provisions of section 552 of title 5 (commonly referred to as the Freedom of Information Act), and such order shall be the exclusive remedy for failure to comply with this section.

(F) If at any time following the filing of a complaint pursuant to this paragraph the Office agrees to search each appropriate exempted file for the requested records, the court shall dismiss the claim based upon such complaint.

(g) Definitions

In this section:

(1) The term ''exempted operational file'' means a file of an element of the intelligence community that, in accordance with this subchapter, is exempted from the provisions of section 552 of title 5 that require search, review, publication, or disclosure of such file.

(2) Except as otherwise specifically provided, the term ''Office'' means the Office of the Director of National Intelligence.

(July 26, 1947, ch. 343, title VII, § 706, as added Pub. L. 111–259, title IV, § 408(a), Oct. 7, 2010, 124 Stat. 2722.)

Editorial Notes

REFERENCES IN TEXT

The Federal Rules of Civil Procedure, referred to in subsec. (f)(2)(D), are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

CODIFICATION

Section was formerly classified to section 432d of this title prior to editorial reclassification and renumbering as this section.

SUBCHAPTER VI—ACCESS TO CLASSIFIED INFORMATION

§ 3161. 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, travel records, and computers used in the performance of Government duties, as determined by the President, in accordance with section 3162 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) 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) 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 congressional intelligence committees.

(July 26, 1947, ch. 343, title VIII, § 801, as added Pub. L. 103–359, title VIII, § 802(a), Oct. 14, 1994, 108 Stat. 3435; amended Pub. L. 106–120, title III, § 305(a), Dec. 3, 1999, 113 Stat. 1611; Pub. L. 107–306, title III, § 353(b)(2)(B), Nov. 27, 2002, 116 Stat. 2402.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 435 of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2002—Subsec. (b)(2). Pub. L. 107–306 substituted ''congressional intelligence committees'' for ''Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate''.

1999—Subsec. (a)(3). Pub. L. 106–120 substituted ''travel records, and computers used in the performance of Government duties'' for ''and travel records''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 1999 AMENDMENT

Pub. L. 106–120, title III, § 305(c), Dec. 3, 1999, 113 Stat. 1612, provided that: ''The President shall modify the

procedures required by section 801(a)(3) of the National Security Act of 1947 [50 U.S.C. 3161(a)(3)] to take into account the amendment to that section made by subsection (a) of this section not later than 90 days after the date of the enactment of this Act [Dec. 3, 1999].''

EFFECTIVE DATE

Pub. L. 103–359, title VIII, § 802(c), Oct. 14, 1994, 108 Stat. 3438, 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].''

INTELLIGENCE COMMUNITY-WIDE POLICY ON PREPUBLICATION REVIEW

Pub. L. 118–31, div. G, title III, § 7322, Dec. 22, 2023, 137 Stat. 1038, provided that: ''Not later than 30 days after the date of the enactment of this Act [Dec. 22, 2023], the Director of National Intelligence shall issue, and submit to the congressional intelligence committees, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate, and the Committee on the Judiciary, the Committee on Oversight and Accountability, and the Committee on Appropriations of the House of Representatives, an intelligence community-wide policy regarding prepublication review.''

[For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in section 7322 of Pub. L. 118–31, set out above, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.]

DECLASSIFICATION OF INFORMATION RELATED TO THE ORIGIN OF COVID–19

Pub. L. 118–2, Mar. 20, 2023, 137 Stat. 4, provided that:

''SECTION 1. SHORT TITLE.

''This Act may be cited as the 'COVID–19 Origin Act of 2023'.

''SEC. 2. SENSE OF CONGRESS.

''It is the sense of Congress that—

''(1) identifying the origin of Coronavirus Disease 2019 (COVID–19) is critical for preventing a similar pandemic from occurring in the future;

''(2) there is reason to believe the COVID–19 pandemic may have originated at the Wuhan Institute of Virology; and

''(3) the Director of National Intelligence should declassify and make available to the public as much information as possible about the origin of COVID–19 so the United States and like-minded countries can—

''(A) identify the origin of COVID–19 as expeditiously as possible, and

''(B) use that information to take all appropriate measures to prevent a similar pandemic from occurring again.

''SEC. 3. DECLASSIFICATION OF INFORMATION RELATED TO THE ORIGIN OF COVID–19.

''Not later than 90 days after the date of the enactment of this Act [Mar. 20, 2023], the Director of National Intelligence shall—

''(1) declassify any and all information relating to potential links between the Wuhan Institute of Virology and the origin of the Coronavirus Disease 2019 (COVID–19), including—

''(A) activities performed by the Wuhan Institute of Virology with or on behalf of the People's Liberation Army;

''(B) coronavirus research or other related activities performed at the Wuhan Institute of Virology prior to the outbreak of COVID–19; and

''(C) researchers at the Wuhan Institute of Virology who fell ill in autumn 2019, including for any such researcher—

''(i) the researcher's name;

''(ii) the researcher's symptoms;

''(iii) the date of the onset of the researcher's symptoms;

''(iv) the researcher's role at the Wuhan Institute of Virology;

''(v) whether the researcher was involved with or exposed to coronavirus research at the Wuhan Institute of Virology;

''(vi) whether the researcher visited a hospital while they were ill; and

''(vii) a description of any other actions taken by the researcher that may suggest they were experiencing a serious illness at the time; and

''(2) submit to Congress an unclassified report that contains—

''(A) all of the information described under paragraph (1); and

''(B) only such redactions as the Director determines necessary to protect sources and methods.''

DIRECTOR OF NATIONAL INTELLIGENCE DECLASSIFICATION REVIEW OF INFORMATION RELATING TO TERRORIST ATTACKS OF SEPTEMBER 11, 2001

Pub. L. 117–103, div. X, title III, § 310, Mar. 15, 2022, 136 Stat. 972, provided that:

''(a) DECLASSIFICATION REVIEW REQUIRED.—Not later than 30 days after the date of the enactment of this Act [Mar. 15, 2022], the Director of National Intelligence shall, in coordination with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, and the heads of such other elements of the intelligence community as the Director of National Intelligence considers appropriate, commence a declassification review (which the Director of National Intelligence shall complete by not later than 120 days after the date of the enactment of this Act) to determine what, if any, additional information relating to the terrorist attacks of September 11, 2001, can be appropriately declassified and shared with the public.

''(b) INFORMATION COVERED.—The information reviewed under subsection (a) shall include the following:

''(1) Information relating to the direction, facilitation, and other support provided to the individuals who carried out the terrorist attacks of September 11, 2001.

''(2) Information from Operation Encore and the PENTTBOM investigation of the Federal Bureau of Investigation.

''(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the findings of the Director with respect to the declassification review conducted under subsection (a).''

[For definitions of ''congressional intelligence committees'' and ''intelligence community'' as used in section 310 of div. X of Pub. L. 117–103, set out above, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.]

EFFICIENT USE OF SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Pub. L. 116–283, div. A, title XVI, § 1623, Jan. 1, 2021, 134 Stat. 4056, provided that: ''Not later than 180 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of National Intelligence, in consultation with the Secretary of Defense, shall issue revised guidance authorizing and directing departments and agencies of the Federal Government and appropriately cleared contractors of such departments and agencies to process, store, use, and discuss sensitive compartmented information at facilities previously approved to handle such information, without need for further approval by the department or agency or by the site. Such guidance shall apply to controlled access programs of the intelligence community and to special access programs of the Department of Defense.''

