

exempted operational file or files in order to make the demonstration required under subparagraph (A) of this paragraph, unless the complainant disputes the Central Intelligence Agency's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence;

(5) in proceedings under paragraphs (3) and (4) of this subsection, the parties shall not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admission may be made pursuant to rules 26 and 36;

(6) if the court finds under this subsection that the Central Intelligence Agency has improperly withheld requested records because of failure to comply with any provision of this section, the court shall order the Central Intelligence Agency to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5 (Freedom of Information Act), and such order shall be the exclusive remedy for failure to comply with this section; and

(7) if at any time following the filing of a complaint pursuant to this subsection the Central Intelligence Agency agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.

(July 26, 1947, ch. 343, title VII, § 701, as added Oct. 15, 1984, Pub. L. 98-477, § 2(a), 98 Stat. 2209; amended Jan. 6, 1996, Pub. L. 104-93, title VII, § 702, 109 Stat. 978.)

#### REFERENCES IN TEXT

The Federal Rules of Civil Procedure, referred to in subsec. (f)(5), are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

#### AMENDMENTS

1996—Subsec. (b)(3). Pub. L. 104-93 substituted "Office of Personnel Security" for "Office of Security".

#### EFFECTIVE DATE

Section 4 of Pub. L. 98-477 provided that: "The amendments made by subsections (a) and (b) of section 2 [enacting this subchapter and amending section 552a of Title 5, Government Organization and Employees] shall be effective upon enactment of this Act [Oct. 15, 1984] and shall apply with respect to any requests for records, whether or not such request was made prior to such enactment, and shall apply to all civil actions not commenced prior to February 7, 1984."

#### SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 432 of this title.

### § 432. Decennial review of exempted operational files

#### (a) Review by Director of Central Intelligence

Not less than once every ten years, the Director of Central Intelligence shall review the exemptions in force under subsection (a) of section 431 of this title to determine whether such exemptions may be removed from any category of exempted files or any portion thereof.

#### (b) Consideration; historical value; public interest

The review required by subsection (a) of this section shall include consideration of the histor-

ical value or other public interest in the subject matter of the particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

#### (c) Judicial review

A complainant who alleges that the Central Intelligence Agency has improperly withheld records because of failure to comply with this section may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District of Columbia. In such a proceeding, the court's review shall be limited to determining (1) whether the Central Intelligence Agency has conducted the review required by subsection (a) of this section within ten years of enactment of this title or within ten years after the last review, and (2) whether the Central Intelligence Agency, in fact, considered the criteria set forth in subsection (b) of this section in conducting the required review.

(July 26, 1947, ch. 343, title VII, § 702, as added Oct. 15, 1984, Pub. L. 98-477, § 2(a), 98 Stat. 2211.)

#### EFFECTIVE DATE

Section effective Oct. 15, 1984, and applicable with respect to any request for records, whether or not such request was made prior to Oct. 15, 1984, and applicable to all civil actions not commenced prior to Feb. 7, 1984, see section 4 of Pub. L. 98-477, set out as a note under section 431 of this title.

#### DECLASSIFICATION AND RELEASE OF CIA INFORMATION OF HISTORICAL VALUE

Section 3 of Pub. L. 98-477 directed Director of Central Intelligence, in consultation with Archivist of the United States, Librarian of Congress, and appropriate representatives of historical discipline selected by Archivist, to prepare and submit report to Congress by June 1, 1985, on feasibility of conducting systematic review for declassification and release of Central Intelligence Agency information of historical value. Director was also required to prepare and submit four unclassified reports, one each six months beginning by Apr. 15, 1985, which were to include a description of the specific measures established by Director to improve processing of requests under section 552 of title 5, United States Code, current budgetary and personnel allocations for such processing, the number of such requests (i) received and processed during the preceding six months, and (ii) pending at time of submission of such report, and an estimate of current average response time for completing the processing of such requests.

#### SUBCHAPTER VI—ACCESS TO CLASSIFIED INFORMATION

### § 435. Procedures

(a) Not later than 180 days after October 14, 1994, 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 to the employing department or agency written consent 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 436 of this title, during the period of access to classified information and for a period of three 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 condition 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 in the executive branch of Government whose access to classified information is being denied or terminated under this subchapter 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.

(b)(1) Subsection (a) of this section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to other law or Executive order to deny or terminate access to classified information if the national security so requires. Such responsibility and power may be exercised only when the agency head determines that the procedures prescribed by subsection (a) of this section cannot be invoked in a manner that is consistent with the national security.

(2) Upon the exercise of such responsibility, the agency head shall submit a report to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

(July 26, 1947, ch. 343, title VIII, §801, as added Oct. 14, 1994, Pub. L. 103-359, title VIII, §802(a), 108 Stat. 3435.)

#### EFFECTIVE DATE

Section 802(c) of Pub. L. 103-359 provided that: "The amendments made by subsections (a) and (b) [enacting this subchapter] shall take effect 180 days after the date of enactment of this Act [Oct. 14, 1994]."

#### SECURITY AGREEMENTS USED IN INTELLIGENCE ACTIVITIES

Pub. L. 104-93, title III, §306, Jan. 6, 1996, 109 Stat. 966, provided that: "Notwithstanding any other provision of law not specifically referencing this section, a non-disclosure policy form or agreement that is to be executed by a person connected with the conduct of an intelligence or intelligence-related activity, other than an employee or officer of the United States Government, may contain provisions appropriate to the particular activity for which such document is to be used. Such form or agreement shall, at a minimum—

"(1) require that the person will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government; and

"(2) provide that the form or agreement does not bar—

"(A) disclosures to Congress; or

"(B) disclosures to an authorized official of an executive agency that are deemed essential to reporting a violation of United States law."

#### VOLUNTARY SERVICE PROGRAM

Pub. L. 104-93, title IV, §402, Jan. 6, 1996, 109 Stat. 969, provided that:

"(a) GENERAL AUTHORITY.—The Director of Central Intelligence is authorized to establish and maintain a program from fiscal years 1996 through 2001 to utilize the services contributed by not more than 50 annuitants who serve without compensation as volunteers in aid of the review for declassification or downgrading of classified information by the Central Intelligence Agency under applicable Executive orders governing the classification and declassification of national security information and Public Law 102-526 [44 U.S.C. 2107 note].

"(b) COSTS INCIDENTAL TO SERVICES.—The Director is authorized to use sums made available to the Central Intelligence Agency by appropriations or otherwise for paying the costs incidental to the utilization of services contributed by individuals under subsection (a). Such costs may include (but need not be limited to) training, transportation, lodging, subsistence, equipment, and supplies. The Director may authorize either direct procurement of equipment, supplies, and services, or reimbursement for expenses, incidental to the effective use of volunteers. Such expenses or services shall be in accordance with volunteer agreements made with such individuals. Sums made available for such costs may not exceed \$100,000.

"(c) APPLICATION OF CERTAIN PROVISIONS OF LAW.—A volunteer under this section shall be considered to be a Federal employee for the purposes of subchapter I of title [chapter] 81 [of title 5] (relating to compensation of Federal employees for work injuries) and section 1346(b) and chapter 171 of title 28 (relating to tort claims). A volunteer under this section shall be covered by and subject to the provisions of chapter 11 of title 18 of the United States Code as if they were employees or special Government employees depending upon the days of expected service at the time they begin volunteering."

#### COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY

Pub. L. 103-236, title IX, Apr. 30, 1994, 108 Stat. 525, provided that:

"SEC. 901. SHORT TITLE.

"This title may be cited as the 'Protection and Reduction of Government Secrecy Act'.

"SEC. 902. FINDINGS.

