be, in contact with a foreign power or an agent of a foreign power, as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

FBI officials have indicated that they seek mandatory access to this identifying information in order to determine if a person who has been in contact with a foreign power or agent thereof is a government or industry employee who might have access to sensitive information of interest to a foreign intelligence service. Accordingly, the Committee has drafted this provision to require that such limited information can be provided only in circumstances where the consumer has been or is about to be in contact with the foreign power or agent.

The Committee has also drafted paragraphs 608(b)(1) and 608(b)(2) in a manner intended to make clear the Committee's intent that the FBI may use this authority to obtain the consumer records of only those persons who either are a foreign power or agent thereof or have been or will be in contact with a foreign power or agent. Although the consumer records of another person, such as a relative or friend of an agent of a foreign power, or identifying information respecting a relative or friend of a person in contact with an agent of a foreign power, may be of interest to FBI

counterintelligence investigators, they are not subject to access under paragraphs 608(b)(1) and 608(b)(2).

It is not the Committee's intent to require any credit reporting agency to gather credit or identifying information on a person for the purpose of fulfilling an FBI request under paragraphs 608(b)(1) and 608(b)(2). A credit reporting agency's obligation under these provisions is to provide information responsible to the FBI's request that the credit reporting agency already has in its possession.

Paragraph 608(b)(3) provides that no consumer reporting agency or officer, employee, or agent of such institution shall disclose to any person, other than those officers, employees or agents of such institution necessary to fulfill the requirement to disclose information to the FBI under subsection 608(b), that the FBI has sought or obtained a consumer report or identifying information respecting any consumer under paragraphs 608(b)(1) or 608(b)(2), nor shall such agency, officer, employee, or agent include in any consumer report any information that would indicate that the FBI has sought or obtained such a consumer report or identifying information. The prohibition against including such information in a consumer report is intended to clarify the obligations of the consumer reporting agencies. It is not intended to preclude employees of consumer reporting agencies from complying with company regulations or policies concerning the internal reporting of information, nor to preclude their complying with a subpoena for such information issued pursuant to appropriate legal authority.

Paragraph 608(b)(3) departs from the parallel provision of the RFPA by clarifying that disclosure is permitted within the contacted institution to the extent necessary to fulfill the FBI request. The Committee has not concluded, or otherwise taken a position whether, disclosure for such purpose would be forbidden by the RFPA; indeed, practicalities would dictate that the RFPA provision not be interpreted to exclude such disclosure. However, the Committee believes that clarification of the obligation for purposes of the FCRA is desirable.

Paragraph 608(b)(4) authorizes the FBI, subject to the availability of appropriations, to pay to the consumer reporting agency assembling or providing credit records a fee in accordance with FCRA procedures for reimbursement for costs reasonably necessary and which have been directly incurred in searching for, reproducing, or transporting books, papers, records, or other data required or requested to be produced under subsection 608(b). The FBI informs the Committee that such reports are commercially available for approximately $7 to $25 and that the FBI could expect to pay fees in approximately that range. FBI officials have advised the Committee that the costs of such reports would be easily recouped from the savings afforded by the reduced need for other investigative techniques aimed at obtaining the same information.

Paragraph 608(b)(5) prohibits the FBI from disseminating information obtained pursuant to subsection 608(b) outside the FBI, except to the Department of Justice or as may be necessary for the conduct of a foreign counterintelligence investigation. This latter phrase is in particular intended to allow for dissemination of information concerning military service personnel subject to the Uniform Code of Military Justice, to appropriate investigative authori-

ties in the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation with the FBI.

Paragraph 608(b)(6) provides that nothing in subsection 608(b) shall be construed to prohibit information from being furnished by the FBI pursuant to a subpoena or court order, or in connection with a judicial or administrative proceeding to enforce the provisions of the FCRA. The paragraph further provides that nothing in subsection 608(b) shall be construed to authorize or permit the withholding of information from the Congress.

Paragraph 608(b)(7) provides that on an annual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all requests made pursuant to paragraphs 608(b)(1) and 608(b)(2).

Similar reports are required to be submitted to the intelligence committees on: (1) use of the FBI's mandatory access provision of the RFPA by section 3414(a)(5)(C) of title 15, United States Code; and (2) use of the FBI's counterintelligence authority, under the Electronic Communications Privacy Act of 1986, to access telephone subscriber and toll billing information, by section 2709(e) of title 18, United States Code. The Committee expects the reports required by FCRA paragraph 608(b)(7) to match the level of detail included in these reports, i.e., a breakdown by quarter, by number of requests, by number of persons or organizations subject to requests, and by U.S. persons and organizations and non-U.S. persons and organizations.

Paragraphs 608(b)(8) through 608(b)(11) parallel the enforcement provisions of the Right to Financial Privacy Act, 12 U.S.C. 3417 and 3418.

Paragraph 608(b)(8) establishes civil penalties for access or disclosure by an agency or department of the United States in violation of subsection 608(b). Damages, costs, reasonable attorney's fees, as determined by the court, and a $100 fine would be awarded to the person to whom the consumer reports related in the event of a violation.

Paragraph 608(b)(9) provides that any credit reporting institution or agent or employee thereof making a disclosure of credit records in good-faith reliance upon a certificate by the FBI pursuant to the provisions of subsection 608(b) shall not be liable to any person for such disclosure under title 15, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

Paragraph 608(b)(10) provides that the remedies and sanctions set forth in subsection 608(b) shall be the only judicial remedies and sanctions for violations of the subsection.

Paragraph 608(b)(11) provides that, in addition to any other remedy contained in subsection 608(b), injunctive relief shall be available to require that the procedures of the subsection are complied with and that in the event of any successful action, costs together with reasonable attorney's fees, as determined by the court, may be recovered.

Section 5

Section 5 amends section 3071 of title 18, United States Code, to provide the Attorney General with discretionary authority to pay rewards for information leading to the arrest or conviction of persons for espionage against the United States or leading to the prevention or frustration of such acts.

Subsection (a) renumbers the existing provisions of section 3071, which provides discretionary authority for the Attorney General to pay rewards for information leading to the arrest or conviction of persons for acts of terrorism against the United States, as subsection (a) of section 3071, and adds a new subsection (b) to this section.

The new subsection (b) provides that, with respect to acts of espionage involving or directed at the United States, the Attorney General may reward any individual who furnishes information in any of three categories: (1) information leading to the arrest or conviction in any country of an individual or individuals for commission of an act of espionage against the United States; (2) information leading to the arrest or conviction of an individual or individuals in similar circumstances for conspiring or attempting to commit an act of espionage against the United States; and (3) information leading to the prevention or frustration of an act of espionage against the United States.

Under 18 U.S.C. 3071, the Attorney General can pay a reward of up to $500,000 for such information.

Subsection (b) amends the list of definitions in 18 U.S.C. 3077 to define the term "act of espionage" as an activity that is a violation of section 793, 794, or 798 of title 18, or section 783(b) of title 50, United States Code.

Subsection (c) contains a clerical amendment to the table of chapters in title 18, United States Code.

Section 6

Section 6 amends chapter 211 of title 18 of the United States Code by adding a new section 3239 to establish jurisdiction in certain U.S. federal courts to try cases involving violations of the espionage laws where the alleged misconduct takes place outside the United States.