TRUSTED INFORMATION PROVIDER PROGRAM FOR NATIONAL SECURITY POSITIONS AND POSITIONS OF TRUST

Pub. L. 115–232, div. A, title IX, § 941, Aug. 13, 2018, 132 Stat. 1941, formerly set out as a note under this section,

was transferred and is set out as a note under section 3352f of this title.

REVIEW OF POSITION DESIGNATIONS FOR DETERMINING APPROPRIATE BACKGROUND INVESTIGATIONS

Pub. L. 115–173, §§ 2, 7, May 22, 2018, 132 Stat. 1291, 1293, provided that:

''SEC. 2. DEFINITIONS.

''In this Act [see Short Title of 2018 Amendment note set out under section 3001 of this title]—

''(1) the term 'Bureau' means the National Background Investigations Bureau of the Office;

''(2) the term 'Director' means the Director of National Intelligence acting as the Security Executive Agent; and

''(3) the term 'Office' means the Office of Personnel Management acting as the Suitability and Credentialing Executive Agent.

''SEC. 7. REVIEW AND UPDATE OF POSITION DESIGNATION GUIDANCE.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given the term in Executive Order 13467 (73 Fed. Reg. 38103) [set out below], or any successor thereto;

''(2) the term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate; and

''(B) the Committee on Oversight and Government Reform [now Committee on Oversight and Accountability] and the Permanent Select Committee on Intelligence of the House of Representatives;

''(3) the term 'background investigation' means any investigation required for the purpose of determining the—

''(A) eligibility of a covered individual for logical and physical access to Federally controlled facilities or information systems;

''(B) suitability or fitness of a covered individual for Federal employment;

''(C) eligibility of a covered individual for access to classified information or to hold a national security sensitive position; or

''(D) fitness of a covered individual to perform work for or on behalf of the United States Government as a contractor employee; and

''(4) the term 'covered individual'—

''(A) means a person who performs work for or on behalf of the executive branch or seeks to perform work for or on behalf of the executive branch;

''(B) is not limited to Federal employees;

''(C) includes all persons, not excluded under subparagraph (D), who require eligibility for access to classified information or eligibility to hold a sensitive position, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees; and

''(D) does not include—

''(i) the President;

''(ii) employees of the President under section 105 or 107 of title 3, United States Code (except to the extent otherwise directed by the President);

''(iii) the Vice President; or

''(iv) employees of the Vice President under section 106 of title 3, United States Code, or an annual legislative branch appropriations Act (except to the extent otherwise directed by the Vice President).

''(b) REVIEW AND UPDATING.—

''(1) INITIAL REVIEW AND UPDATE OF GUIDANCE.—Not later than 180 days after the date of enactment of this Act [May 22, 2018], the Director and the Director of the Office shall review and make recommendations to Congress and the President as appropriate to issue guidance to assist agencies in determining—

''(A) position sensitivity designation; and

''(B) the appropriate background investigation to initiate for each position designation.

''(2) REVIEWS AND REVISIONS OF POSITION DESIGNATIONS.—Not less frequently than every 4 years, the President, acting through relevant agencies (as determined by the President) and in accordance with the guidance described in paragraph (1), shall review and, if necessary, revise the position designation of positions within agencies.

''(c) REPORTS TO CONGRESS.—Not later than 30 days after completing a review under subsection (b)(2), the President shall submit to the appropriate congressional committees a report on—

''(1) any issues identified in the review; and

''(2) the number of position designations revised as a result of the review.

''(d) NO CHANGE IN AUTHORITY.—Nothing in this section limits or expands the authority of any agency to designate a position as sensitive or as requiring its occupant to have access to classified information.''

CLASSIFICATION REVIEW OF EXECUTIVE BRANCH MATERIALS IN THE POSSESSION OF THE CONGRESSIONAL INTELLIGENCE COMMITTEES

Pub. L. 111–259, title VII, § 702, Oct. 7, 2010, 124 Stat. 2745, provided that: ''The Director of National Intelligence is authorized to conduct, at the request of one of the congressional intelligence committees and in accordance with procedures established by that committee, a classification review of materials in the possession of that committee that—

''(1) are not less than 25 years old; and

''(2) were created, or provided to that committee, by an entity in the executive branch.''

[For definition of ''congressional intelligence committees'' as used in section 702 of Pub. L. 111–259, set out above, see section 2 of Pub. L. 111–259, set out as a note under section 3003 of this title.]

PROMOTION OF ACCURATE CLASSIFICATION OF INFORMATION

Pub. L. 111–258, § 6, Oct. 7, 2010, 124 Stat. 2651, provided that:

''(a) INCENTIVES FOR ACCURATE CLASSIFICATIONS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an Executive agency with an officer or employee who is authorized to make original classification decisions or derivative classification decisions may consider such officer's or employee's consistent and proper classification of information.

''(b) INSPECTOR GENERAL EVALUATIONS.—

''(1) REQUIREMENT FOR EVALUATIONS.—Not later than September 30, 2016, the inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency—

''(A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and

''(B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.

''(2) DEADLINES FOR EVALUATIONS.—

''(A) INITIAL EVALUATIONS.—Each first evaluation required by paragraph (1) shall be completed no later than September 30, 2013.

''(B) SECOND EVALUATIONS.—Each second evaluation required by paragraph (1) shall review progress made pursuant to the results of the first evaluation and shall be completed no later than September 30, 2016.

''(3) REPORTS.—

''(A) REQUIREMENT.—Each inspector general who is required to carry out an evaluation under paragraph (1) shall submit to the appropriate entities a report on each such evaluation.

''(B) CONTENT.—Each report submitted under subparagraph (A) shall include a description of—

''(i) the policies, procedures, rules, regulations, or management practices, if any, identified by the inspector general under paragraph (1)(B); and

''(ii) the recommendations, if any, of the inspector general to address any such identified policies, procedures, rules, regulations, or management practices.

''(C) COORDINATION.—The inspectors general who are required to carry out evaluations under paragraph (1) shall coordinate with each other and with the Information Security Oversight Office to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons.

''(4) APPROPRIATE ENTITIES DEFINED.—In this subsection, the term 'appropriate entities' means—

''(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate;

''(B) the Committee on Homeland Security, the Committee on Oversight and Government Reform [now Committee on Oversight and Accountability], and the Permanent Select Committee on Intelligence of the House of Representatives;

''(C) any other committee of Congress with jurisdiction over a department or agency referred to in paragraph (1);

''(D) the head of a department or agency referred to in paragraph (1); and

''(E) the Director of the Information Security Oversight Office.''

[For definitions of terms used in section 6 of Pub. L. 111–258, set out above, see section 3 of Pub. L. 111–258, set out as a note under section 3344 of this title.]

DECLASSIFICATION OF INFORMATION

Pub. L. 106–567, title VII, Dec. 27, 2000, 114 Stat. 2856, as amended by Pub. L. 108–458, title I, §1102, Dec. 17, 2004, 118 Stat. 3699; Pub. L. 110–53, title VI, §602, Aug. 3, 2007, 121 Stat. 335; Pub. L. 111–259, title III, §365, Oct. 7, 2010, 124 Stat. 2702; Pub. L. 112–235, §2, Dec. 28, 2012, 126 Stat. 1626; Pub. L. 113–126, title III, §311, July 7, 2014, 128 Stat. 1399, known as the Public Interest Declassification Act of 2000 and formerly set out as a note under this section, was transferred to subchapter III–A (§3355 et seq.) of chapter 45 of this title.