"The Congress makes the following findings:

"(1) During the Cold War an extensive secrecy system developed which limited public access to information and reduced the ability of the public to participate with full knowledge in the process of governmental decisionmaking.

“(2) In 1992 alone 6,349,532 documents were classified and approximately three million persons held some form of security clearance.

“(3) The burden of managing more than 6 million newly classified documents every year has led to tremendous administrative expense, reduced communication within the government and within the scientific community, reduced communication between the government and the people of the United States, and the selective and unauthorized public disclosure of classified information.

“(4) It has been estimated that private businesses spend more than \$14 billion each year implementing government mandated regulations for protecting classified information.

“(5) If a smaller amount of truly sensitive information were classified the information could be held more securely.

“(6) In 1970 a Task Force organized by the Defense Science Board and headed by Dr. Frederick Seitz concluded that ‘more might be gained than lost if our Nation were to adopt—unilaterally, if necessary—a policy of complete openness in all areas of information’.

“(7) The procedures for granting security clearances have themselves become an expensive and inefficient part of the secrecy system and should be closely examined.

“(8) A bipartisan study commission specially constituted for the purpose of examining the consequences of the secrecy system will be able to offer comprehensive proposals for reform.

#### “SEC. 903. PURPOSE.

“It is the purpose of this title to establish for a two-year period a Commission on Protecting and Reducing Government Secrecy—

“(1) to examine the implications of the extensive classification of information and to make recommendations to reduce the volume of information classified and thereby to strengthen the protection of legitimately classified information; and

“(2) to examine and make recommendations concerning current procedures relating to the granting of security clearances.

#### “SEC. 904. COMPOSITION OF THE COMMISSION.

“(a) ESTABLISHMENT.—To carry out the purpose of this title, there is established a Commission on Protecting and Reducing Government Secrecy (in this title referred to as the ‘Commission’).

“(b) COMPOSITION.—The Commission shall be composed of twelve members, as follows:

“(1) Four members appointed by the President, of whom two shall be appointed from the executive branch of the Government and two shall be appointed from private life.

“(2) Two members appointed by the Majority Leader of the Senate, of whom one shall be a Member of the Senate and one shall be appointed from private life.

“(3) Two members appointed by the Minority Leader of the Senate, of whom one shall be a Member of the Senate and one shall be appointed from private life.

“(4) Two members appointed by the Speaker of the House of Representatives, of whom one shall be a Member of the House and one shall be appointed from private life.

“(5) Two members appointed by the Minority Leader of the House of Representatives, of whom one shall be a Member of the House and one shall be appointed from private life.

“(c) CHAIRMAN.—The Commission shall elect a Chairman from among its members.

“(d) QUORUM; VACANCIES.—After its initial meeting, the Commission shall meet upon the call of the Chairman or a majority of its members. Seven members of the Commission shall constitute a quorum. Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

“(e) APPOINTMENT OF MEMBERS; INITIAL MEETING.—(1) It is the sense of the Congress that members of the Commission should be appointed not later than 60 days after the date of enactment of this title [Apr. 30, 1994].

“(2) If after 60 days from the date of enactment of this Act seven or more members of the Commission have been appointed, those members who have been appointed may meet and select a Chairman who thereafter shall have authority to begin the operations of the Commission, including the hiring of staff.

#### “SEC. 905. FUNCTIONS OF THE COMMISSION.

“The functions of the Commission shall be—

“(1) to conduct, for a period of 2 years from the date of its first meeting, an investigation into all matters in any way related to any legislation, executive order, regulation, practice, or procedure relating to classified information or granting security clearances; and

“(2) to submit to the Congress a final report containing such recommendations concerning the classification of national security information and the granting of security clearances as the Commission shall determine, including proposing new procedures, rules, regulations, or legislation.

#### “SEC. 906. POWERS OF THE COMMISSION.

“(a) IN GENERAL.—(1) The Commission or, on the authorization of the Commission, any subcommittee or member thereof, may, for the purpose of carrying out the provisions of this title—

“(A) hold such hearings and sit and act at such times and places, take such testimony, receive such evidence, administer such oaths, and

“(B) require, by subpoena or otherwise, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, and documents,

as the Commission or such designated subcommittee or designated member may deem advisable.

“(2) Subpoenas issued under paragraph (1)(B) may be issued under the signature of the Chairman of the Commission, the chairman of any designated subcommittee, or any designated member, and may be served by any person designated by such Chairman, subcommittee chairman, or member. The provisions of sections 102 through 104 of the Revised Statutes of the United States (2 U.S.C. 192–194) shall apply in the case of any failure of any witness to comply with any subpoena or to testify when summoned under authority of this section.

“(b) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriation Acts, enter into contracts to enable the Commission to discharge its duties under this title.

“(c) INFORMATION FROM FEDERAL AGENCIES.—The Commission is authorized to secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government information, suggestions, estimates, and statistics for the purposes of this title. Each such department, bureau, agency, board, commission, office, establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Commission, upon request made by the Chairman.

“(d) ASSISTANCE FROM FEDERAL AGENCIES.—(1) The Secretary of State is authorized on a reimbursable or non-reimbursable basis to provide the Commission with administrative services, funds, facilities, staff, and other support services for the performance of the Commission’s functions.

“(2) The Administrator of General Services shall provide to the Commission on a reimbursable basis such administrative support services as the Commission may request.

“(3) In addition to the assistance set forth in paragraphs (1) and (2), departments and agencies of the United States are authorized to provide to the Commission such services, funds, facilities, staff, and other support services as they may deem advisable and as may be authorized by law.

“(e) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

“(f) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as departments and agencies of the United States.

“SEC. 907. STAFF OF THE COMMISSION.

“(a) IN GENERAL.—The Chairman, in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of a staff director and such other personnel as may be necessary to enable the Commission to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable to a person occupying a position at level V of the Executive Schedule under section 5316 of title 5, United States Code. Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

“(b) CONSULTANT SERVICES.—The Commission is authorized to procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code.

“SEC. 908. COMPENSATION AND TRAVEL EXPENSES.

“(a) COMPENSATION.—(1) Except as provided in paragraph (2), each member of the Commission may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Commission.

“(2) Members of the Commission who are officers or employees of the United States or Members of Congress shall receive no additional pay on account of their service on the Commission.

“(b) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703(b) of title 5, United States Code.

“SEC. 909. SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.

“The appropriate executive departments and agencies shall cooperate with the Commission in expeditiously providing to the Commission members and staff appropriate security clearances in a manner consistent with existing procedures and requirements, except that no person shall be provided with access to classified information pursuant to this section who would not otherwise qualify for such security clearance.

“SEC. 910. FINAL REPORT OF COMMISSION; TERMINATION.

“(a) FINAL REPORT.—Not later than two years after the date of the first meeting of the Commission, the Commission shall submit to the Congress its final report, as described in section 905(2).

“(b) TERMINATION.—(1) The Commission, and all the authorities of this title, shall terminate on the date which is 60 days after the date on which a final report is required to be transmitted under subsection (a).

“(2) The Commission may use the 60-day period referred to in paragraph (1) for the purpose of concluding its activities, including providing testimony to com-

mittees of Congress concerning its final report and disseminating that report.”

REPORTS RELATING TO CERTAIN SPECIAL ACCESS PROGRAMS AND SIMILAR PROGRAMS

Pub. L. 103-160, div. A, title XI, § 1152, Nov. 30, 1993, 107 Stat. 1758, provided that:

“(a) IN GENERAL.—(1) Not later than February 1 of each year, the head of each covered department or agency shall submit to Congress a report on each special access program carried out in the department or agency.