Specifically, section 6 grants jurisdiction to the U.S. District Court for the District of Columbia and such other federal courts authorized by law to try cases involving a violation of section 793, 784, 798, 952, or 1030(a)(1) of title 18; section 601 of the National Security Act of 1947; or subsection (b) or (c) of the Subversive Activities Control Act of 1950, which were begun or committed upon the high seas or elsewhere out of the jurisdiction of any particular state or district.

Section 7

Section 7 amends several espionage statutes in order to ensure consistency among these statutes in terms of the application of criminal forfeiture provisions.

Subsections 7(a) and 7(c) amend section 798 of title 18, United States Code, and section 783 of title 50, United States Code, respectively, to provide the same criminal forfeiture provisions as

apply to violations of sections 793 and 794 of title 18, as amended by this section.

Under existing law, persons convicted of violating section 793 or 794 of title 18, United States Code, forfeit to the United States any property constituting, or derived from, any proceeds of espionage activities, as well as any property used, or intended to be used, to commit or facilitate the commission of espionage. In addition, the provisions of subsections (b), (c), and (e) through (o) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (pertaining to the ability of the Government to obtain the proceeds of illicit narcotics trafficking from third parties) are made available to the Government in espionage cases.

When the subsections of section 413 were renumbered by congressional action in 1986, the corresponding subsections in sections 793 and 794 of title 18 were not renumbered at the same time. As a consequence, one of the key subsections of section 413—subsection (p), which permits the Government, in cases where it can be shown that the defendant has deliberately placed the proceeds of narcotics trafficking beyond the jurisdiction of U.S. courts, to substitute other property of the defendant—appeared to have been eliminated insofar as its use in espionage cases were concerned. The Committee believes this was an oversight, and not what Congress intended. Section 7 corrects this error in sections 793 and 794, and applies the same procedures to violations of section 798 of title 18, United States Code, and to section 783 of title 50, United States Code.

Section 8

Section 8 amends 5 U.S.C. 8312 to add a new subsection (d) which provides that for purposes of section 8312, which sets forth criminal offenses a conviction for which may result in the termination of an annuity or retired pay of a federal employee, an offense is established if the Attorney General certifies to the agency administering the annuity or retired pay that—

(1) the individual has been convicted by an impartial court of appropriate jurisdiction within a foreign country in circumstances in which the conduct violates the provisions of law enumerated in subsections (b)(1) and (c)(1) of section 8312, or would violate such provisions had such conduct occurred within the United States, and that such conviction is not being appealed or that the final action has been taken on such appeal within the foreign country concerned;

(2) that such conviction was obtained in accordance with procedures that afforded the defendant due process rights comparable to those provided by the U.S. Constitution, and such conviction was based upon evidence that would have been admissible in U.S. courts; and

(3) that such conviction occurred after the effective date of the subsection.

Section 9

Section 9 amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to add a new title III establishing statutory procedures

for the approval and conduct of physical searches within the United States for foreign intelligence purposes.

Subsection 9(a) redesignates the existing title III as title IV and adds a new title III entitled "Physical Searches within the United States for Foreign Intelligence Purposes." A section-by-section analysis of the new title III provisions follows. To the extent that these new provisions are the same as comparable provisions for electronic surveillance in title I of the FISA, the following analysis restates much of the legislative history pertaining to such provisions as it applies to physical searches for foreign intelligence purposes.

Authorization of physical searches for foreign intelligence purposes

Section 301(a) authorizes submission of applications to the Foreign Intelligence Surveillance Court for an order approving a physical search in the United States, for the purpose of collecting foreign intelligence information, of the premises, property, information or material of a foreign power or an agent of a foreign power as defined in section 101 of the Act. Applications may be submitted only if the President has, by prior written authorization, empowered the Attorney General to approve the submission. This section does not require the President to authorize each specific application. The President may authorize the Attorney General generally to seek applications under this title or upon such terms and conditions as the President wishes, so long as the terms and conditions are consistent with this title.

Subsection (a) also authorizes a judge to whom an application is made to grant an order for physical search in the United States, for the purpose of collecting foreign intelligence information, of the specified premises, property, information or material, "notwithstanding any other law." The "notwithstanding any other law" language is intended to extend as well to any treaty obligations that might otherwise conflict with this law. The "notwithstanding any other law" wording also deals with the contention that 28 U.S.C. 1251 would prevent the Foreign Intelligence Surveillance Court from approving a physical search pursuant to this title.

Section 301(b) provides that the Foreign Intelligence Surveillance Court, as defined in section 309(3), shall have jurisdiction to hear applications for and grant orders approving physical search for the purpose of obtaining foreign intelligence anywhere within the United States under the procedures set forth in this title. No judge shall hear the same application which has been denied previously by another judge. Subsection (b) also provides that, if any judge denies an application for an order authorizing a physical search under this Act, such judge shall provide immediately for the record a written statement of each reason for that decision. On motion of the United States, the record shall be transmitted, under seal, to the Court of Review, established by section 103(b) of the Act. As with title I, this provision is intended to make clear that if the Government desires to pursue an application after a denial, it must seek review in the special court of review; it cannot apply to another judge of the Foreign Intelligence Surveillance Court. Obviously, where one judge has asked for additional information before approving an application, and that judge is unavailable when the Government comes forward with such additional information, the

Government may seek approval from another judge. It would, however, have to inform the second judge about the first application.

The Committee intends that, as under title I, the judges of the Foreign Intelligence Surveillance Court should have an opportunity to examine, when appropriate, the applications, orders, and statements of reasons for decisions in other cases.

Section 301(c) provides that the Court of Review shall have jurisdiction to review the denial of any application made under this title. 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.

Subsection 301(d) provides that judicial proceedings under this title shall be concluded as expeditiously as possible. The record of proceedings under this title, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Director of Central Intelligence. The Committee intends that such measures shall be the same as those established pursuant to title I and thus shall include such document, physical, personnel, or communications security measures as are necessary to protect information concerning proceedings under this title from unauthorized disclosure. As under title I, such measures may also include the use of secure premises provided by the Executive branch to hear an application and the employment of Executive branch personnel to provide clerical and administrative assistance.

Application for an order

Section 302(a) specifies what information must be included in the application for a court order. Applications must be made by a Federal officer in writing under oath or affirmation. If the officer making the application is unable to verify the accuracy of the information or representations upon which the application is based, the application should include affidavits by other officers who are able to provide such personal verification. Thus, for example, if the applicant should be an attorney in the Department of Justice who had not personally gathered the information contained in the application, it would be necessary that the application also contain an affidavit by an officer personally attesting to the status and reliability of any informants or other covert sources of information. By this means the source of all information contained in the applications and its accuracy will have been sworn to by a named official of the U.S. Government and a chain of responsibility established for judicial review.

Each application must be approved by the Attorney General, who may grant such approval if he or she finds that the criteria and requirements set forth in this title have been satisfied. The Attorney General's written approval must indicate his or her belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause to believe that the target is a foreign power or an agent of a foreign power, that the premises

or property to be searched contains foreign intelligence information, and that the premises or property to be searched is owned, used, possessed by or is in transit to or from a foreign power or an agent of a foreign power, as well as his or her belief that all other statutory criteria have been met.

Paragraph (1) of subsection (a) requires that the application include the identity of the Federal officer making the application.

Paragraph (2) requires that the application contain evidence of the authority to make this application. This would consist, under the current Executive order, of the Presidential authorization to the Attorney general and the Attorney General's approval of the particular application.

Paragraph (3) requires the application to include the identity, if known, of the target of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered. Thus, if the Government knows the identity of the target of the search, it is required to identify the target. The target may be an individual or an entity.