CERTIFICATION AND REPORT RELATED TO AUTOMATIC DECLASSIFICATION OF DEPARTMENT OF DEFENSE RECORDS

Pub. L. 106–65, div. A, title X, §1041(c), (d), Oct. 5, 1999, 113 Stat. 758, provided that:

''(c) CERTIFICATION REQUIRED WITH RESPECT TO AUTOMATIC DECLASSIFICATION OF RECORDS.—No records of the Department of Defense that have not been reviewed for declassification shall be subject to automatic declassification unless the Secretary of Defense certifies to Congress that such declassification would not harm the national security.

''(d) REPORT ON AUTOMATIC DECLASSIFICATION OF DEPARTMENT OF DEFENSE RECORDS.—Not later than February 1, 2001, the Secretary of Defense shall submit to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate a report on the efforts of the Department of Defense relating to the declassification of classified records under the control of the Department of Defense. Such report shall include the following:

''(1) An assessment of whether the Department will be able to review all relevant records for declassification before any date established for automatic declassification.

''(2) An estimate of the cost of reviewing records to meet any requirement to review all relevant records for declassification by a date established for automatic declassification.

''(3) An estimate of the number of records, if any, that the Department will be unable to review for declassification before any such date and the affect [sic] on national security of the automatic declassification of those records.

''(4) An estimate of the length of time by which any such date would need to be extended to avoid the automatic declassification of records that have not yet been reviewed as of such date.''

SUPPLEMENT TO PLAN FOR DECLASSIFICATION OF RESTRICTED DATA AND FORMERLY RESTRICTED DATA

Pub. L. 106–65, div. C, title XXXI, §3149, Oct. 5, 1999, 113 Stat. 938, which was formerly set out as a note under this section, was renumbered section 4523 of Pub. L. 107–314, the Bob Stump National Defense Authorization Act for Fiscal Year 2003, by Pub. L. 108–136, div. C, title XXXI, §3141(h)(13)(A)–(C), Nov. 24, 2003, 117 Stat. 1775, and is classified to section 2673 of this title.

IDENTIFICATION IN BUDGET MATERIALS OF AMOUNTS FOR DECLASSIFICATION ACTIVITIES AND LIMITATION ON EXPENDITURES FOR SUCH ACTIVITIES

Pub. L. 106–65, div. C, title XXXI, §3173, Oct. 5, 1999, 113 Stat. 949, which was formerly set out as a note under this section, was renumbered section 4525 of Pub. L. 107–314, the Bob Stump National Defense Authorization Act for Fiscal Year 2003, by Pub. L. 108–136, div. C, title XXXI, §3141(h)(15)(A)–(C), Nov. 24, 2003, 117 Stat. 1775, and is classified to section 2675 of this title.

PROTECTION AGAINST INADVERTENT RELEASE OF RESTRICTED DATA AND FORMERLY RESTRICTED DATA

Pub. L. 105–261, div. C, title XXXI, §3161, Oct. 17, 1998, 112 Stat. 2259, as amended by Pub. L. 106–65, div. A, title X, §1067(3), Oct. 5, 1999, 113 Stat. 774; Pub. L. 106–398, §1 [div. C, title XXXI, §3193(a)], Oct. 30, 2000, 114 Stat. 1654, 1654A–480, which was formerly set out as a note under this section, was renumbered section 4522 of Pub. L. 107–314, the Bob Stump National Defense Authorization Act for Fiscal Year 2003, by Pub. L. 108–136, div. C, title XXXI, §3141(h)(12)(A)–(C), Nov. 24, 2003, 117 Stat. 1774, and is classified to section 2672 of this title.

VOLUNTARY SERVICE PROGRAM

Pub. L. 104–93, title IV, §402, Jan. 6, 1996, 109 Stat. 969, authorized the Director of Central Intelligence to establish and maintain a program from fiscal years 1996 through 2001 to utilize the services contributed by not more than 50 annuitants who served 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 Pub. L. 102–526 (44 U.S.C. 2107 note).

COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY

Pub. L. 103–236, title IX, Apr. 30, 1994, 108 Stat. 525, known as the ''Protection and Reduction of Government Secrecy Act'', established for a two-year period a Commission on Protecting and Reducing Government Secrecy to conduct 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 to submit to the Congress a final report containing such recommendations not later than two years after the date of the first meeting of the Commission and terminated Commission 60 days after the date on which a final report is submitted (final report submitted on Mar. 3, 1997).

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 Documents

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; Ex. Ord. No. 13284, §15, Jan. 23, 2003, 68 F.R. 4076, 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 Secretary of Homeland Security, 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, formerly 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; Ex. Ord. No. 13691, §6, Feb. 13, 2015, 80 F.R. 9351; Ex. Ord. No. 13708, §4, Sept. 30, 2015, 80 F.R. 60273, 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 nongovernment 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) [50 U.S.C. 3001 et seq.], the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458, see Tables for classification], and the Federal Advisory Committee Act, as amended ([former] 5 U.S.C. App. 2) [see 5 U.S.C. 1001 et seq.], 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 13526 of December 29, 2009 [set out below], or any predecessor or successor order, 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) In consultation with the National Security Advisor, the Director of the Information Security Oversight Office, in accordance with Executive Order 13526 of December 29, 2009, 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 National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458, see Tables for classification], the National Security Act of 1947, as amended [50 U.S.C. 3001 et seq.], or Executive Order 12333 of December 8, 1981 [50 U.S.C. 3001 note], as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities) [set out below].

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 National Archives and Records Administration 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 [see 5 U.S.C. 1001 et seq.], except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the the [sic] Archivist of the United States 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, the Director of National Intelligence, and the Secretary of Homeland Security, 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 National Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Secretary of Homeland Security shall prescribe and issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program.

(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) The Manual shall also prescribe arrangements necessary to permit and enable secure sharing of classified information under a designated critical infrastructure protection program to such authorized individuals and organizations as determined by the Secretary of Homeland Security.

(e) In establishing particular requirements, restrictions, and other safeguards within the Manual, the Secretary of Defense, the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security 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.

(f) 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 13526 of December 29, 2009 [set out below], or any successor order, 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.

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 National Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of National Intelligence 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, or with the Director of the Central Intelligence Agency 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 information 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 Secretary of Homeland Security may determine the eligibility for access to Classified National Security Information of contractors, licensees, and grantees and their respective employees under a designated critical infrastructure protection program, including parties to agreements with such program; the Secretary of Homeland Security may inspect and monitor contractor, licensee, and grantee programs and facilities or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency, to inspect and monitor these programs or facilities in whole or in part, on behalf of the Secretary of Homeland Security.

(e) 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) [Amended Ex. Ord. No. 10865, set out above.]

(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.

EXTENSION OF TERM OF NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE

Term of National Industrial Security Program Policy Advisory Committee extended until Sept. 30, 2025, by Ex. Ord. No. 14109, Sept. 29, 2023, 88 F.R. 68447, set out as a note under section 1013 of Title 5, Government Organization and Employees.

Previous extensions of term of National Industrial Security Program Policy Advisory Committee were contained in the following prior Executive Orders:

Ex. Ord. No. 14048, Sept. 30, 2021, 86 F.R. 55465, extended term until Sept. 30, 2023.