“(2) Each such report shall set forth—

“(A) the total amount requested by the department or agency for special access programs within the budget submitted under section 1105 of title 31, United States Code, for the fiscal year following the fiscal year in which the report is submitted; and

“(B) for each program in such budget that is a special access program—

“(i) a brief description of the program;

“(ii) in the case of a procurement program, a brief discussion of the major milestones established for the program;

“(iii) the actual cost of the program for each fiscal year during which the program has been conducted before the fiscal year during which that budget is submitted; and

“(iv) the estimated total cost of the program and the estimated cost of the program for (I) the current fiscal year, (II) the fiscal year for which the budget is submitted, and (III) each of the four succeeding fiscal years during which the program is expected to be conducted.

“(b) NEWLY DESIGNATED PROGRAMS.—(1) Not later than February 1 of each year, the head of each covered department or agency shall submit to Congress a report that, with respect to each new special access program of that department or agency, provides—

“(A) notice of the designation of the program as a special access program; and

“(B) justification for such designation.

“(2) A report under paragraph (1) with respect to a program shall include—

“(A) the current estimate of the total program cost for the program; and

“(B) an identification, as applicable, of existing programs or technologies that are similar to the technology, or that have a mission similar to the technology, or that have a mission similar to the mission, of the program that is the subject of the notice.

“(3) In this subsection, the term ‘new special access program’ means a special access program that has not previously been covered in a notice and justification under this subsection.

“(c) REVISION IN CLASSIFICATION OF PROGRAMS.—(1) Whenever a change in the classification of a special access program of a covered department or agency is planned to be made or whenever classified information concerning a special access program of a covered department or agency is to be declassified and made public, the head of the department or agency shall submit to Congress a report containing a description of the proposed change or the information to be declassified, the reasons for the proposed change or declassification, and notice of any public announcement planned to be made with respect to the proposed change or declassification.

“(2) Except as provided in paragraph (3), a report referred to in paragraph (1) shall be submitted not less than 14 days before the date on which the proposed change, declassification, or public announcement is to occur.

“(3) If the head of the department or agency determines that because of exceptional circumstances the requirement of paragraph (2) cannot be met with respect to a proposed change, declassification, or public announcement concerning a special access program of the department or agency, the head of the department

or agency may submit the report required by paragraph (1) regarding the proposed change, declassification, or public announcement at any time before the proposed change, declassification, or public announcement is made and shall include in the report an explanation of the exceptional circumstances.

“(d) REVISION OF CRITERIA FOR DESIGNATING PROGRAMS.—Whenever there is a modification or termination of the policy and criteria used for designating a program of a covered department or agency as a special access program, the head of the department or agency shall promptly notify Congress of such modification or termination. Any such notification shall contain the reasons for the modification or termination and, in the case of a modification, the provisions of the policy as modified.

“(e) WAIVER OF REPORTING REQUIREMENT.—(1) The head of a covered department or agency may waive any requirement under subsection (a), (b), or (c) that certain information be included in a report under that subsection if the head of the department or agency determines that inclusion of that information in the report would adversely affect the national security. Any such waiver shall be made on a case-by-case basis.

“(2) If the head of a department or agency exercises the authority provided under paragraph (1), the head of the department or agency shall provide the information described in that subsection with respect to the special access program concerned, and the justification for the waiver, to Congress.

“(f) INITIATION OF PROGRAMS.—A special access program may not be initiated by a covered department or agency until—

“(1) the appropriate oversight committees are notified of the program; and

“(2) a period of 30 days elapses after such notification is received.

“(g) DEFINITIONS.—For purposes of this section:

“(1) COVERED DEPARTMENT OR AGENCY.—(A) Except as provided in subparagraph (B), the term ‘covered department or agency’ means any department or agency of the Federal Government that carries out a special access program.

“(B) Such term does not include—

“(i) the Department of Defense (which is required to submit reports on special access programs under section 119 of title 10, United States Code);

“(ii) the Department of Energy, with respect to special access programs carried out under the atomic energy defense activities of that department (for which the Secretary of Energy is required to submit reports under section 93 of the Atomic Energy Act of 1954 [42 U.S.C. 2122a]); or

“(iii) an agency in the Intelligence Community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a)).

“(2) SPECIAL ACCESS PROGRAM.—The term ‘special access program’ means any program that, under the authority of Executive Order 12356 [formerly set out below] (or any successor Executive order), is established by the head of a department or agency whom the President has designated in the Federal Register as an original ‘secret’ or ‘top secret’ classification authority that imposes ‘need-to-know’ controls or access controls beyond those controls normally required (by regulations applicable to such department or agency) for access to information classified as ‘confidential’, ‘secret’, or ‘top secret’.”

DISCLOSURE OF INFORMATION CONCERNING UNACCOUNTED FOR UNITED STATES PERSONNEL OF COLD WAR, KOREAN CONFLICT, AND VIETNAM ERA

Pub. L. 102-190, div. A, title X, §1082, Dec. 5, 1991, 105 Stat. 1480, as amended by Pub. L. 103-337, div. A, title X, §1036, Oct. 5, 1994, 108 Stat. 2841; Pub. L. 104-106, div. A, title X, §1085, Feb. 10, 1996, 110 Stat. 457, provided that:

“(a) PUBLIC AVAILABILITY OF INFORMATION.—(1) Except as provided in subsection (b), the Secretary of Defense shall, with respect to any information referred to

in paragraph (2), place the information in a suitable library-like location within a facility within the National Capital region for public review and photocopying.

“(2) Paragraph (1) applies to any record, live-sighting report, or other information in the custody of the official custodian referred to in subsection (d)(3) that may pertain to the location, treatment, or condition of (A) United States personnel who remain not accounted for as a result of service in the Armed Forces or other Federal Government service during the Korean conflict, the Vietnam era, or the Cold War, or (B) their remains.

“(b) EXCEPTIONS.—(1) The Secretary of Defense may not make a record or other information available to the public pursuant to subsection (a) if—

“(A) the record or other information is exempt from the disclosure requirements of section 552 of title 5, United States Code, by reason of subsection (b) of that section; or

“(B) the record or other information is in a system of records exempt from the requirements of subsection (d) of section 552a of such title pursuant to subsection (j) or (k) of that section.

“(2) The Secretary of Defense may not make a record or other information available to the public pursuant to subsection (a) if the record or other information specifically mentions a person by name unless—

“(A) in the case of a person who is alive (and not incapacitated) and whose whereabouts are known, that person expressly consents in writing to the disclosure of the record or other information; or

“(B) in the case of a person who is dead or incapacitated or whose whereabouts are unknown, a family member or family members of that person determined by the Secretary of Defense to be appropriate for such purpose expressly consent in writing to the disclosure of the record or other information.

“(3)(A) The limitation on disclosure in paragraph (2) does not apply in the case of a person who is dead or incapacitated or whose whereabouts are unknown if the family member or members of that person determined pursuant to subparagraph (B) of that paragraph cannot be located by the Secretary of Defense—

“(i) in the case of a person missing from the Vietnam era, after a reasonable effort; and

“(ii) in the case of a person missing from the Korean Conflict or Cold War, after a period of 90 days from the date on which any record or other information referred to in paragraph (2) is received by the Department of Defense for disclosure review from the Archivist of the United States, the Library of Congress, or the Joint United States-Russian Commission on POW/MIAs.

“(B) Paragraph (2) does not apply to the access of an adult member of the family of a person to any record or information to the extent that the record or other information relates to that person.

“(C) The authority of a person to consent to disclosure of a record or other information for the purposes of paragraph (2) may be delegated to another person or an organization only by means of an express legal power of attorney granted by the person authorized by that paragraph to consent to the disclosure.

“(c) DEADLINES.—(1) In the case of records or other information originated by the Department of Defense, the official custodian shall make such records and other information available to the public pursuant to this section not later than January 2, 1996. Such records or other information shall be made available as soon as a review carried out for the purposes of subsection (b) is completed.