The word "target" is nowhere defined in this title, although it is a key term, because the standards to be applied differ depending on who or what is targeted. The Committee intends that the target of a physical search be the individual or entity about whom or from whom information is sought. In most cases this would be the individual or entity who owns, uses, or possesses the premises or property to be searched. In some cases, however, it would be the individual or entity to or from whom property is in transit.

An individual cannot be a foreign power, only an agent of a foreign power. Therefore, if the search is to be directed at an individual about whom information is sought, that individual is the target and must be shown to be an "agent of a foreign power." Where two or three individuals are associated with one another, it might be argued that they are an "association" or an "entity," which, if the proper showing is made, could be considered a "foreign power." (This would especially be true if the individuals engaged in "international terrorism" and thereby might be a group engaged in international terrorism, which is a defined "foreign power.") This does not mean, however, that property of each of these individuals can then be individually searched merely upon a showing that together they are a "foreign power." Rather, to search the property of each individual would require a showing that each was an "agent of a foreign power."

Often, however, associations or entities will act in a "corporate" capacity, as distinguished from the act of an individual in the association or entity. For example, corporations own or lease property, enter into contracts, and otherwise act as an entity distinct from the individuals therein. The fact that an individual officer or employee, acting in his or her official capacity, may sign the deed, lease, or contract on behalf of the corporation does not vitiate the fact that it is the corporation rather than the individual who is acting. Thus, it is possible to target a "foreign power" in such circumstances. In addition, it will be possible under this title to target a "foreign power" in certain rare cases where the facility targeted, while owned, used, or possessed by the entity, is in fact dedicated

to the use of one particular member of the entity, for instance, where each officer is assigned his or her own office. However, in order to justify the target as a "foreign power" rather than as an "agent of a foreign power," the information sought must be concerning the entity, not the individual.

The judge in considering the application, wherever the Government claims the target is a "foreign power," and especially where U.S. persons are officers or employees of the "foreign power," must scrutinize the description of the information sought, and the property or premises to be searched; see section 402(a)(3), *infra*, to determine whether the target is really the "foreign power" rather than an "agent of a foreign power." The judge must also closely scrutinize the minimization procedures to assure that where the target is a "foreign power," the individual U.S. persons who may be members or employees of the power are properly protected.

In addition, paragraph (3) requires that the application contain a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered. The description should be as specific as possible and should detail what type of premises or property is likely to be searched and what types of information, material, or property are likely to be seized, reproduced, or altered. Such specifics are necessary if the judge is meaningfully to assess the sufficiency and appropriateness of the minimization procedures.

Paragraph (4) requires a statement of the facts and circumstances justifying the applicant's belief that the target of the physical search is a foreign power or an agent of a foreign power, that the premises or property to be searched contains foreign intelligence information, and that the premises or property to be searched or owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power.

Paragraph (5) requires a statement of the proposed minimization procedures. The statement of procedures required under this paragraph should be full and complete and normally subject to close judicial review. It is the intention of the Committee that minimization procedures be as uniform as possible for similar physical searches. The application of uniform procedures to identical searches will result in a more consistent implementation of the procedures, improved capability to assure compliance with the procedures, and ultimately a higher level of protection for the rights of U.S. persons.

Paragraph (6) requires the application to contain a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted. This statement should be sufficiently detailed so as to state clearly what foreign intelligence the Government seeks. A simple assertion that "foreign intelligence information" is sought will not suffice. There must be an explanation of what specific foreign intelligence information is sought. This requirement is designed to prevent physical searches of one target when the true purpose of the search is to gather information about another target for other than foreign intelligence purposes. It is also designed to make explicit that the sole purpose of such physical search is to secure "foreign intelligence information," as defined, and not to obtain some other type of information. The

statement should also be as detailed and specific as possible in light of the need for the judge in his or her order to specify the manner in which the physical search is to be conducted.

Paragraph (7) requires that each application include a certification or certifications by the Assistant to the President for National Security Affairs or by an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate. Such certification or certifications must include statements—

That the certifying official deems the information sought to be foreign intelligence information;

That the purpose of the search is to obtain foreign intelligence information;

That such information cannot reasonably be obtained by normal investigative techniques;

That designate the type of foreign intelligence information being sought according to the categories described in section 101(e) of the Act; and

Explaining the basis for the certification that such information cannot be obtained by normal investigative techniques and the certification that the foreign intelligence information being sought falls within a category or categories described in section 101(e) of the Act.

This paragraph contemplates that such certifications shall be in writing and signed by an official designated pursuant to this paragraph. Such certifications shall be as detailed and specific as possible.

Paragraph (8) requires a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

Section 302(b) provides that the Attorney General may require any other affidavit or certification from any other officer in connection with the application. This section is intended to permit the Attorney General such additional latitude as may be necessary in order to consider applications submitted pursuant to this title.

Section 302(c) provides that the judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 303. Such additional proffers would, of course, be made part of the record and would be subject to the security safeguards applied to the application and order.

Issuance of an order

Section 303(a) specifies the findings the judge must make before granting an *ex parte* order approving physical search under this title. While the issuance of an order is mandatory if the judge finds that all the requirements of this section are met, the judge has the discretion to modify the order sought, for example, with regard to the period of authorization or the minimization procedures to be followed. Modifications in the minimization procedures should take

into account the impact of inconsistent procedures on successful implementation.

Paragraph (1) of this subsection requires the judge to find that the President has authorized the Attorney General to approve such applications.

Paragraph (2) requires the judge to find that the application has been made by a Federal officer and that the Attorney General has approved the application being submitted.

Paragraph (3) requires a finding that there is "probable cause" to believe that the target of the physical search is a foreign power or an agent of a foreign power, that the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power, and that physical search of such premises or property can reasonably be expected to yield foreign intelligence information which cannot reasonably be obtained by normal investigative means.

In determining whether "probable cause" exists under this section, the court should keep in mind that this standard is not the ordinary "probable cause" that a crime is being committed, applicable to searches and seizures for law enforcement purposes. Where a U.S. person is believed to be an "agent of a foreign power," for example, there must be "probable cause" to believe that the person is engaged in certain activities, but the criminality of these activities need not always be demonstrated to the same degree. The key words—"involve or may involve"—indicate that the ordinary criminal probable cause standard does not apply with respect to the showing of criminality. For example, the activity identified by the Government may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, this would suffice. It is not intended that the Government show probable cause as to each and every element of the crime likely to be committed.

The determination by the court as to whether there is probable cause that the person is engaging in certain activities or, for example, whether an entity is directed and controlled by a foreign government or governments, should include consideration of the same aspects of the reliability of the Government's information as is made in the ordinary criminal context—for example, the reliability of any informant, the circumstances of the informant's knowledge, or the age of the information relied upon. On the other hand, all of the same strictures with respect to these matters which have developed in the criminal context may not be appropriate in the foreign intelligence context. That is, in the criminal context certain "rules" have developed or may develop for judging reliability of information. See, for example, *Spinelli* v. *United States,* 393 U.S. 410 (1969). It is not the Committee's intention that these "rules" necessarily be applied to consideration of probable cause under this title. Rather it is the Committee's intent that in judging the reliability of the information presented by the Government, the court look to the totality of the information and consider its reliability on a case-by-case basis.