Ex. Ord. No. 13889, Sept. 27, 2019, 84 F.R. 52743, extended term until Sept. 30, 2021.

Ex. Ord. No. 13811, Sept. 29, 2017, 82 F.R. 46363, extended term until Sept. 30, 2019.

Ex. Ord. No. 13708, Sept. 30, 2015, 80 F.R. 60271, extended term until Sept. 30, 2017.

Ex. Ord. No. 13652, Sept. 30, 2013, 78 F.R. 61817, extended term until Sept. 30, 2015.

Ex. Ord. No. 13585, Sept. 30, 2011, 76 F.R. 62281, extended term until Sept. 30, 2013.

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 declas-

sified. 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.

EXECUTIVE ORDER NO. 12958

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; Ex. Ord. No. 13142, Nov. 19, 1999, 64 F.R. 66089; Ex. Ord. No. 13292, Mar. 25, 2003, 68 F.R. 15315, which related to classified national security information, was revoked by Ex. Ord. No. 13526, § 6.2(g), Dec. 29, 2009, 75 F.R. 731, set out below.

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

Ex. Ord. No. 12968, Aug. 2, 1995, 60 F.R. 40245, as amended by Ex. Ord. No. 13467, § 3(b), June 30, 2008, 73 F.R. 38107; Ex. Ord. No. 13764, § 3(v), Jan. 17, 2017, 82 F.R. 8128, 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 [formerly 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 Executive Agent'' 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 Executive Agent'' means the Security Executive Agent 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 [formerly 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 [sic] [et seq.]) [now 50 U.S.C. 3121 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 Executive Agent.

(c) Not later than 180 days after the effective date of this order, the Security Executive Agent 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 or appropriate automated procedures. 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 Executive Agent 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 Executive Agent 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 Executive Agent 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 fa-

vorable 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 Executive Agent shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

SEC. 3.5. *Continuous Evaluation*. An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation as further defined by and under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.

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 (5 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 Executive Agent, 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 Executive Agent.

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 Executive Agent Responsibilities and Implementation*. (a) With respect to actions taken by the Security Executive Agent pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Director of National Intelligence shall serve as the final authority for implementation.
(b) Any guidelines, standards, or procedures developed by the Security Executive Agent 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 Executive Agent shall consult where appropriate with the Overseas Security Executive Agent. In carrying out its responsibilities under section 1.3(c) of this order, the Security Executive Agent 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 [formerly 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.

EX. ORD. NO. 13467. REFORMING PROCESSES RELATED TO SUITABILITY FOR GOVERNMENT EMPLOYMENT, FITNESS FOR CONTRACTOR EMPLOYEES, AND ELIGIBILITY FOR ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION

Ex. Ord. No. 13467, June 30, 2008, 73 F.R. 38103, as amended by Ex. Ord. No. 13741, §1, Sept. 29, 2016, 81 F.R. 68289; Ex. Ord. No. 13764, §3, Jan. 17, 2017, 82 F.R. 8117; Ex. Ord. No. 13869, §2, Apr. 24, 2019, 84 F.R. 18125, provided:
By the authority vested in me as President by the Constitution and the laws of the United States of America, including sections 3301, 7103(b), and 7301 of title 5, United States Code, and in order to strengthen and ensure a secure, efficient, timely, reciprocal, and aligned system for investigating and determining suitability or fitness for Government employment, fitness to work as a contractor or a nonappropriated fund employee, eligibility for access to classified information or to hold a sensitive position, and authorization to be issued a Federal credential, while providing fair, impartial, and equitable treatment, and protecting individual rights under the Constitution and laws of the United States, and taking appropriate account of title III of Public Law 108–458, it is hereby ordered as follows:

PART 1—POLICY, APPLICABILITY, AND DEFINITIONS

SECTION 1.1. *Policy*. (a) Executive branch vetting policies and procedures relating to suitability, contractor or Federal employee fitness, eligibility to hold a sensitive position, authorization to be issued a Federal credential for access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, shall provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.
(b) The Government's tools, systems, and processes for conducting these background investigations and managing sensitive investigative information should keep pace with technological advancements, regularly integrating current best practices to better anticipate, detect, and counter malicious activities, and threats posed by external or internal actors who may seek to do harm to the Government's personnel, property, and information. To help fulfill these responsibilities, there shall be a primary executive branch investigative service provider whose mission is to provide effective, efficient, and secure background investigations for the Federal Government.
(c) Executive branch vetting policies and procedures shall be sustained by an enhanced risk-management approach that facilitates early detection of issues by an informed, aware, and responsible Federal workforce; results in quality decisions enabled by improved vetting capabilities; and advances Government-wide capabilities through enterprise approaches.
(d) The appointment or retention of each covered individual shall be subject to an investigation. Federal investigative standards established pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security, and the scope of the investigation shall be determined in the first instance according to the degree of material adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security.'' [sic]
(e) Investigative agencies shall control the reports, information, and other investigative materials that are developed during the vetting process. Recipient departments and agencies may retain and use the received re-

ports, information, and other investigative material within that recipient for authorized purposes (including, but not limited to, adjudications, hearings and appeals, continuous evaluation, inspector general functions, counterintelligence, research, and insider threat programs), in compliance with the Privacy Act of 1974, as amended (section 552a of title 5, United States Code). Investigative agencies shall ensure that their applicable System of Records Notices include, at a minimum, the authorized uses of the recipient departments and agencies such as those set forth above. Recipient departments and agencies shall not make any external releases of received information, other than to an investigative subject for the purpose of providing procedural rights or administrative due process; and shall direct any other requests for external releases of copies of the reports, information, and other investigative materials to the investigative agency. In the event redisclosure by the recipient agency is required by compulsory legal process, the recipient agency shall consult with the investigating agency. The investigative agency shall maintain the reports, information, and other investigative material in a system of records subject to the Privacy Act and ensure that any re-disclosure does not violate statutory restrictions or result in the unauthorized disclosure of: classified information, information subject to a claim of privilege, or information that is otherwise lawfully exempt from disclosure. Subject to Security Executive Agent authorizations consistent with section 3341(e)(5) of title 50, United States Code, the investigative agencies shall make reports, information, and other investigative material available, as necessary, to carry out the responsibilities set forth in this order, including but not limited to, authorized executive branch-sponsored research and initiatives for enterprise-wide continuous performance improvement of vetting policy and procedures, as permitted by law.

SEC. 1.2. *Applicability*. (a) This order applies to vetting of all covered individuals as defined in section 1.3(h), except that:

(i) the provisions regarding eligibility for physical access to federally controlled facilities and logical access to federally controlled information systems do not apply to individuals exempted in accordance with guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12 of August 27, 2004; and

(ii) the qualification standards for enlistment, appointment, and induction into the Armed Forces pursuant to title 10, United States Code, are unaffected by this order.

(b) This order also applies to vetting for employees of agencies working in or for the legislative or judicial branches when the vetting is conducted by the executive branch.

SEC. 1.3. *Definitions*. For the purpose of this order: (a) ''Adjudication'' means the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is:

(i) suitable for Government employment;

(ii) eligible for logical and physical access;

(iii) eligible for access to classified information;

(iv) eligible to hold a sensitive position; or

(v) fit to perform work for or on behalf of the Government as a Federal employee, contractor, or nonappropriated fund employee.