“(2) Whenever a department or agency of the Federal Government receives any record or other information referred to in subsection (a) that is required by this section to be made available to the public, the head of that department or agency shall ensure that such record or other information is provided to the Secretary of Defense, and the Secretary shall make such record or other information available in accordance with subsection (a) as soon as possible and, in any

event, not later than one year after the date on which the record or information is received by the department or agency of the Federal Government.

“(3) If the Secretary of Defense determines that the disclosure of any record or other information referred to in subsection (a) by the date required by paragraph (1) or (2) may compromise the safety of any United States personnel referred to in subsection (a)(2) who remain not accounted for but who may still be alive in captivity, then the Secretary may withhold that record or other information from the disclosure otherwise required by this section. Whenever the Secretary makes a determination under the preceding sentence, the Secretary shall immediately notify the President and the Congress of that determination.

“(d) DEFINITIONS.—For purposes of this section:

“(1) The terms ‘Korean conflict’ and ‘Vietnam era’ have the meanings given those terms in section 101 of title 38, United States Code.

“(2) The term ‘Cold War’ means the period from the end of World War II to the beginning of the Korean conflict and the period from the end of the Korean conflict to the beginning of the Vietnam era.

“(3) The term ‘official custodian’ means—

“(A) in the case of records, reports, and information relating to the Korean conflict or the Cold War, the Archivist of the United States; and

“(B) in the case of records, reports, and information relating to the Vietnam era, the Secretary of Defense.”

DISCLOSURE OF INFORMATION CONCERNING AMERICAN PERSONNEL LISTED AS PRISONER, MISSING, OR UNACCOUNTED FOR IN SOUTHEAST ASIA

Pub. L. 100-453, title IV, §404, Sept. 29, 1988, 102 Stat. 1908, provided that:

“(a) This section is enacted to ensure that current disclosure policy is incorporated into law.

“(b) Except as provided in subsection (c), the head of each department or agency—

“(1) with respect to which funds are authorized under this Act [see Tables for classification], and

“(2) which holds or receives live sighting reports of any United States citizen reported missing in action, prisoner of war, or unaccounted for from the Vietnam Conflict,

shall make available to the next-of-kin of that United States citizen all reports, or portions thereof, held by that department or agency which have been correlated or possibly correlated to that citizen.

“(c) Subsection (b) does not apply with respect to—

“(1) information that would reveal or compromise sources and methods of intelligence collection; or

“(2) specific information that previously has been made available to the next-of-kin.

“(d) The head of each department or agency covered by subsection (a) shall make information available under this section in a timely manner.”

EXECUTIVE ORDER No. 10501

Ex. Ord. No. 10501, Nov. 5, 1953, 18 F.R. 7049, as amended by Ex. Ord. No. 10816, May 7, 1959, 24 F.R. 3777; Ex. Ord. No. 10901, Jan. 9, 1961, 26 F.R. 217; Ex. Ord. No. 10964, Sept. 20, 1961, 26 F.R. 8932; Ex. Ord. No. 10985, Jan. 12, 1962, 27 F.R. 439; Ex. Ord. No. 11097, Feb. 28, 1963, 28 F.R. 2225; Ex. Ord. No. 11382, Nov. 28, 1967, 32 F.R. 16247, which related to safeguarding official information, was superseded by Ex. Ord. No. 11652, Mar. 8, 1972, 37 F.R. 5209, formerly set out below.

EX. ORD. NO. 10865. SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

Ex. Ord. No. 10865, Feb. 20, 1960, 25 F.R. 1583, as amended by Ex. Ord. No. 10909, Jan. 17, 1961, 26 F.R. 508; Ex. Ord. No. 11382, Nov. 28, 1967, 32 F.R. 16247; Ex. Ord. No. 12829, §203(g), Jan. 6, 1993, 58 F.R. 3479, provided:

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interest of individuals affected thereby and provide maximum possible safeguards to protect such interests:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the armed forces of the United States, it is hereby ordered as follows:

SECTION 1. When used in this order, the term “head of a department” means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term “head of a department” also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829 [set out below].

SEC. 2. An authorization for access to classified information pursuant to Executive Order No. 12829 [set out below] may be granted by the head of a department or his designee, including but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an “applicant”, for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

SEC. 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked pursuant to Executive Order No. 12829 [set out below] by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee including, but not limited to, those officials named in section 8 of this order for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

SEC. 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the department to be good and sufficient.

(b) Whenever procedures under paragraphs (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SEC. 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SEC. 6. The head of a department of the United States or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Standardized Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees

of the executive branch of the Government or members of the armed forces of the United States not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An officer or employee of the executive branch of the Government or a member of the armed forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other department or agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination.

SEC. 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

SEC. 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a department by this order may be delegated to the the [sic] deputy of that department, or the principal assistant to the head of that department, as the case may be.

SEC. 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

#### MODIFICATION OF EXECUTIVE ORDER NO. 10865

Ex. Ord. No. 10865, Feb. 20, 1960, 25 F.R. 1583, as amended, set out above, when referring to functions of the Atomic Energy Commission is modified to provide that all such functions shall be exercised by the Secretary of Energy and the Nuclear Regulatory Commission, see section 4(a)(1) of Ex. Ord. No. 12038, Feb. 3, 1978, 43 F.R. 4957, set out under section 7151 of Title 42, The Public Health and Welfare.

#### EXECUTIVE ORDER NO. 10985

Ex. Ord. No. 10985, Jan. 12, 1962, 27 F.R. 439, which amended Executive Order No. 10501, which related to safeguarding official information, was superseded by Ex. Ord. No. 11652, Mar. 8, 1972, 37 F.R. 5209, formerly set out below.

#### EXECUTIVE ORDER NO. 11097

Ex. Ord. No. 11097, Feb. 28, 1963, 28 F.R. 2225, which amended Executive Order No. 10501, which related to safeguarding official information, was superseded by Ex. Ord. No. 11652, Mar. 8, 1972, 37 F.R. 5209, formerly set out below.

#### EXECUTIVE ORDER NO. 11652

Ex. Ord. No. 11652, Mar. 8, 1972, 37 F.R. 5209, as amended by Ex. Ord. No. 11714, Apr. 24, 1973, 38 F.R. 10245; Ex. Ord. No. 11862, June 11, 1975, 40 F.R. 25197; Ex. Ord. No. 12038, Feb. 3, 1978, 43 F.R. 4957, which related to the classification and declassification of national security information and material, was revoked by Ex. Ord. No. 12065, June 28, 1978, 43 F.R. 28949, formerly set out below.

EX. ORD. NO. 11932. CLASSIFICATION OF CERTAIN INFORMATION AND MATERIAL OBTAINED FROM ADVISORY BODIES CREATED TO IMPLEMENT THE INTERNATIONAL ENERGY PROGRAM

Ex. Ord. No. 11932, Aug. 4, 1976, 41 F.R. 32691, provided: The United States has entered into the Agreement on an International Energy Program of November 18, 1974, which created the International Energy Agency. This program is a substantial factor in the conduct of our foreign relations and an important element of our national security. The effectiveness of the Agreement depends significantly upon the provision and exchange of information and material by participants in advisory bodies created by the International Energy Agency. Confidentiality is essential to assure the free and open discussion necessary to accomplish the tasks assigned to those bodies. I have consulted with the Secretary of State, the Attorney General and the Administrator of the Federal Energy Administration concerning the handling and safeguarding of information and material in the possession of the United States which has been obtained pursuant to the program, and I find that some of such information and material requires protection as provided in Executive Order No. 11652 of March 8, 1972, as amended [formerly set out above].