In addition, in order to find "probable cause" to believe the subject of the surveillance is an "agent of a foreign power," as defined in section 101(b) of the Act, the judge must, of course, find that

each and every element of that status exists. For example, if a U.S. citizen or resident alien is alleged to be acting on behalf of a foreign entity, the judge must first find probable cause to believe that the entity is a "foreign power" as defined in section 101(a) of the Act. There must also be probable cause to believe the person is acting for or on behalf of that foreign power and probable cause to believe that the efforts undertaken by the person on behalf of the foreign power constitute sabotage, international terrorism, or clandestine intelligence activities.

Similar findings of probable cause are required for each element necessary to establish that a U.S. citizen is conspiring with or aiding and abetting someone engaged in sabotage, international terrorism, or clandestine intelligence activities.

The proviso in paragraph (3)(A) states that no U.S. 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. This provision is intended to reinforce the intent of the Committee that lawful political activities should never be the sole basis for a finding of probable cause to believe that a U.S. person is a foreign power or an agent of a foreign power. For example, the advocacy of violence falling short of incitement is protected by the first amendment, under the Supreme Court's decision in *Brandenburg* v. *Ohio,* 395 U.S. 444 (1969). Therefore, the pure advocacy of the commission of terrorist acts would not, in and of itself, be sufficient to establish probable cause that an individual or group is preparing for the commission of such acts. However, one cannot cloak oneself in first amendment immunity by advocacy, where one is engaged in clandestine intelligence activities, terrorism, or sabotage.

Paragraphs (3) (B) and (C) require the judge to find probable cause to believe that the premises or property to be searched is owned, used, possessed by, or in transit to or from a foreign power or an agent of a foreign power and that physical search of such premises or property can reasonably be expected to yield foreign intelligence information which cannot reasonably be obtained by normal investigative means.

Paragraph (4) requires the judge to find that the procedures described in the application to minimize the acquisition and retention, and prohibit dissemination, of certain information relating to U.S. persons fit the definition of minimization procedures in this title. The Committee contemplates that the court would give these procedures most careful consideration. If the court does not believe they will be effective, the procedures should be modified.

Paragraph (5) requires that the judge find that the application contains the statements required by section 302. If the statements do not conform to the requirements of section 302, they can and must be rejected by the court.

Section 303(b) specifies what the order approving the physical search must contain. Paragraph (1)(A) requires that it must specify the identity, if known, or a description of the target of the physical search. Paragraph (1)(B) provides that the order must also specify the nature and location of each of the premises or property to be searched; and paragraph (1)(C) provides that the order must specify the type of information, material or property to be seized, al-

tered, or reproduced. Paragraph (1)(D) provides that the order must also include a statement of the manner in which the search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search. These requirements are designed in light of the Fourth Amendment's requirements that warrants describe with particularity and specificity the person, place, and objects to be searched and seized. Finally, paragraph (1)(E) provides that the order must specify the time period during which physical searches are approved.

The Committee intends that an order may authorize more than one search of separate premises, or more than one search of the same premises so long as such searches occur within the time periods authorized under the order. Thus, if an authorized physical search is undertaken but terminated without achieving its purpose, a second physical search of the same premises to achieve the same purpose may be instituted so long as such search has been specifically authorized by the order and occurs within the time period specified in the order.

Paragraph (2) of section 303(b) details what the court directs in the order. The order must direct that minimization procedures will be followed. The order may also direct that a landlord, custodian, or other specified person furnish information, facilities or assistance necessary to accomplish the search successfully and in secrecy and with a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search. If this is done, the court shall direct that the person rendering the assistance maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the search or the aid furnished that such person wishes to retain. The order presented to the person rendering assistance need not be the entire order approved by the judge under this title. Rather, only that portion of the order described in section 303(b)(2) (B)–(C), signed by the judge, need be given to the specified person. This portion of the order should specify the person directed to give assistance, the nature of the assistance required, and the period of time during which such assistance is authorized. Finally, paragraph (2)(E) requires that the order direct that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search. This report may be made to a judge other than the judge who granted the order approving the search.

Section 303(c)(1) requires that an order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that if the physical search is targeted against a foreign power as defined in section 101(a) (1), (2), or (3) of FISA, an order shall approve such search for the period specified in the application, or for one year, whichever is less. The comparable periods in title I are the same.

Section 303(c)(2) provides that extensions of an order issued under this title may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that

an extension of an order under this Act for a physical search targeted against a foreign power as defined in section 101(a) (5) and (6), or against a foreign power, as defined in section 101(a)(4), which is not a United States person, may be for a period not to exceed a year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period. Comparable time periods are permitted by title I for extensions of electronic surveillances of the foreign powers in these categories.

Section 303(c)(3) provides that at or before the end of the period of time for which a physical search is approved by an order or extension, or at any time after a physical search has been carried out, the judge who approved the order or extension or the judge to whom the return has been made may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated. This provision is not intended to require that the judge assess such compliance, nor is it intended to limit such assessments to any particular intervals. However, it is useful to spell out the judge's authority explicitly so that there will be no doubt that a judge may review the manner in which information about U.S. persons is being handled at any time after an order approving such search has been issued.

Section 303(d) permits the Attorney General to approve physical searches for foreign intelligence purposes in emergency situations. The requirements set forth in this section are comparable to those provisions in title I of the Act pertaining to emergency electronic surveillances.

Subsection (d)(1) authorizes the Attorney General to authorize the execution of an emergency physical search if the Attorney General determines that an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an order authorizing such search can with due diligence be obtained, and the factual basis for issuance of an order under this title to approve such a search exists, and if the Attorney General or the Attorney General's designee informs a judge having jurisdiction under section 103 of the Act at the time of authorization that the decision has been made to execute an emergency search and an application is made to that judge as soon as practicable but not more than 24 hours after the emergency search is authorized by the Attorney General.

Subsection (d)(2) provides that the Attorney General shall require that the minimization procedures shall be followed whenever an emergency search is authorized pursuant to this section.

Subsection (d)(3) provides that in the absence of a judicial order approving such search, an emergency search authorized by the Attorney General shall terminate when the information sought is obtained, or when the application for the order is denied; or 24 hours from the time of the authorization, whichever is earlier.

Subsection (d)(4) provides that where an application or a physical search is denied, or in any other case where a physical search is terminated and no order is issued approving the search, no information obtained or evidence derived from such search shall be received in evidence or otherwise disclosed in any judicial or adminis-

trative proceeding, and no information concerning any United States person acquired from such search shall be subsequently 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 301.

Subsection 303(e) provides that applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the application. This is identical to the requirement in title I, and the purpose is to assure accountability.

Use of information

Section 304 places additional constraints on Government use of information obtained from physical search under this title and establishes detailed procedures under which information may be received in evidence, suppressed, or discovered. With respect to the use of information in legal proceedings, notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any motions concerning evidence derived from physical search. In addition, the Attorney General should at all times be able to assess whether and to what extent the information made available by the Government to a State or local authority will be used.

Subsection (a) requires that information concerning U.S. persons acquired from physical search pursuant to this title may be used and disclosed by Federal officers and employees, without the consent of the U.S. person, only in accordance with the minimization procedures defined in section 309(4). This provision ensures that the use of such information is carefully restricted to actual foreign intelligence or law enforcement purposes. No information (whether or not it concerns a U.S. person) acquired from a physical search pursuant to this title may be used or disclosed except for lawful purposes. This is to ensure that information concerning foreign visitors and other non-U.S. persons, the use of which is not restricted to foreign intelligence or law enforcement purposes, is not used for illegal purposes.