(b) ''Agency'' means any ''Executive agency'' as defined in section 105 of title 5, United States Code, including the ''military departments,'' as defined in section 102 of title 5, United States Code, and any other entity within the executive branch that comes into possession of classified information or has designated positions as sensitive, except such an entity headed by an officer who is not a covered individual.

(c) ''Classified information'' means information that has been determined pursuant to Executive Order 13526 of December 29, 2009, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

(d) ''Continuous evaluation (CE)'' means a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility. CE is intended to complement continuous vetting efforts.

(e) ''Continuous performance improvement'' means assessing national policy and operations, adverse events, and emerging trends and technology throughout the Government's end-to-end vetting program. It relies on research to generate data-driven decisions and uses outcome-based measurements to adjust policy and operations.

(f) ''Continuous vetting'' means reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.

(g) ''Contractor'' means an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

(h) ''Covered individual'' means a person who performs, or who seeks to perform, work for or on behalf of the executive branch (e.g., Federal employee, military member, or contractor), or otherwise interacts with the executive branch such that the individual must undergo vetting, but does not include:

(i) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code;

(ii) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3, United States Code, or annual legislative branch appropriations acts; or

(iii) with respect to background investigations only, [the] duly elected or appointed governor of a State or territory, or an official who has succeeded to that office under applicable law in accordance with Executive Order 13549 of August 18, 2010, and its implementing directive.

(i) ''End-to-end automation'' means an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant documentation of the application (but not an employment application), investigation, adjudication, and continuous evaluation processes.

(j) ''Federally controlled facilities'' and ''federally controlled information systems'' have the meanings prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12.

(k) ''Fitness'' means the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability), or as a ''contractor employee'' or a ''nonappropriated fund employee'' as those terms are defined in Executive Order 13488 of January 16, 2009, as amended.

(l) ''Investigation'' means the collection and analysis of pertinent facts and data to support a determination of whether a covered individual is, and continues to be:

(i) eligible for access to classified information;

(ii) eligible to hold a sensitive position;

(iii) suitable or fit for Federal employment;

(iv) fit to perform work for or on behalf of the Federal Government as a contractor or nonappropriated fund employee; or

(v) authorized to be issued a Federal credential.

(m) ''Logical and physical access'' means access other than occasional or intermittent access to federally controlled facilities or information systems.

(n) ''National Background Investigations Bureau'' (NBIB) means the National Background Investigations Bureau, established within the Office of Personnel Management under section 1103(a)(3) of title 5, United States Code, or a successor entity, with responsibility for conducting effective, efficient, and secure personnel background investigations pursuant to law, rule, regulation, or Executive Order.

(o) ''Sensitive Position'' means any position within or in support of a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified information, and regardless of whether the occupant is an employee, a military service member, or a contractor.

(p) ''Suitability'' has the meaning and coverage provided in 5 CFR Part 731.

(q) ''Vetting'' is the process by which covered individuals undergo investigation, evaluation, and adjudication of whether they are, and remain over time, suitable or fit for Federal employment, eligible to occupy a sensitive position, eligible for access to classified information, eligible to serve as a nonappropriated fund employee or a contractor, eligible to serve in the military, or authorized to be issued a Federal credential. Vetting includes all steps in the end-to-end process, including determining need (appropriate position designation), validating need (existence of a current investigation or adjudication), collecting background information via standard forms, investigative activity, adjudication, providing administrative due process or other procedural rights, and ongoing assessments to ensure that individuals continue to meet the applicable standards for the position for which they were favorably adjudicated.

PART 2—VETTING ENTERPRISE, RECIPROCITY, CONTINUOUS PERFORMANCE IMPROVEMENT, AND GOVERNANCE

SEC. 2.1. *Vetting Enterprise.* (a) The executive branch-wide vetting enterprise shall use, to the greatest extent practicable, aligned and consistent vetting policies, procedures, and standards, as determined by the Council and the Executive Agents. The Executive Agents shall issue guidance to implement this provision.

(b) The aligned executive branch-wide vetting enterprise shall employ modern and consistent standards and methods, enable innovations with enterprise information technology capabilities and end-to-end automation to the extent practicable, and ensure that relevant information maintained by agencies can be accessed and shared rapidly across the executive branch, while protecting national security, protecting privacy-related information, protecting civil rights and civil liberties, ensuring resulting decisions are in the national interest and in accordance with due process requirements, and providing the Federal Government with an effective trusted workforce.

(c) The investigative and adjudicative standards for fitness shall, to the extent practicable, be consistent with the standards for suitability. The Executive Agents shall establish in Federal investigative standards the elements of the level of investigation necessary for vetting for fitness.

(d) All covered individuals shall be subject to continuous vetting under standards (including, but not limited to, the frequency of such vetting) as determined by the Security Executive Agent or the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions, as applicable.

(e) Vetting shall include a search of records of the Federal Bureau of Investigation, including a fingerprint-based search, and any other appropriate biometric or database searches not precluded by law.

SEC. 2.2. *Reciprocity.* Except as otherwise authorized by law or policy issued by the applicable Executive Agent, agencies shall accept background investigations and adjudications conducted by other authorized agencies unless an agency determines that a particular background investigation or adjudication does not sufficiently address the standards used by that agency in determining the fitness of its excepted service employees who cannot be noncompetitively converted to the competitive service. Except as described above and except to the extent authority to apply additional requirements is vested by statute in an agency, an agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) that exceed existing requirements without the approval of the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions or Security Executive Agent, as appropriate. Any additional requirements approved by the appropriate Executive Agent shall be limited to those that are necessary to address significant needs unique to the agency involved, to protect national security, or to satisfy a requirement imposed by law.

SEC. 2.3. *Continuous Performance Improvement.* Executive branch vetting policies, processes, and procedures shall be supported by institutionalized enterprise-wide continuous performance improvement, which shall align with and support process improvements.

SEC. 2.4. *Establishment and Functions of Performance Accountability Council.* (a) There is hereby established a Security, Suitability, and Credentialing Performance Accountability Council (Council).

(b) The Deputy Director for Management, Office of Management and Budget, shall serve as Chair of the Council and shall have authority, direction, and control over the Council's functions. Membership on the Council shall include the Suitability and Credentialing Executive Agent, the Security Executive Agent, and the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security]. These four officials collectively shall constitute ''the Security, Suitability, and Credentialing Performance Accountability Council Principals.'' The Director of the Defense Counterintelligence and Security Agency shall also serve as a member of the Council. The Chair shall select a Vice Chair to act in the Chair's absence. The Chair shall have authority to designate officials from additional agencies who shall serve as members of the Council. Council membership shall be limited to Federal Government employees in leadership positions.

(c) The Council shall be accountable to the President to achieve, consistent with this order, the goals of the executive branch vetting enterprise, and is responsible for driving implementation of reform efforts and enterprise development, ensuring accountability by agencies, ensuring the Executive Agents align their respective processes, and sustaining continuous performance improvement and reform momentum.