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, it is hereby ordered as follows:

SECTION 1. Information and material obtained pursuant to the International Energy Program and which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States shall be classified pursuant to Executive Order No. 11652 of March 8, 1972, as amended [formerly set out above]. The Secretary of State shall have the responsibility for the classification, declassification and safeguarding of information and material in the possession of the United States Government which has been obtained pursuant to:

(a) Section 252(c)(3), (d)(2), or (e)(3) of the Energy Policy and Conservation Act (89 Stat. 871; 42 U.S.C. 6272(c)(3), (d)(2), (e)(3)), or

(b) The Voluntary Agreement and Program relating to the International Energy Program (40 F.R. 16041, April 8, 1975), or

(c) Any similar Voluntary Agreement and Program entered into under the Energy Policy and Conservation Act [42 U.S.C. 6201 et seq.] after the date of this Order.

SEC. 2. Information or material classified pursuant to Section 1 of this Order may be exempted from the General Declassification Schedule established by Section 5 of Executive Order No. 11652 [formerly set out above] if it was obtained by the United States on the understanding that it be kept in confidence, or if it might otherwise be exempted under Section 5(B) of such Order.

SEC. 3. (a) Within 60 days of the date of this Order, the Secretary of State shall promulgate regulations which implement his responsibilities under this Order.

(b) The directives issued under Section 6 of Executive Order No. 11652 [formerly set out above] shall not apply to information and material classified under this Order. However, the regulations promulgated by the Secretary of State shall:

(1) conform, to the extent practicable, to the policies set forth in Section 6 of Executive Order No. 11652 [formerly set out above], and

(2) provide that he may take such measures as he deems necessary and appropriate to ensure the confidentiality of any information and material classified under this Order that may remain in the custody or control of any person outside the United States Government.

GERALD R. FORD.

EXECUTIVE ORDER NO. 12065

Ex. Ord. No. 12065, June 28, 1978, 43 F.R. 28949, as amended by Ex. Ord. No. 12148, July 20, 1979, 44 F.R.

43239; Ex. Ord. No. 12163, Sept. 29, 1979, 44 F.R. 56673, which related to classification and declassification of national security information and material, was revoked by Ex. Ord. No. 12356, Apr. 2, 1982, 47 F.R. 14874, 15557, formerly set out below.

EXECUTIVE ORDER NO. 12356

Ex. Ord. No. 12356, Apr. 2, 1982, 47 F.R. 14874, 15557, which prescribed a uniform system for classifying, declassifying, and safeguarding national security information, was revoked by Ex. Ord. No. 12958, §6.1(d), Apr. 17, 1995, 60 F.R. 19843, set out below.

EX. ORD. NO. 12812. DECLASSIFICATION AND RELEASE OF MATERIALS PERTAINING TO PRISONERS OF WAR AND MISSING IN ACTION

Ex. Ord. No. 12812, July 22, 1992, 57 F.R. 32879, provided:

WHEREAS, the Senate, by S. Res. 324 of July 2, 1992, has asked that I "expeditiously issue an Executive order requiring all executive branch departments and agencies to declassify and publicly release without compromising United States national security all documents, files, and other materials pertaining to POWs and MIAs;" and

WHEREAS, indiscriminate release of classified material could jeopardize continuing United States Government efforts to achieve the fullest possible accounting of Vietnam-era POWs and MIAs; and

WHEREAS, I have concluded that the public interest would be served by the declassification and public release of materials pertaining to Vietnam-era POWs and MIAs as provided below;

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, I hereby order as follows:

SECTION 1. All executive departments and agencies shall expeditiously review all documents, files, and other materials pertaining to American POWs and MIAs lost in Southeast Asia for the purposes of declassification in accordance with the standards and procedures of Executive Order No. 12356 [formerly set out above].

SEC. 2. All executive departments and agencies shall make publicly available documents, files, and other materials declassified pursuant to section 1, except for those the disclosure of which would constitute a clearly unwarranted invasion of personal privacy of returnees, family members of POWs and MIAs, or other persons, or would impair the deliberative processes of the executive branch.

SEC. 3. This order is not intended to create any right or benefit, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

GEORGE BUSH.

EX. ORD. NO. 12829. NATIONAL INDUSTRIAL SECURITY PROGRAM

Ex. Ord. No. 12829, Jan. 6, 1993, 58 F.R. 3479, as amended by Ex. Ord. No. 12885, Dec. 14, 1993, 58 F.R. 65863, provided:

This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to non-government organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a



single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.

Therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, including the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011–2286) [42 U.S.C. 2011 *et seq.*], the National Security Act of 1947, as amended (codified as amended in scattered sections of the United States Code) [see Short Title note set out under section 401 of this title], and the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2) [5 App. U.S.C.], it is hereby ordered as follows:

#### PART 1. ESTABLISHMENT AND POLICY

SECTION 101. *Establishment.* (a) There is established a National Industrial Security Program. The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. For the purposes of this order, the terms “contractor, licensee, or grantee” means current, prospective, or former contractors, licensees, or grantees of United States agencies. The National Industrial Security Program shall be applicable to all executive branch departments and agencies.

(b) The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order No. 12356 of April 2, 1982 [formerly set out above], or its successor, and the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 *et seq.*].

(c) For the purposes of this order, the term “contractor” does not include individuals engaged under personal services contracts.

SEC. 102. *Policy Direction.* (a) The National Security Council shall provide overall policy direction for the National Industrial Security Program.

(b) The Director of the Information Security Oversight Office, established under Executive Order No. 12356 of April 2, 1982 [formerly set out above], shall be responsible for implementing and monitoring the National Industrial Security Program and shall:

(1) develop, in consultation with the agencies, and promulgate subject to the approval of the National Security Council, directives for the implementation of this order, which shall be binding on the agencies;

(2) oversee agency, contractor, licensee, and grantee actions to ensure compliance with this order and implementing directives;

(3) review all agency implementing regulations, internal rules, or guidelines. The Director shall require any regulation, rule, or guideline to be changed if it is not consistent with this order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation, rule, or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority, pursuant to terms of applicable contracts, licenses, grants, or regulations, to conduct on-site reviews of the implementation of the National Industrial Security Program by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific classified information, or other forms of cooperation, would pose an exceptional national security risk, the affected agency head or the senior official designated under section 203(a) of this order may request the National Security Council to deny access to the Director. The Director shall not have access pending a prompt decision by the National Security Council;

(5) report any violations of this order or its implementing directives to the head of the agency or to the senior official designated under section 203(a) of this order so that corrective action, if appropriate, may be taken. Any such report pertaining to the implementation of the National Industrial Security Program by a

contractor, licensee, or grantee shall be directed to the agency that is exercising operational oversight over the contractor, licensee, or grantee under section 202 of this order;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the National Industrial Security Program;

(7) consider, in consultation with the advisory committee established by this order, affected agencies, contractors, licensees, and grantees, and recommend to the President through the National Security Council changes to this order; and

(8) report at least annually to the President through the National Security Council on the implementation of the National Industrial Security Program.

(c) Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 *et seq.*], or the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended [see Short Title note set out under section 401 of this title], or Executive Order No. 12333 of December 8, 1981 [50 U.S.C. 401 note].

SEC. 103. *National Industrial Security Program Policy Advisory Committee.* (a) *Establishment.* There is established the National Industrial Security Program Policy Advisory Committee (“Committee”).

The Director of the Information Security Oversight Office shall serve as Chairman of the Committee and appoint the members of the Committee. The members of the Committee shall be the representatives of those departments and agencies most affected by the National Industrial Security Program and nongovernment representatives of contractors, licensees, or grantees involved with classified contracts, licenses, or grants, as determined by the Chairman.