There is no specific restriction in this title regarding to whom Federal officers may disclose information concerning U.S. persons acquired pursuant to this title, although specific minimization procedures might require specific restrictions in particular cases. First, the Committee believes that dissemination should be permitted to State and local law enforcement officials. If Federal agents conducting a physical search authorized under this title were to acquire information relating to a violation of State criminal law, such as homicide, the agents could hardly be expected to conceal such information from the appropriate local officials. There will be an appropriate weighing of criminal law enforcement needs against possible harm to national security from the disclosure. Second, the Committee can conceive of situations where disclosure should be made outside of Government channels. For example, Federal agents may learn of a terrorist plot to kidnap a business executive. Certainly in such cases they should be permitted to disclose such information

to the executive and his or her company in order to provide for the executive's security.

Finally, the Committee believes that foreign intelligence information relating to crimes, espionage activities, or the acts and intentions of foreign powers may, in some circumstances, be appropriately disseminated to cooperating intelligence services of other nations. So long as all the procedures of this title are followed by the Federal officers, including minimization and the limitations on dissemination, this cooperative relationship should not be terminated by a blanket prohibition on dissemination to foreign intelligence services. The Committee wishes to stress, however, that any such dissemination be reviewed carefully to ensure that there is a sufficient reason why disclosure of information to foreign intelligence services is in the interests of the United States.

Disclosure, in compelling circumstances, to local officials for the purpose of enforcing the criminal law, to the targets of clandestine intelligence activity or planned violence, or to foreign intelligence services under the circumstances described above is generally the only exception to the rule that dissemination should be limited to Federal officials.

Subsection (b) requires that any disclosure of information for law enforcement purposes be accompanied by a statement that such evidence, or any information derived therefrom, may be used in a criminal proceeding only with the advance authorization of the Attorney General. This provision is designed to eliminate circumstances in which a local prosecutor has no knowledge that evidence was obtained through a foreign intelligence search. In granting approval of the use of evidence the Attorney General would alert the prosecutor to the search and the prosecutor, in turn, could alert the court in accordance with subsection (c) or (d).

Subsections (c) through (i) set forth the procedures under which information acquired by means of physical search under this title may be received in evidence or otherwise used or disclosed in any trial, hearing or other Federal or State proceeding. Although the primary purpose of physical search conducted pursuant to this title is not the gathering of criminal evidence, it is contemplated that such evidence will be acquired and these subsections establish the procedural mechanisms by which such information may be used in formal proceedings. Notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any notions concerning evidence derived from physical search under this title.

At the outset the Committee recognizes that nothing in these subsections abrogates the rights afforded a criminal defendant under *Brady* v. *Maryland,* 373 U.S. 83 (1963), and the Jencks Act, 18 United States Code, Section 3500 *et seq.* These legal principles inhere in any such proceedings and are wholly consistent with the procedures detailed here. Furthermore, nothing contained in this section is intended to alter the traditional principle that the Government cannot use material against a criminal defendant and then withhold from him such material at trial. *United States* v. *Andolschek,* 142 F. 2d 503 (2nd. Cir. 1944).

Subsection (c) states that whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding before any court, department, officer, agen-

cy, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search of the premises or property of that aggrieved person pursuant to the authority of this title, the United States 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 United States intends to so disclose or so use such information. This provision applies to information acquired from a physical search under this title or any fruits thereof.

Subsection (d) places the same requirements upon the States and their political subdivisions, and also requires notice to the Attorney General. The Attorney General should at all times be able to assess whether and to what extent the use of information made available by the Government to a State or local authority may be used.

Subsection (e) provides a separate statutory mechanism by which an aggrieved person against whom evidence derived or obtained from a physical search under this title is to be or has been introduced or otherwise used or disclosed in any trial, hearing or proceeding may move to suppress the information acquired by physical search or evidence derived therefrom. The grounds for such a motion would be that (1) the information was unlawfully acquired, or (2) the search was not made in conformity with the order of authorization or approval. A motion under this subsection must be made before the trial, hearing, or proceeding unless there was no opportunity to make such a motion or the movant was not aware of the grounds for the motion. It should be noted that the term "aggrieved person," as defined in section 309(d), does not include those who are mentioned in documents obtained or copied in a physical search.

Subsection (f) states in detail the procedure the court shall follow when it receives a notification under subsection (c) or (d) or a suppression motion is filed under subsection (e). This procedure applies, for example, whenever an individual makes a motion pursuant to subsection (d) or any other statute or rule of the United States (e.g., Rule 12 of the Federal Rules of Criminal Procedure) to discover, obtain, or suppress evidence or information obtained or derived from physical search conducted pursuant to this title. Although a number of different procedures might be used to attack the legality of the search, it is this procedure "notwithstanding any other law" that must be used to resolve the question. The procedures set out in subsection (f) apply whatever the underlying rule or statute referred to in the motion. This is necessary to prevent the carefully drawn procedures in subsection (f) from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

The special procedures in subsection (f) cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security of the United States. If no such assertion is made, it is envisioned that mandatory disclosure of the application and order, and discretionary disclosure of other surveillance materials, would be available to the defendant. When the procedure is so triggered, however, the Gov-

ernment must make available to the court a copy of the court order and accompanying application upon which the physical search was based.

The court must then conduct an *ex parte, in camera* inspection of these materials as well as any other documents relating to the search which the Government may be ordered to provide, to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. The subsection further provides that in making such a determination, the court may order disclosed to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

The procedures set forth in subsection (f) are intended to strike a reasonable balance between an entirely *in camera* proceeding which might adversely affect the defendant's ability to defend himself or herself, and mandatory disclosure, which might occasionally result in the revelation of sensitive foreign intelligence information. The decision whether it is necessary to order disclosure to a person is for the court to make after reviewing the underlying documentation and determining its volume, scope, and complexity. In some cases, the court will likely be able to determine the legality of the search without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be targeted, or search records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, it is contemplated that the court will likely decide to order disclosure to the defendant, in whole or in part, since such disclosure "is necessary to make an accurate determination of the legality of the physical search."

Cases may arise, of course, where the court believes that disclosure is necessary to make an accurate determination of legality, but the Government argues that to do so, even given the court's broad discretionary power to excise certain sensitive portions, would damage the national security. In such situations the Government must choose—either disclose the material or forego the use of the search-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed.

Subsection (g) states that if the United States district court pursuant to subsection (f) determines that the physical search 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 the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search 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.

The general phrase "in accordance with the requirements of law" has been chosen to deal with the problem of what procedures are to be followed in those cases where the trial court determines that

the surveillance was unlawfully authorized or conducted. The evidence obtained would not, of course, be admissible during the trial. But beyond this, in the case of an illegal surveillance, the Government is constitutionally mandated to surrender to the defendant all the records of the surveillance in its possession in order for the defendant to make an intelligent motion on the question of taint. The Supreme Court in *Alderman* v. *United States,* 394 U.S. 165 (1968), held that, once a defendant claiming evidence against him was the fruit of unconstitutional electronic surveillance has established the illegality of such surveillance (and his "standing" to object), he must be given confidential materials in the Government's files to assist him in establishing the existence of "taint." The Court rejected the Government's contention that the trial court could be permitted to screen the files *in camera* and give the defendant only material which was "arguably relevant" to his claim, saying such screening would be sufficiently subject to error to interfere with the effectiveness of adversary litigation of the question of "taint." The Supreme Court refused to reconsider the *Alderman* rule and, in fact, reasserted its validity in its *Keith* decision. (*United States* v. *Alderman,* supra, at 393.)