(d) The Council shall:

(i) ensure enterprise-wide alignment of suitability, security, credentialing, and as appropriate, fitness processes;

(ii) hold agencies accountable for the implementation of suitability, security, fitness, and credentialing processes and procedures;

(iii) define requirements for enterprise-wide reciprocity management information technology, and develop standards for enterprise-wide information technology;

(iv) work with agencies to implement continuous performance improvement programs, policies, and procedures; establish annual goals and progress metrics; and prepare annual reports on results;

(v) ensure and oversee the development of tools and techniques for enhancing background investigations and adjudications;

(vi) enable discussion and consensus resolution of differences in processes, policies, and procedures among the Council Principals, and other agencies as appropriate;

(vii) share best practices;

(viii) advise the Executive Agents on policies affecting the alignment of investigations and adjudications;

(ix) work with agencies to develop agency policies and procedures to enable sharing of vetting information consistent with the law and the protection of privacy and civil liberties and to the extent necessary for enterprise-wide efficiency, effectiveness, and security;

(x) monitor performance to identify and drive enterprise-level process enhancements, and make recommendations for changes to executive branch-wide guidance and authorities to resolve overlaps or close policy gaps where they may exist;

(xi) promote data-driven, transparent, and expeditious policy-making processes; and

(xii) develop and continuously reevaluate and revise outcome-based metrics that measure the quality, efficiency and effectiveness of the vetting enterprise.

(e) The Chair shall, to further the goals of the vetting enterprise and to the extent consistent with law, establish subordinate entities, mechanisms, and policies to support and assist in exercising the Council's authorities and responsibilities, and facilitate, consistent with the executive branch's enterprise strategy, adoption of enterprise-wide standards and solutions to ensure security, quality, reciprocity, efficiency, effectiveness, and timeliness. The Chair may assign, in whole or in part, to the head of any agency (solely or jointly) any function within the Council's authority or responsibilities pursuant to this order.

SEC. 2.5. *Establishment, Designation, and Functions of Executive Agents.* (a) There are hereby established a Suitability and Credentialing Executive Agent and a Security Executive Agent.

(b) The Director of the Office of Personnel Management shall serve as the Suitability and Credentialing Executive Agent. With respect to the Suitability Executive Agent functions, the Director:

(i) shall, pursuant to sections 1103 and 1104 of title 5, United States Code, and the Civil Service Rules, be responsible for suitability and fitness by prescribing suitability standards and minimum standards of fitness for employment; prescribing position designation requirements with regard to the risk to the efficiency and integrity of the service; prescribing applicable investigative standards, policies, and procedures for suitability and fitness; prescribing suitability and fitness reciprocity standards; making suitability determinations; and taking suitability actions;

(ii) shall issue regulations, guidance, and standards to fulfill the Director's responsibilities related to suitability and fitness under Executive Order 13488 of January 16, 2009, as amended;

(iii) shall promote reciprocal recognition of suitability or fitness determinations among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of suitability and fitness;

(iv) shall continue to initially approve, and periodically review for renewal, agencies' requests to administer polygraphs in connection with appointment in the competitive service, in consultation with the Security Executive Agent as appropriate;

(v) shall make a continuing review of agency programs for suitability and fitness vetting to determine whether they are being implemented according to this order;

(vi) may issue guidelines and instructions to the heads of agencies to promote appropriate uniformity, centralization, efficiency, effectiveness, reciprocity, timeliness, and security in processes relating to determining suitability or fitness; and

(vii) shall, pursuant to section 1104 of title 5, United States Code, prescribe performance standards and a system of oversight for any suitability or fitness function delegated by the Director to the head of another agency, including uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of delegated functions.

(c) With respect to the Credentialing Executive Agent functions, the Director of the Office of Personnel Management:

(i) shall develop standards for investigations, reinvestigations, and continuous vetting for a covered individual's eligibility for a personal identity verification credential permitting logical and physical access to federally controlled facilities and federally controlled information systems (PIV credential);

(ii) shall develop adjudicative guidelines for a covered individual's eligibility for a PIV credential;

(iii) shall develop guidelines on reporting and recording determinations of eligibility for a PIV credential;

(iv) shall develop standards for unfavorable determinations of eligibility for a PIV credential, including procedures for denying and revoking the eligibility for a PIV credential, for reconsideration of unfavorable determinations, and for rendering the PIV credential inoperable;

(v) shall develop standards and procedures for suspending eligibility for a PIV credential when there is a reasonable basis to believe there may be an unacceptable risk pending an inquiry or investigation, including special standards and procedures for imminent risk;

(vi) shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations and adjudications relating to eligibility for a PIV credential;

(vii) may develop guidelines and instructions to the heads of agencies as necessary to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to eligibility for a PIV credential;

(viii) shall monitor and make a continuing review of agency programs for determining eligibility for a PIV credential to determine whether they are being implemented according to this order; and

(ix) shall consult to the extent practicable with other agencies with responsibilities related to PIV credentials to ensure that policies and procedures are consistent with law including:

(A) the Office of Management and Budget, in exercising its responsibilities under section 11331 of title 40, United States Code, section 3553(a) of title 44, United States Code, division A, sections 1086(b)(2) and (b)(3) of Public Law 114–92, and Homeland Security Presidential Directive 12 of August 27, 2004;

(B) the Department of Homeland Security, in exercising its responsibilities under sections 3553(b), (f), and (g) of title 44, United States Code;

(C) the Department of Defense, in exercising its responsibilities under section 3553(e) of title 44, United States Code, and division A, sections 1086(a)(1)(E), (b)(1), and (b)(2) of Public Law 114–92;

(D) the Office of the Director of National Intelligence, in exercising its responsibilities under section 3553(e) of title 44, United States Code, and division A, section 1086(b)(2) of Public Law 114–92;

(E) the Department of Commerce and the National Institute of Standards and Technology, in exercising their responsibilities under section 278g–3 of title 15, United States Code, and Homeland Security Presidential Directive 12 of August 27, 2004;

(F) the General Services Administration, in exercising its responsibilities under division A, section 1086(b)(2) of Public Law 114–92; and

(G) the Federal Acquisition Regulation agencies, in exercising their responsibilities under [former] chapter 137 of title 10, section 121(c) of title 40, and section 20113 of title 51, United States Code.

(d) In fulfilling the Credentialing Executive Agent function of developing policies and procedures for determining eligibility for a PIV credential and to protect the national security, the Director of the Office of Personnel Management shall coordinate with and obtain the concurrence of the other Council Principals. Agencies with authority to establish standards or guidelines or issue instructions related to PIV credentials shall retain the discretion as to whether to estab-

lish policies, guidelines, or instructions developed by the Credentialing Executive Agent.

(e) The Director of National Intelligence shall serve as the Security Executive Agent. The Security Executive Agent:

(i) shall direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any agency;

(ii) shall make a continuing review of agencies' national security background investigation and adjudication programs to determine whether they are being implemented according to this order;

(iii) shall be responsible for developing and issuing uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position;

(iv) may issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position, to include such matters as investigations, polygraphs, adjudications, and reciprocity;

(v) may, if consistent with the national security, authorize exceptions to or waivers of national security investigative requirements, and may issue implementing or clarifying guidance as necessary;

(vi) shall serve as the final authority to designate an agency or agencies, to the extent that it is not practicable to use the Defense Counterintelligence and Security Agency, to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position;

(vii) shall serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 of August 2, 1995, as amended;

(viii) shall ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of eligibility; and

(ix) may assign, in whole or in part, to the head of any agency (solely or jointly) any of the functions detailed in (i) through (viii) of this subsection, with the agency's exercise of such assigned functions to be subject to the Security Executive Agent's oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate.