(b) *Functions.* (1) The Committee members shall advise the Chairman of the Committee on all matters concerning the policies of the National Industrial Security Program, including recommended changes to those policies as reflected in this order, its implementing directives, or the operating manual established under this order, and serve as a forum to discuss policy issues in dispute.

(2) The Committee shall meet at the request of the Chairman, but at least twice during the calendar year.

(c) *Administration.* (1) Members of the Committee shall serve without compensation for their work on the Committee. However, nongovernment members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(2) To the extent permitted by law and subject to the availability of funds, the Administrator of General Services shall provide the Committee with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(d) *General.* Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended [5 App. U.S.C.], except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

#### PART 2. OPERATIONS

SEC. 201. *National Industrial Security Program Operating Manual.* (a) The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence, shall issue and maintain a National Industrial Security Program Operating Manual (“Manual”).

The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under

the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 *et seq.*]. The Director of Central Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information.

(b) The Manual shall prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information to contractors, licensees, or grantees. The Manual shall apply to the release of classified information during all phases of the contracting process including bidding, negotiation, award, performance, and termination of contracts, the licensing process, or the grant process, with or under the control of departments or agencies.

(c) The Manual shall also prescribe requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information.

(d) In establishing particular requirements, restrictions, and other safeguards within the Manual, the Secretary of Defense, the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence shall take into account these factors: (i) the damage to the national security that reasonably could be expected to result from an unauthorized disclosure; (ii) the existing or anticipated threat to the disclosure of information; and (iii) the short- and long-term costs of the requirements, restrictions, and other safeguards.

(e) To the extent that is practicable and reasonable, the requirements, restrictions, and safeguards that the Manual establishes for the protection of classified information by contractors, licensees, and grantees shall be consistent with the requirements, restrictions, and safeguards that directives implementing Executive Order No. 12356 of April 2, 1982 [formerly set out above], or the Atomic Energy Act of 1954, as amended, establish for the protection of classified information by agencies. Upon request by the Chairman of the Committee, the Secretary of Defense shall provide an explanation and justification for any requirement, restriction, or safeguard that results in a standard for the protection of classified information by contractors, licensees, and grantees that differs from the standard that applies to agencies.

(f) The Manual shall be issued to correspond as closely as possible to pertinent decisions of the Secretary of Defense and the Director of Central Intelligence made pursuant to the recommendations of the Joint Security Review Commission and to revisions to the security classification system that result from Presidential Review Directive 29, but in any event no later than June 30, 1994.

SEC. 202. *Operational Oversight.* (a) The Secretary of Defense shall serve as Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees. The heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

(b) The Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor [sic] contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf.

(c) The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to in-

formation under their respective programs classified under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 *et seq.*]. The Secretary or the Commission may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on behalf of the Secretary or the Commission, respectively.

(d) The Executive Agent shall have the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the National Industrial Security Program.

SEC. 203. *Implementation.* (a) The head of each agency that enters into classified contracts, licenses, or grants shall designate a senior agency official to direct and administer the agency's implementation and compliance with the National Industrial Security Program.

(b) Agency implementing regulations, internal rules, or guidelines shall be consistent with this order, its implementing directives, and the Manual. Agencies shall issue these regulations, rules, or guidelines no later than 180 days from the issuance of the Manual. They may incorporate all or portions of the Manual by reference.

(c) Each agency head or the senior official designated under paragraph (a) above shall take appropriate and prompt corrective action whenever a violation of this order, its implementing directives, or the Manual occurs.

(d) The senior agency official designated under paragraph (a) above shall account each year for the costs within the agency associated with the implementation of the National Industrial Security Program. These costs shall be reported to the Director of the Information Security Oversight Office, who shall include them in the reports to the President prescribed by this order.

(e) The Secretary of Defense, with the concurrence of the Administrator of General Services, the Administrator of the National Aeronautics and Space Administration, and such other agency heads or officials who may be responsible, shall amend the Federal Acquisition Regulation to be consistent with the implementation of the National Industrial Security Program.

(f) All contracts, licenses, or grants that involve access to classified information and that are advertised or proposed following the issuance of agency regulations, rules, or guidelines described in paragraph (b) above shall comply with the National Industrial Security Program. To the extent that is feasible, economical, and permitted by law, agencies shall amend, modify, or convert preexisting contracts, licenses, or grants, or previously advertised or proposed contracts, licenses, or grants, that involve access to classified information for operation under the National Industrial Security Program. Any direct inspection or monitoring of contractors, licensees, or grantees specified by this order shall be carried out pursuant to the terms of a contract, license, grant, or regulation.

(g) Executive Order No. 10865 of February 20, 1960 [set out above], as amended by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, is hereby amended as follows:

(1) Section 1(a) and (b) are revoked as of the effective date of this order.

(2) Section 1(c) is renumbered as Section 1 and is amended to read as follows:

"SECTION 1. When used in this order, the term 'head of a department' means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term 'head of a department' also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense

concerning authorizations for access to classified information pursuant to Executive Order No. 12829.”

(3) Section 2 is amended by inserting the words “pursuant to Executive Order No. 12829” after the word “information.”

(4) Section 3 is amended by inserting the words “pursuant to Executive Order No. 12829” between the words “revoked” and “by” in the second clause of that section.

(5) Section 6 is amended by striking out the words “The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section (1)(b),” at the beginning of the first sentence, and inserting in their place “The head of a department of the United States . . . .”

(6) Section 8 is amended by striking out paragraphs (1) through (7) and inserting in their place “. . . the deputy of that department, or the principal assistant to the head of that department, as the case may be.”

(h) All delegations, rules, regulations, orders, directives, agreements, contracts, licenses, and grants issued under preexisting authorities, including section 1(a) and (b) of Executive Order No. 10865 of February 20, 1960, as amended, by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, shall remain in full force and effect until amended, modified, or terminated pursuant to authority of this order.

(i) This order shall be effective immediately.

EX. ORD. NO. 12937. DECLASSIFICATION OF SELECTED RECORDS WITHIN NATIONAL ARCHIVES OF UNITED STATES

Ex. Ord. No. 12937, Nov. 10, 1994, 59 F.R. 59097, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

SECTION 1. The records in the National Archives of the United States referenced in the list accompanying this order are hereby declassified.

SEC. 2. The Archivist of the United States shall take such actions as are necessary to make such records available for public research no later than 30 days from the date of this Order, except to the extent that the head of an affected agency and the Archivist have determined that specific information within such records must be protected from disclosure pursuant to an authorized exemption to the Freedom of Information Act, 5 U.S.C. 552, other than the exemption that pertains to national security information.

SEC. 3. Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

WILLIAM J. CLINTON.

Records in the following record groups (“RG”) in the National Archives of the United States shall be declassified. Page numbers are approximate. A complete list of the selected records is available from the Archivist of the United States.

I. All unreviewed World War II and earlier records, including:

A.	RG 18, Army Air Forces	1,722,400 pp.
B.	RG 65, Federal Bureau of Investigation	362,500 pp.
C.	RG 127, United States Marine Corps	195,000 pp.
D.	RG 216, Office of Censorship	112,500 pp.
E.	RG 226, Office of Strategic Services	415,000 pp.
F.	RG 60, United States Occupation Headquarters	4,422,500 pp.