When the court determines that the physical search was lawfully authorized and conducted, it would, of course, deny any motion to suppress.

Subsection (h) states that orders granting motions or requests under subsection (g), decisions under this section that a physical search 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 the physical search 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. It is intended that all orders regarding legality and disclosure shall be final and binding only where the rulings are against the Government.

Subsection (i) states that if an emergency search is authorized pursuant to section 303(d) and a subsequent order approving the search is not obtained, the judge shall cause to be served on any U.S. person who was the subject of such search a notice, noting the fact of the application; the period authorized for the search; and whether during the period information was or was not obtained. On an *ex parte* showing of good cause to the judge, service of the notice required by this subsection may be postponed for up to 90 days. On a further *ex parte* showing of good cause, the court shall forego ordering the serving of the notice required by this subsection. Comparable provisions governing notice of emergency electronic surveillances are set forth in title I of the Act.

Congressional oversight

Section 305(a) provides that 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 physical searches conducted pursuant to this title.

In addition, on an annual basis the Attorney General shall provide to those committees a report setting forth with respect to the preceding calendar year: (a) the total number of applications made

for orders approving physical searches under this title; and (b) the total number of such orders either granted, modified, or denied. The comparable provision of title I requires a public report to the Administrative Office of the United States Courts. The reports concerning physical searches are to be submitted to the Committees, and my be classified, because the Justice Department has advised that the numbers may be so few as to reveal sensitive information concerning U.S. foreign counterintelligence activities. If this concern should be confirmed by experience under the Act, the Committees will consider appropriate alternative methods of informing the public concerning this practice consistent with the needs of national security.

Penalties

Section 306(a)(1) makes it a criminal offense for officers or employees of the United States to intentionally engage in physical search within the United States under color of law for the purpose of obtaining foreign intelligence information except as authorized by statute. Section 306(a)(2) makes it a criminal offense for officers or employees of the United States to intentionally disclose or use information obtained under color of law by physical search, knowing or having reason to know that the information was obtained through physical search not authorized by statute and conducted in the United States for the purpose of obtaining foreign intelligence information.

Section 306(b) provides an affirmative defense to a law enforcement or investigative officer that the officer engaged in such an activity for law enforcement purposes in the course of his official duties, and the physical search was authorized by and conducted pursuant to a search warrant or court order of a court or competent jurisdiction. Section 306(c) provides that the penalty for violation of subsection (a) is a fine of not more than $10,000 or imprisonment for not more than five years, or both. Section 306(d) makes clear that 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 when the offense was committed.

One of the important purposes of this title is to afford security to intelligence personnel so that if they act in accordance with the statute, they will be insulated from liability; it is not to afford them immunity when they intentionally violate the law. The word "intentionally" was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. The Government would have to prove beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation.

Civil liability

Section 307 imposes civil liability for violations of section 306, and authorizes an "aggrieved person," as defined in section 309(2), to recover actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater; punitive damages; and reasonable attorney's fees and other investigative and litigation costs reasonably incurred. Since the civil cause of action only arises in connection with a violation

of the criminal provision, the statutory defense does not have to be restated. Although included in the definition of "aggrieved person," foreign powers and non-U.S. persons who act in the United States as officers or employees of foreign powers or as members of international terrorist groups would be prohibited from bringing actions under section 307. Other foreign visitors, including those covered by section 101(b)(1)(B) of the definition of "agent of a foreign power," would have a cause of action under this provision. Those barred from the civil remedy will be primarily those persons who are themselves immune from criminal or civil liability because of their diplomatic status.

Authorization during time of war

Section 308 provides that the President, through the Attorney General, may, notwithstanding any other law, authorize physical searches without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress. A similar provision is made for electronic surveillance during time of war in title I.

Definitions

Section 309 provides definitions of terms used in this title.

Section 309(1) incorporates by reference the definitions used in title I of the Act pertaining to electronic surveillance. These include definitions of the terms "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State."

These definitions are crucial to the understanding and implementation of title III as well as title I. In particular, the definitions of "foreign power," "agent of a foreign power" and "United States person" set forth the categories of persons or entities which may be targeted for electronic surveillance and physical search under the Act. Depending upon the category into which such person or entity may fall, the approval authority and time periods prescribed by the Act for an electronic surveillance or a physical search will vary. The Committee intends that the entire legislative history of these terms, as set forth in the congressional reports pertaining to title I governing electronic surveillance, be applied to their use in title III pertaining to physical search. The legislative history of these provisions can be found in Senate Report 95–604 (Report of the Committee on Judiciary); Senate Report 95–701 (Report of the Select Committee on Intelligence); and House Report 95–1283 (Report of the Permanent Select Committee on Intelligence).

Sections 309 (2) through (5) provide definitions of other terms used in this title.

Section 309(2) of this title defines "aggrieved person" to mean a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search. As defined, the term is intended to be coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to physical search.

Section 309(3) of this title defines "Foreign Intelligence Surveillance Court" to mean the court established by section 103(a) of the Act, which provides that 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. Pursuant to section 103(d) of the Act, 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 first judges designated under subsection (a) were to be designated for terms of from one to seven years so that one term expired each year. As a result, there has been a regular annual rotation of at least one new judge onto the Foreign Intelligence Surveillance Court since 1979.

The legislative history of the FISA established the intent of Congress that the court shall sit continuously in the District of Columbia, that the designated judges shall serve by rotation determined by the Chief Justice, that they may be assigned to other judicial duties in the District of Columbia which are not inconsistent with their duties under this Act, and that more than one judge shall be available at all times to perform the duties required by this Act.

Section 309(4) defines "minimization procedures," with respect to physical search, in three paragraphs that are similar to the definition of this term in section 101(h) of the Act.

Paragraph (4)(A) defines "minimization procedures" as specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, 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.

The definition begins by stating that the minimization procedures must be specific procedures. This is intended to demonstrate that the definition is not itself a statement of the minimization procedures but rather a general statement of principle which will be given content by the specific procedures which will govern the actual searches. It is also intended to suggest that the actual procedures be as specific as practicable in light of the search technique and its purposes.

The definition then states that the procedures must be "reasonably designed in light of the purposes and technique of the particular physical search." It is recognized that minimization procedures may have to differ depending on the search technique. For instance, minimization with respect to searches of packages entrusted to couriers would not be comparable to searches involving entry of residential premises.

The definition of minimization speaks in terms of minimizing acquisition and retention and prohibiting dissemination.

The Committee recognizes that in some cases it may not be possible or reasonable to avoid acquiring irrelevant information in a physical search. It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be as strict as

for law enforcement searches. By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible and appropriate, as with copies of photographed or reproduced documents. In certain cases destruction might take place almost immediately, while in other cases the information might be retained for a reasonable time in order to determine whether it did indeed relate to one of the approved purposes. Procedures governing minimization—particularly how long information should be retained and how it should be destroyed once it is deemed irrelevant—are normally approved by the court and subject to judicial supervision.

The standard for dissemination is higher than for acquisition and retention, but the prohibition on dissemination should be reasonably designed to be consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. Information being held to determine its usefulness should not be disseminated until that determination was made (or would only be disseminated to those who could determine its usefulness). Even with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information. And, again, the judge, in approving the minimization procedures, could require specific restrictions on the retrieval of such information.