(f) Nothing in this section shall be construed in a manner that would limit the authorities of the Director of the Office of Personnel Management, the Director of National Intelligence, or the Secretary of Defense under law.

SEC. 2.6. *Roles and Responsibilities of the Department of Defense, the Office of Personnel Management, and the Office of Management and Budget.*

(a) The National Background Investigations Bureau shall, until such functions are transferred or delegated, as applicable, to the Defense Counterintelligence and Security Agency:

(i) serve as the primary executive branch service provider for background investigations for eligibility for access to classified information; eligibility to hold a sensitive position; suitability or, for employees in positions not subject to suitability, fitness for Government employment; fitness to perform work for or on behalf of the Government as a contractor; fitness to work as a nonappropriated fund employee, as defined in Executive Order 13488 of January 16, 2009, as amended; and authorization to be issued a Federal credential for logical and physical access to federally controlled facilities or information systems;

(ii) provide effective, efficient, and secure personnel background investigations for the Federal Government;

(iii) provide the Council information, to the extent permitted by law, on matters of performance, timeliness, capacity, information technology modernization, continuous performance improvement, and other relevant aspects of NBIB operations;

(iv) be headquartered in or near Washington, District of Columbia;

(v) have dedicated resources, including but not limited to a senior privacy and civil liberties official;

(vi) institutionalize interagency collaboration and leverage expertise across the executive branch;

(vii) continuously improve investigative operations, emphasizing information accuracy and protection, and regularly integrate best practices, including those identified by subject matter experts from industry, academia, or other relevant sources;

(viii) conduct personnel background investigations in accordance with uniform and consistent policies, procedures, standards, and requirements established by the Security Executive Agent and the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions; and

(ix) conduct other personnel background investigations as authorized by law, rule, regulation, or Executive Order;'' [sic]

except that throughout the transition period ending on or before September 30, 2019, as described in sections 2.6(d)(vi) and 2.6(e)(viii) of this order, the National Background Investigations Bureau and its personnel may continue to perform background investigations for the Defense Counterintelligence and Security Agency.

(b) The Secretary of Defense shall design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, vetting information technology systems that support all background investigation processes conducted by the National Background Investigations Bureau. Design and operation of the information technology systems for the National Background Investigations Bureau shall comply with applicable information technology standards and, to the extent practicable, ensure security and interoperability with other background investigation information technology systems. The Secretary of Defense shall operate the database in the information technology systems containing appropriate data relevant to the granting, denial, or revocation of eligibility for access to classified information or eligibility for a sensitive position pertaining to military, civilian, or Government contractor personnel, see section 3341(e) of title 50, United States Code, consistent with and following an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code.

(i) Pursuant to sections 113 and 191 of title 10, United States Code, the Secretary of Defense shall rename the Defense Security Service (DSS) as the Defense Counterintelligence and Security Agency (DCSA). Subject to the authority, direction, and control of the Secretary of Defense and as further described in subsections (b)(ii) through (b)(iv) of this section, the DCSA shall serve as the primary Federal entity for conducting background investigations for the Federal Government. The DCSA shall, as a continuation of the former DSS, serve as the primary Department of Defense component for the National Industrial Security Program and shall execute responsibilities relating to continuous vetting, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense consistent with law. The Secretary of Defense may rename the DCSA and reassign any of its responsibilities to another Department of Defense component or components, provided, however, that the Secretary of Defense shall consult with the Directors of National Intel-

ligence, the Office of Personnel Management, and the Office of Management and Budget before renaming the DCSA or reassigning the responsibilities specified in section 2.6(b)(ii) and (iv) of this order to another Department of Defense component.

(ii) Pursuant to and consistent with section 3001(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(c)), sections [sic] 925(a)(1) and (d)(2) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note), and in accordance with subsection (d) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for the Federal Government for determining whether covered individuals are or continue to be eligible for access to classified information or eligible to hold a sensitive position.

(iii) Pursuant to and consistent with sections [sic] 925(a)(1) and (d)(2) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note) and in accordance with subsection (d) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for determining the suitability or, for employees in positions not subject to suitability, fitness for Department of Defense employment; fitness to perform work for or on behalf of the Department of Defense as a contractor; fitness to work as a nonappropriated fund employee, as defined in Executive Order 13488 of January 16, 2009, [5 U.S.C. 7301 note] as amended; and authorization to be issued a Federal credential for logical and physical access to facilities or information systems controlled by the Department of Defense.

(iv) Consistent with and following an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code, and consistent with subsection (e) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for the Federal Government not described in subsections (b)(ii) and (b)(iii) of this section, for determining suitability or, for employees in positions not subject to suitability, fitness for Government employment; fitness to perform work for or on behalf of the Government as a contractor; fitness to work as a nonappropriated fund employee, as defined in Executive Order 13488 of January 16, 2009, as amended; and authorization to be issued a Federal credential for logical and physical access to federally controlled facilities or information systems.

(v) The DCSA shall conduct other background investigations as authorized by law, designation, rule, regulation, or Executive Order.

(vi) The DCSA shall provide information to the Council established by section 2.4 of this order regarding matters of performance, including timeliness and continuous improvement, capacity, information technology modernization, and other relevant aspects of its operations. The DCSA shall be subject to the oversight of the Security Executive Agent, including implementation of Security Executive Agent policies, procedures, guidance, and instructions, in conducting investigations for eligibility to access classified information or to hold a sensitive position. The DCSA, through the Secretary of Defense, also shall be subject to the oversight of the Suitability and Credentialing Executive Agent, including implementation of Suitability and Credentialing Executive Agent policies, procedures, guidance, and instructions, and applicable Office of Personnel Management regulations, in conducting investigations of suitability or fitness and eligibility for logical and physical access.

(vii) The Secretary of Defense shall design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, information technology systems that support all personnel vetting processes conducted by the Department of Defense. Design and operation of these information technology systems shall comply with applicable information technology standards and, to the extent practicable, ensure security and interoperability with other personnel vetting or related information technology systems. The Secretary of Defense shall maintain and safeguard the information relevant to the granting, denial, or revocation of eligibility for access to classified information, or eligibility for a sensitive position, or relevant to suitability, fitness, or credentialing determinations pertaining to military, civilian, or Government contractor personnel. The Secretary of Defense shall operate the database in the information technology systems containing appropriate data relevant to the granting, denial, or revocation of eligibility for access to classified information or eligibility for a sensitive position pertaining to military, civilian, or Government contractor personnel, see section 3341(e) of title 50, United States Code, consistent with, as applicable, an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code.

(viii) The Secretary of Defense shall, by June 24, 2019, execute a written agreement with the Director of the Office of Personnel Management designating the appropriate support functions to be transferred as part of the investigative mission, consistent with section 925(d)(2)(B) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note), and setting forth expectations for the transition period, including for detailing personnel, funding background investigations, using and safeguarding information technology, managing facilities and property, contracting, administrative support, records access, and addressing any claims.

(ix) The Secretary of Defense shall, upon finalization of the agreement described in paragraph (viii) of this subsection and in accordance with its terms:

(A) establish the Personnel Vetting Transformation Office within the Department of Defense, which will include personnel from the Department of Defense and other stakeholder agencies, as appropriate; and

(B) commence efforts to receive transferred or delegated functions and, as appropriate, associated Office of Personnel Management operations, resources, and personnel, to the DCSA.