G.	RG 331, Allied Operational and Occupation Headquarters, World War II (including 350 reels of Allied Force Headquarters)	3,097,500 pp.
H.	RG 332, United States Theaters of War, World War II	1,182,500 pp.
I.	RG 338, Mediterranean Theater of Operations and European Command	9,500,000 pp.
	Subtotal for World War II and earlier	21.0 million pp.
II.	Post-1945 Collections (Military and Civil)	
A.	RG 19, Bureau of Ships, Pre-1950 General Correspondence (selected records)	1,732,500 pp.
B.	RG 51, Bureau of the Budget, 52.12 Budget Preparation Branch, 1952-69	142,500 pp.
C.	RG 72, Bureau of Aeronautics (Navy) (selected records)	5,655,000 pp.
D.	RG 166, Foreign Agricultural Service, Narrative Reports, 1955-61	1,272,500 pp.
E.	RG 313, Naval Operating Forces (selected records)	407,500 pp.
F.	RG 319, Office of the Chief of Military History Manuscripts and Background Papers (selected records)	933,000 pp.
G.	RG 337, Headquarters, Army Ground Forces (selected records)	1,269,700 pp.
H.	RG 341, Headquarters, United States Air Force (selected records)	4,870,000 pp.
I.	RG 389, Office of the Provost Marshal General (selected records)	448,000 pp.
J.	RG 391, United States Army Regular Army Mobil Units	240,000 pp.
K.	RG 428, General Records of the Department of the Navy (selected records)	31,250 pp.
L.	RG 472, Army Vietnam Collection (selected records)	5,864,000 pp.
	Subtotal for Other	22.9 million pp.
	TOTAL	43.9 million pp.

EX. ORD. NO. 12951. RELEASE OF IMAGERY ACQUIRED BY SPACE-BASED NATIONAL INTELLIGENCE RECONNAISSANCE SYSTEMS

Ex. Ord. No. 12951, Feb. 22, 1995, 60 F.R. 10789, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to release certain scientifically or environmentally useful imagery acquired by space-based national intelligence reconnaissance systems, consistent with the national security, it is hereby ordered as follows:

SECTION 1. *Public Release of Historical Intelligence Imagery.* Imagery acquired by the space-based national intelligence reconnaissance systems known as the Corona, Argon, and Lanyard missions shall, within 18 months of the date of this order, be declassified and transferred to the National Archives and Records Administration with a copy sent to the United States Geological Survey of the Department of the Interior consistent with procedures approved by the Director of Central Intelligence and the Archivist of the United States. Upon transfer, such imagery shall be deemed declassified and shall be made available to the public.

SEC. 2. *Review for Future Public Release of Intelligence Imagery.* (a) All information that meets the criteria in section 2(b) of this order shall be kept secret in the interests of national defense and foreign policy until deemed otherwise by the Director of Central Intelligence. In consultation with the Secretaries of State and Defense, the Director of Central Intelligence shall

establish a comprehensive program for the periodic review of imagery from systems other than the Corona, Argon, and Lanyard missions, with the objective of making available to the public as much imagery as possible consistent with the interests of national defense and foreign policy. For imagery from obsolete broad-area film-return systems other than Corona, Argon, and Lanyard missions, this review shall be completed within 5 years of the date of this order. Review of imagery from any other system that the Director of Central Intelligence deems to be obsolete shall be accomplished according to a timetable established by the Director of Central Intelligence. The Director of Central Intelligence shall report annually to the President on the implementation of this order.

(b) The criteria referred to in section 2(a) of this order consist of the following: imagery acquired by a space-based national intelligence reconnaissance system other than the Corona, Argon, and Lanyard missions.

SEC. 3. *General Provisions.* (a) This order prescribes a comprehensive and exclusive system for the public release of imagery acquired by space-based national intelligence reconnaissance systems. This order is the exclusive Executive order governing the public release of imagery for purposes of section 552(b)(1) of the Freedom of Information Act [5 U.S.C. 552(b)(1)].

(b) Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

SEC. 4. *Definition.* As used herein, "imagery" means the product acquired by space-based national intelligence reconnaissance systems that provides a likeness or representation of any natural or man-made feature or related objective or activities and satellite positional data acquired at the same time the likeness or representation was acquired.

WILLIAM J. CLINTON.

EX. ORD. NO. 12958. CLASSIFIED NATIONAL SECURITY INFORMATION

Ex. Ord. No. 12958, Apr. 17, 1995, 60 F.R. 19825, as amended by Ex. Ord. No. 12972, Sept. 18, 1995, 60 F.R. 48863, provided:

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

SECTION 1.1. *Definitions.* For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that

has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

SEC. 1.2. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

SEC. 1.3. *Classification Levels.* (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

SEC. 1.4. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

SEC. 1.5. *Classification Categories.*

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

SEC. 1.6. *Duration of Classification.* (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair the development or use of technology within a United States weapons system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

SEC. 1.7. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from declassification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

SEC. 1.8. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

SEC. 1.9. *Classification Challenges.* (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

## PART 2—DERIVATIVE CLASSIFICATION

SEC. 2.1. *Definitions.* For purposes of this order:

(a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

SEC. 2.2. *Use of Derivative Classification.* (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

SEC. 2.3. *Classification Guides.* (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative

classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

- (1) has program or supervisory responsibility over the information or is the senior agency official; and
- (2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

#### PART 3—DECLASSIFICATION AND DOWNGRADING

SEC. 3.1. *Definitions.* For purposes of this order:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

- (1) the occurrence of a specific date or event as determined by the original classification authority; or
- (2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

- (1) the official who authorized the original classification, if that official is still serving in the same position;
- (2) the originator's current successor in function;
- (3) a supervisory official of either; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

SEC. 3.2. *Authority for Declassification.* (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in

violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

SEC. 3.3. *Transferred Information.* (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act [probably means chapters 21 to 31 of Title 44, Public Printing and Documents]. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

SEC. 3.4. *Automatic Declassification.* (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

- (1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;
- (2) reveal information that would assist in the development or use of weapons of mass destruction;
- (3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the

mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

SEC. 3.5. *Systematic Declassification Review.* (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

SEC. 3.6. *Mandatory Declassification Review.* (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act [see Short Title of 1984 Amendment note, set out under section 401 of this title]; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or



(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

**SEC. 3.7. Processing Requests and Reviews.** In response to a request for information under the Freedom of Information Act [5 U.S.C. 552], the Privacy Act of 1974 [5 U.S.C. 552a], or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

**SEC. 3.8. Declassification Database.** (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the

database established under paragraph (a), above, shall be available to the public.

#### PART 4—SAFEGUARDING

**SEC. 4.1. Definitions.** For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

**SEC. 4.2. General Restrictions on Access.** (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a

need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

**SEC. 4.3. Distribution Controls.** (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

**SEC. 4.4. Special Access Programs.** (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

- (1) the vulnerability of, or threat to, specific information is exceptional; and
- (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or
- (3) the program is required by statute.

(b) *Requirements and Limitations.* (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy

validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

**SEC. 4.5. Access by Historical Researchers and Former Presidential Appointees.** (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

- (1) are engaged in historical research projects; or
  - (2) previously have occupied policy-making positions to which they were appointed by the President.
- (b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

- (1) determines in writing that access is consistent with the interest of national security;
- (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and
- (3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

#### PART 5—IMPLEMENTATION AND REVIEW

**SEC. 5.1. Definitions.** For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

- (1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
  - (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
  - (3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.
- (c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

**SEC. 5.2. Program Direction.** (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

- (1) classification and marking principles;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

**SEC. 5.3. Information Security Oversight Office.** (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget

shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;
- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
- (7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
- (8) report at least annually to the President on the implementation of this order; and
- (9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

**SEC. 5.4. Interagency Security Classification Appeals Panel.**

- (a) Establishment and Administration.
- (1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.
  - (2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.
  - (3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.
  - (4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.
  - (5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.
  - (6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.
- (b) *Functions.* The Panel shall:
- (1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

- (2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

- (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) *Rules and Procedures.* The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

**SEC. 5.5. Information Security Policy Advisory Council.**

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) *Functions.* The Council shall:

- (1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;

- (2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

- (3) serve as a forum to discuss policy issues in dispute.