There are a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition. These may include, where appropriate, but are not limited to:

(A) destruction of unnecessary information acquired;

(B) provisions with respect to what may be filed and on what basis, what may be retrieved and on what basis, and what may be disseminated, to whom and on what basis;

(C) provision for the deletion of the identity of United States persons where not necessary to assess the importance of, or to understand the information;

(D) provisions relating to the proper authority in particular cases to approve the retention or dissemination of the identity of United States persons;

(E) provisions relating to internal review of the minimization process; and

(F) provisions relating to adequate accounting of information concerning United States persons used or disseminated.

Minimization, however, is not required with respect to all information which may be acquired by physical search. For example, publicly available, information need not be minimized. By publicly available, the Committee means information which in fact is generally available to the public. Such information can include generally published information or information in the public record which is generally available to the public, e.g., statements of incorporation on file in state offices. Also included would be trade names such as a Xerox copier, a Boeing 747, etc.

In addition, only information concerning a United States person need be minimized. This includes both documents written by a United States person and documents which are written by others

but which mention the United States person. The Supreme Court has held that persons have no constitutionally protected right of privacy with respect to what others say about them. See *Alderman* v. *United States*, 394 U.S. 195 (1968). Nevertheless, the Executive Branch in its own procedures has demonstrated that it can minimize retention and prohibit dissemination of such information consistent with legitimate foreign intelligence needs. The Committee notes, moreover, that documents, although written or owned by one person, may constitute a more accurate and authoritative record of another U.S. person's activities than would the typical communication. Recognizing the less substantial privacy interest in such information, however, the "reasonably designed" procedures may take account of the differences between information in which persons have a constitutionally protected interest and that in which they do not. Therefore, more flexibility in the procedures may be afforded with respect to information concerning U.S. persons obtained from documents written by others. Of course, information concerning U.S. persons may come in other circumstances where their privacy is invaded; in such situations the person whose property is searched has had his or her privacy interests invaded and minimization procedures are required.

Because minimization is only required with respect to information concerning U.S. persons, where materials seized or reproduced are encoded or otherwise not processed, so that the contents are unknown, there is no requirement to minimize the acquisition and retention, or to prohibit the dissemination, of such materials until their contents are known. Nevertheless, the minimization procedures can be structured to apply to other agencies of Government, so that if any agency different from the searching agency decodes or processes the materials, it could be required to minimize the retention and dissemination of information therein concerning U.S. persons.

It is recognized that writers of documents are unlikely to state that they are or are not U.S. persons. Intelligence officers and analysts therefore must use their judgment as to when the procedures apply. While not suggesting that the procedures require the following, as a general rule, persons in the United States might be presumed to be U.S. persons unless there is some reason to believe otherwise. The Committee does not intend or expect, however, that intelligence officers will destroy possibly meaningful information merely because there is a question whether a person is a U.S. person.

The definition states that minimization procedures must minimize acquisition and retention, and prohibit dissemination, of information subject to minimization "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

"Foreign intelligence information" is, of course, a defined term, and with respect to U.S. persons, it must be "necessary" to the listed security and foreign relations purposes. However, the definition of "minimization procedures" does not state that only "foreign intelligence information" can be acquired, retained, or disseminated. The Committee recognizes that bits and pieces of information, which taken together could not possibly be considered "necessary,"

may together or over time take on significance and become "necessary." Nothing in this definition is intended to forbid the retention or even limited dissemination of such bits and pieces before their full significance becomes apparent.

An example would be where the Government conducts a surreptitious entry to photograph papers and effects of a known spy, who is a U.S. person. It is "necessary" to identify anyone working with that spy in his or her network, for example, by providing information, or to whom the spy reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all the spy's contacts and acquaintances and movements. Among those contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities, and may have to be disseminated in order to determine their innocence. Where after a reasonable period of time, which may in fact be an extended period of time, there is no reason to believe such persons are involved in the clandestine intelligence activities, there should be some effort, for example, either to destroy the information concerning such persons, or to seal the file so that it is not normally available, or to make the file not retrievable by the name of the innocent person. It is recognized that the failure to gather further incriminating information concerning the contacts or acquaintances of the spy does not necessarily mean they are in fact innocent—instead, they may merely be very sophisticated and well-versed in their espionage tradecraft. Therefore, for an extended period it may be necessary to have information concerning such acquaintances, for an investigation of another spy may indicate the same acquaintance, which may justify more intensive scrutiny of the person, which then may result in breaking his or her cover.

One of the results of minimizing retention and dissemination under this title is that some information will be destroyed, retained in a non-identifiable manner, or sealed in a manner to prevent dissemination. Although there may be cases in which information acquired from a physical search for foreign intelligence purposes will be used as evidence of a crime, these cases are expected to be relatively few in number, unlike the case in searches in criminal investigations, the very purpose of which is to obtain evidence of criminal activity. In light of the relatively few cases in which information acquired under this allow the destruction of information that is not foreign intelligence information or evidence of criminal activity. This course will safeguard the privacy of individuals more effectively, insuring that irrelevant information will not be filed.

The definition of minimization procedures states that the Attorney General shall adopt appropriate procedures. In most cases, of course, these procedures will be reviewed and approved, modified, or disapproved by the judge approving the physical search. Experience under title I suggests the administrative need for minimization procedures to be as uniform as possible. This does not mean, however, that judges should not fully scrutinize proposed minimization procedures simply because the same procedures have been approved by another judge in another case. Not only might the earlier judge have overlooked something, but also it is critical to determine

at least that factors militating in favor of uniformity are not outweighed by other considerations. For instance, the Committee expects that minimization procedures for searches of the property of individuals would be more strict that those for searches of the property of foreign powers. If the judge believes a modification is called for, he or she should require it. If the Government finds the change unacceptable, it may, of course, appeal the decision to the special Court of Review.

Paragraph (B) of the definition requires that all minimization procedures contain a requirement that any information which is not foreign intelligence information as defined in section 101(e)(1) of the Act not be disseminated in a manner which identifies a United States person, without such person's consent, unless the identity is necessary to understand such foreign intelligence information or assess its importance. The purpose of this special dissemination standard is to protect United States persons from dissemination of information which identifies them in those areas where the Government's need for their identity is least established. The adjectival use of the name of a United States person entity, such as the brand name of a product, is not restricted by this provision because such information is publicly available.

Two exceptions are allowed to the prohibition on dissemination in paragraph (B). The first allows dissemination where a U.S. person's identity is "necessary to understand" foreign intelligence information. The person's identity must be needed to make the information fully intelligible. If the information can be understood without identifying the U.S. person, it should be disseminated that way. However, sometimes it might be difficult or impossible to make sense of the information without a U.S. person's to make sense of the information without a U.S. person's identity. The second exception allows dissemination where a U.S. person's identity is necessary to "assess [the] importance" of foreign intelligence information. The word "importance" means important in terms of the interests set out in the definition of foreign intelligence information. "Necessary" does not mean that the identity must be essential to understand the information or assess its importance. The word necessary requires that a knowledgeable intelligence analyst make a determination that the identity will contribute in a meaningful way to the ability of the recipient of the information to understand the information or assess its importance.

Paragraph (C) of the definition allows retention and dissemination of information which 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. As noted above, *see* section 101(e) of the Act, evidence of certain crimes like espionage would itself constitute "foreign intelligence information," as defined, because it is necessary to protect against clandestine intelligence activities by foreign powers or their agents. Similarly, much information concerning international terrorism would likewise constitute evidence of crimes and also be "foreign intelligence information," as defined. This paragraph does not relate to information, even though it constitutes evidence of a crime, which is also needed by the United States in order to obtain, produce or disseminate foreign intelligence information. Rather, this paragraph applies to evi-

dence of crimes which otherwise would have to be minimized because it was not needed to obtain, produce, or disseminate foreign intelligence information. For example, in the course of a search evidence of a crime totally unrelated to intelligence matters might be incidentally acquired. Such evidence should not be required to be destroyed. Where the information is not foreign intelligence information, however, retention and dissemination of such evidence is allowed only for law enforcement purposes. Such purposes include arrest, prosecution, and other law enforcement measures taken for the purpose of preventing the crime. Thus, this paragraph is not a loophole by which the Government can generally keep and disseminate derogatory information about individuals which may be a technical violation of law, where there is no intent actually to enforce the criminal law. On the other hand, where the evidence also constitutes "foreign intelligence information," as defined, this paragraph does not apply, and the information may be disseminated and used for purposes other than enforcing the criminal law.

Section 309(5) defines "physical search" to mean any physical intrusion into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include "electronic surveillance" as defined in subsection 101(f) of FISA. The definition expressly includes "altering" property so as to ensure that the court is informed and approves of any planned physical alteration of property incidental to a search, e.g., the replacement of a lock so as to conceal the fact of the search.

This definition is meant to be broadly inclusive, because the effect of including a particular means of search is not to prohibit it but to subject it to the statutory procedures. It is not mean, however, to require a court order in any case where a search warrant would not be required in an ordinary criminal context. Thus, where courts have held searches for law enforcement purposes to be lawful in the absence of a search warrant, e.g., items seized were in the "plain view" of government agents or a search was undertaken in "exigent circumstances," such searches are excluded from the definition of "physical search" in this paragraph.

On the other hand, the provision that "a warrant would be required for law enforcement purposes" does not necessarily mean that a court had previously required a warrant for the particular type of search carried out under this title. The technique involved may not have come before a court for a determination as to whether a warrant is required. Nevertheless, the search activity is intended to be covered if a warrant would be required for law enforcement purposes, as determined on the basis of an assessment of the similarity to other activities which the courts have ruled upon, and the reasonableness of the expectation of privacy that a U.S. person would have with respect to such activity.

Finally, the definition specifically excludes "electronic surveillance" as defined by section 101(f) of the Act. The Committee also does not intend that this title affect the acquisition by the United States Government of foreign intelligence information from inter-

national or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic surveillance communications system, utilizing a means other than electronic surveillance as defined in section 101(f) of the Act.

Subsection (b) of section 9 of the bill amends the table of contents to the Foreign Intelligence Surveillance Act of 1978 to delete the items relating to the existing title III and add the items relating to the new title III as added by this bill.

Subsection (c) of section 9 of the bill states that the amendments made by subsections (a) and (b) shall become effective 90 days after the date of enactment of this Act, except that any physical search approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of this title (as added by this Act), if that search is conducted within 180 days following the date of enactment of this Act pursuant to regulations issued by the Attorney General, which are in the possession of the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives prior to the date of enactment.

This provision allows some flexibility in the timing of implementation of the statutory physical search procedures. The Committee intends that the Attorney General shall begin making applications for orders under this title and the court may grant such orders as soon as practicable after the effective date of this title. Prior to the first application, U.S. intelligence officers may conduct physical searches under the Executive branch procedures previously in effect. The Committee intends that after the Attorney General makes the first application to the court under this title, no subsequent physical search which requires a court order under this title shall be approved by the Attorney General without a court order. Searches approved by the Attorney General prior to that date, but not yet conducted, may be carried out so long as they occur within 180 days of enactment.

Section 10. Lesser criminal offense for the unauthorized removal of classified documents

Subsection (a) of section 10 of the bill adds a new section 1924 to chapter 93 of title 18, Untied States Code, to establish a misdemeanor offense for the unauthorized removal and retention of classified documents or material.

Subsection (a) of the new section 1924 provides that whoever being an officer, employee, contractor, or consultant of the United States, and by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain them at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than 1 year, or both.

Subsection (b) of the new section 1924 defines the term "classified information of the United States" as meaning information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive

order to require protection against unauthorized disclosure in the interests of national security.

Subsection (b) of section 10 of the bill amends the table of contents for chapter 93, title 18, United States Code, to include an item relating to the new section 1924 added by the bill.

COMMITTEE ACTION

On May 24, 1994, the Select Committee on Intelligence approved the bill as amended by a vote of 15–2, and ordered that it be favorably reported.

ESTIMATE OF COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate, the Committee attempted to estimate the costs which would be incurred in carrying out the provisions of this bill in fiscal year 1995 and in each of the five years thereafter. While several of the provisions of the bill (and the implementing regulations required by the bill) can be expected to increase the administrative costs associated with personnel security programs, the Committee believes these costs can be absorbed within existing levels of appropriations. In its action on the Intelligence Authorization Act for Fiscal Year 1995, the Committee in fact authorized certain increases in personnel security funding, based upon available appropriations, to enable intelligence agencies to obtain and utilize the information available to them under section 2 of S. 2056.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to existing law, the Committee requested and received the following cost estimate from the Congressional Budget Office regarding this bill:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 27, 1994.

Hon. DENNIS DECONCINI,
Chairman, Select Committee on Intelligence,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2056, the Counterintelligence and Security Enhancements Act of 1994, as ordered reported by the Senate Select Committee on Intelligence on May 24, 1994. Enactment of the authorization act would not affect direct spending or receipts. Therefore, pay-as-you-go procedures would not apply to the bill.

If you wish further details on this estimate, we will be pleased to provide them.

Sincerely,

ROBERT D. REISCHAUER, *Director.*

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

1. Bill number: S. 2056.

2. Bill title: Counterintelligence and Security Enhancements Act of 1994.

3. Bill status: As ordered reported by the Senate Select Committee on Intelligence on May 24, 1994.

4. Bill purpose: To enhance the counterintelligence and security posture of the United States through better coordination of efforts by Federal agencies to detect and prevent acts of espionage.

5. Estimated cost to the Federal Government:

[By fiscal year, in millions of dollars]

	1995	1996	1997	1998	1999
Estimated authorization of appropriations	(1)	(1)	(1)	(1)	(1)
Estimated outlays	(1)	(1)	(1)	(1)	(1)

[1] Less than $500,000.

Basis of estimate: The bill extends access to financial records, consumer credit records, and travel records to authorized investigative agencies provided that such information is to be used for an authorized law enforcement investigation, foreign counterintelligence inquiry, or security determination. Fees may be paid to the reporting agencies to cover processing costs. Cost associated with the provision should be insignificant.

6. Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts through 1998. This authorization bill would not affect direct spending or receipts. Therefore, this bill has no pay-as-you-go implications.

7. Estimated cost to State and local governments: None.

8. Estimate comparison: None.

9. Previous CBO estimate: None.

10. Estimate prepared by: Elizabeth A. Chambers.

11. Estimate approved by: C.G. Nuckols, Assistant Director for Budget Analysis.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds no substantial regulatory impact will be incurred by implementation of this legislation. In a small number of cases, private entities may be requested to produce records requested by the Government on a reimbursable basis. But there are no regulatory requirements levied by this legislation upon the private sector.

CHANGES IN EXISTING LAW

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of Standing Rule XXVI to expedite the business of the Senate.

○

79-010 (84)