(c) *Meetings.* The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) *Administration.*

- (1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

- (2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

- (3) To the extent permitted by law and subject to the availability of funds, the Information Security

Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended [5 App. U.S.C.], that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

SEC. 5.6. *General Responsibilities.* Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order; and

(c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

SEC. 5.7. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

#### PART 6—GENERAL PROVISIONS

SEC. 6.1. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 *et seq.*], or the National Security Act of 1947, as amended [act July 26, 1947, see Short Title note set out under section 401 of this title]. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act [5 U.S.C. 552], the Privacy Act [5 U.S.C. 552a], and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

SEC. 6.2. *Effective Date.* This order shall become effective 180 days from the date of this order.

WILLIAM J. CLINTON.

#### OFFICIALS DESIGNATED TO CLASSIFY NATIONAL SECURITY INFORMATION

Order of President of the United States, dated Oct. 13, 1995, 60 F.R. 53845, provided:

Pursuant to the provisions of Section 1.4 of Executive Order No. 12958 of April 17, 1995, entitled "Classified National Security Information," [set out above] I hereby designate the following officials to classify information originally as "Top Secret", "Secret", or "Confidential":

#### TOP SECRET

##### EXECUTIVE OFFICE OF THE PRESIDENT:

The Vice President  
 The Chief of Staff to the President  
 The Director, Office of Management and Budget  
 The Assistant to the President for National Security Affairs  
 The Director, Office of National Drug Control Policy  
 The Chairman, President's Foreign Intelligence Advisory Board

## DEPARTMENTS AND AGENCIES:

The Secretary of State  
 The Secretary of the Treasury  
 The Secretary of Defense  
 The Secretary of the Army  
 The Secretary of the Navy  
 The Secretary of the Air Force  
 The Attorney General  
 The Secretary of Energy  
 The Chairman, Nuclear Regulatory Commission  
 The Director, United States Arms Control and Disarmament Agency  
 The Director of Central Intelligence  
 The Administrator, National Aeronautics and Space Administration  
 The Director, Federal Emergency Management Agency

## SECRET

## EXECUTIVE OFFICE OF THE PRESIDENT:

The United States Trade Representative  
 The Chairman, Council of Economic Advisers  
 The Director, Office of Science and Technology Policy

## DEPARTMENTS AND AGENCIES:

The Secretary of Commerce  
 The Secretary of Transportation  
 The Administrator, Agency for International Development  
 The Director, United States Information Agency

## CONFIDENTIAL

The President, Export-Import Bank of the United States  
 The President, Overseas Private Investment Corporation

Any delegation of this authority shall be in accordance with Section 1.4(c) of Executive Order No. 12958.

This Order shall be published in the Federal Register.

WILLIAM J. CLINTON.

Order of President of the United States, dated Feb. 27, 1996, 61 F.R. 7977, provided:

Pursuant to the provisions of section 1.4 of Executive Order No. 12958 of April 17, 1995, entitled "Classified National Security Information," [set out above] I hereby designate the following additional officials to classify information originally as "Top Secret":

The Chair, Commission on the Roles and Capabilities of the United States Intelligence Community

The Director, National Counterintelligence Center

The Chair of the Commission on the Roles and Capabilities of the United States Intelligence Community, shall exercise the authority to classify information originally as "Top Secret" during the existence of the Commission and for such time afterwards as may be necessary to complete the Commission's administrative affairs.

The authority of the Director of the National Counterintelligence Center to classify information originally as "Top Secret" is limited to those circumstances in which the original classification of information is necessary in order for the Center to fulfill its mission and functions.

Any delegation of this authority shall be in accordance with section 1.4(c) of Executive Order No. 12958.

This order shall be published in the Federal Register.

WILLIAM J. CLINTON.

## EX. ORD. NO. 12968. ACCESS TO CLASSIFIED INFORMATION

Ex. Ord. No. 12968, Aug. 2, 1995, 60 F.R. 40245, provided:

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can

cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

## PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS

SECTION 1.1. *Definitions.* For the purposes of this order: (a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation 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.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958 [set out above], or any successor order, Executive Order No. 12951 [set out above], or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 [et seq.]), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) "Special access program" has the meaning provided in section 4.1 of Executive Order No. 12958 [set out above], or any successor order.

SEC. 1.2. *Access to Classified Information.* (a) No employee shall be granted access to classified information

unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401(6));

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a [1681 *et seq.*]); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act [of 1978, 12 U.S.C. 3401 *et seq.*], the Fair Credit Reporting Act [15 U.S.C. 1681 *et seq.*] or any other applicable law.

SEC. 1.3. *Financial Disclosure.* (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 *et seq.*);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of:

(A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but

not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended [42 U.S.C. 2165(f)]).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

SEC. 1.4. *Use of Automated Financial Record Data Bases.* As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

SEC. 1.5. *Employee Education and Assistance.* The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to: (a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

## PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

SEC. 2.1. *Eligibility Determinations.* (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

SEC. 2.2. *Level of Access Approval.* (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

SEC. 2.3. *Temporary Access to Higher Levels.* (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

- (1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;
- (2) will not exceed 180 days; and
- (3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

SEC. 2.4. *Reciprocal Acceptance of Access Eligibility Determinations.* (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be

conveyed to any other agency that considers affording the employee access to its information.

SEC. 2.5. *Specific Access Requirement.* (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

SEC. 2.6. *Access by Non-United States Citizens.* (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

#### PART 3—ACCESS ELIGIBILITY STANDARDS

SEC. 3.1. *Standards.* (a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further

inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

SEC. 3.2. *Basis for Eligibility Approval.* (a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

SEC. 3.3. *Special Circumstances.* (a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed

within the prior 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

SEC. 3.4. *Reinvestigation Requirements.* (a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

#### PART 4—INVESTIGATIONS FOR FOREIGN GOVERNMENTS

SEC. 4. *Authority.* Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

#### PART 5—REVIEW OF ACCESS DETERMINATIONS

SEC. 5.1. *Determinations of Need for Access.* A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

SEC. 5.2. *Review Proceedings for Denials or Revocations of Eligibility for Access.* (a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative



or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

#### PART 6—IMPLEMENTATION

SEC. 6.1. *Agency Implementing Responsibilities.* Heads of agencies that grant employees access to classified information shall: (a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

SEC. 6.2. *Employee Responsibilities.* (a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

SEC. 6.3. *Security Policy Board Responsibilities and Implementation.* (a) With respect to actions taken by the Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Security Policy Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

SEC. 6.4. *Sanctions.* Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

#### PART 7—GENERAL PROVISIONS

SEC. 7.1. *Classified Information Procedures Act.* Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App.).

SEC. 7.2. *General.* (a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

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

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

(3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450 [5 U.S.C. 7311 note], the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended [set out above], or access by historical researchers and former presidential appointees under Executive Order No. 12958 [set out above] or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.

WILLIAM J. CLINTON.

**§ 436. Requests by authorized investigative agencies**

**(a) Generally**

(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer 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 an employee in the executive branch of Government 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 in the executive branch of Government 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 three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, 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 the employing agency deems credible indicates 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) of this section.

**(b) Disclosure of requests**

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) Records or information; inspection or copying**

(1) Notwithstanding any other provision of law (other than section 6103 of title 26), an entity receiving a request for records or information under subsection (a) of this section 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 subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

**(d) Reimbursement of costs**

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) Dissemination of records or information received**

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) Construction of section**

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.).

(July 26, 1947, ch. 343, title VIII, §802, as added Oct. 14, 1994, Pub. L. 103-359, title VIII, §802(a), 108 Stat. 3436.)