(x) The Secretary of Defense shall:

(A) no later than June 24, 2019, and every 180 days thereafter until the transfer is complete, provide a report to the President, in coordination with the Director of the Office of Personnel Management and through the Director of the Office of Management and Budget, regarding the status of the transfer, including any resource or funding shortfall and gaps in authority;

(B) take necessary actions to enable the Department of Defense to receive any resources, including personnel, made available as a result of subsection (d) of this section; and

(C) notify the President upon completion of the transition period.

(xi) In the event the agreement described in paragraph (viii) of this subsection and section 2.6(e)(v) of this order is not executed by June 24, 2019, beginning on such date, the Secretary of Defense shall begin to take necessary actions to begin execution of paragraph (ix) until the agreement described in paragraph (viii) of this subsection is executed, at which time the Secretary of Defense shall ensure actions subject to such agreement under paragraph (ix) of this subsection are executed in accordance with its terms.'' [sic]

(c) Existing delegations of authority to conduct background investigations made by the Director of the Office of Personnel Management, as the Suitability and Credentialing Executive Agent or as otherwise authorized by statute or Executive Order, to any agency relating to suitability, fitness, or credentialing determinations, existing designations made by the Director of National Intelligence, as the Security Executive Agent or as otherwise authorized by statute or Executive Order, relating to investigating persons who are proposed for access to classified information or for eligibility to hold a sensitive position, or existing delega-

tions of authority to conduct background investigations made by the President to any other agency through any Executive Order shall remain in effect. Nothing in this order shall be construed to limit the authority of any agency to conduct its own background investigations when specifically authorized or directed to do so by statute or any preexisting delegation from the President.

(d) Consistent with section 3503 of title 5, United States Code, subchapter I of chapter 83 of title 10, United States Code, and section 925(d)(1) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note), the Secretary of Defense and the Director of the Office of Personnel Management, in consultation with the Director of the Office of Management and Budget and the Security Executive Agent, shall, consistent with applicable law, provide for the transfer of the functions described in sections 2.6(b)(ii) and (iii) of this order from the Office of Personnel Management's NBIB to DCSA, and any appropriate Office of Personnel Management-associated personnel and resources, including infrastructure and the investigation-related support functions. The transfer shall commence no later than June 24, 2019, and shall:

(i) be executed with the assistance of the Personnel Vetting Transformation Office established pursuant to paragraph (b)(ix) of this section, which shall, in providing such assistance, consider input from other stakeholder agencies, as appropriate;

(ii) be conducted in accordance with a risk management approach that is consistent with Office of Management and Budget Circular A–123;

(iii) include any appropriate funds that the Secretary of Defense and the Director of the Office of Personnel Management, with the concurrence of the Director of the Office of Management and Budget, determine to be available and necessary to finance and discharge the functions transferred;

(iv) be consistent with the transition from legacy information technology as required by subsection (b)(vii) of this section;

(v) build upon the implementation plan developed pursuant to section 951(a)(1) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328) [10 U.S.C. 1564 note], which is being implemented pursuant to section 925 of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note); and

(vi) permit NBIB to conduct background investigations for DCSA, as necessary, until September 30, 2019.

(e) The Director of the Office of Personnel Management shall:

(i) no later than June 24, 2019, take any steps necessary to make effective the delegation, pursuant to section 1104(a)(2) of title 5, United States Code, of the functions described in subsection (b)(iv) of this section;

(ii) promptly establish appropriate performance standards and oversight as required by section 1104(b) of title 5, United States Code;

(iii) work in coordination with the Secretary of Defense to reassign appropriate resources, including personnel, to the DCSA and provide all necessary and appropriate support to the DCSA in a timely manner to enable it to fulfill its responsibilities under this order;

(iv) no later than June 24, 2019, provide the Secretary of Defense with a complete inventory of NBIB personnel, resources, and assets, and other Office of Personnel Management personnel and resources that primarily support NBIB;

(v) no later than June 24, 2019, execute a written agreement with the Secretary of Defense designating the appropriate support functions to be transferred as part of the investigative mission, consistent with section 925(d)(2)(B) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note), as described in section 2.6(b)(viii) of this order;

(vi) immediately upon the finalization of the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order, commence efforts to transition transferred or delegated functions and, as appropriate, associated Office of Personnel Management authorities, operations, resources, and personnel, to the DCSA;

(vii) during the transition period, coordinate with the Department of Defense regarding any decisions concerning NBIB's personnel structure, finances, contracts, or organization to the extent provided in the written agreement described by paragraph (b)(viii) of this section;

(viii) no later than September 30, 2019, complete the transfer of all designated administrative and operational functions to the Department of Defense and revoke any applicable delegation or designation to NBIB of investigative or other authority; and

(ix) in the event the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order is not executed by June 24, 2019, beginning on such date, the Director of the Office of Personnel Management shall begin to take necessary actions to begin execution of paragraphs (iii) through (viii) of this subsection until the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order is executed, at which time the Director of the Office of Personnel Management shall ensure actions subject to such agreement under paragraphs (iii) through (viii) of this subsection are executed in accordance with its terms.

(f) The Director of the Office of Management and Budget shall:

(i) facilitate an effective transfer of functions, including personnel and resources;

(ii) support the Department of Defense's efforts to establish a single, centralized funding capability for its background investigations, as required by section 925(e)(1) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. 1564 note);

(iii) mediate any disagreements between the Secretary of Defense and the Director of the Office of Personnel Management that may arise during or outside of the transition period and facilitate resolution of the conflicting positions; and

(iv) develop, in consultation with the Secretary of Defense and the Director of the Office of Personnel Management, an appropriate funding plan for the activities undertaken pursuant to this order.

SEC. 2.7. *Additional Functions.* (a) The duties assigned to the Security Policy Board by Executive Order 12968 of August 2, 1995, to consider, coordinate, and recommend policy directives for executive branch security policies, procedures, and practices are reassigned to the Security Executive Agent.

(b) Heads of agencies shall:

(i) designate, or cause to be designated, as a ''sensitive position,'' any position occupied by a covered individual in which the occupant could bring about by virtue of the nature of the position, a material adverse effect on the national security;

(ii) establish and maintain within their respective agencies, an effective program to ensure that employment and retention of any covered individual within the agency is clearly consistent with the interests of national security and, as applicable, meets standards for eligibility for access to classified information or to hold a sensitive position, suitability, fitness, or credentialing, established by the respective Executive Agent;

(iii) carry out any function assigned to the agency head by the Chair, and shall assist the Chair, the Council, the Executive Agents, the National Background Investigations Bureau, and the Department of Defense in carrying out any function under sections 2.4, 2.5, and 2.6 of this order;

(iv) implement any policy or procedure established pursuant to this order;

(v) to the extent permitted by law, make available to the Council, the Executive Agents, the National Background Investigations Bureau, and the Department of Defense such information as may be requested to implement this order, including information necessary to implement enterprise-wide vetting policies and procedures;

(vi) except as authorized by section 3341(e)(5) of title 50, United States Code, promptly furnish, or cause to be promptly furnished, to the Office of Personnel Management the information deemed by the Executive Agents to be necessary for purposes of record keeping and reciprocity including, but not limited to, the date on which a background investigation is initiated, the date on which the background investigation is closed, and the specific adjudicative or access decision made. The Executive Agents shall determine the appropriate timeline pursuant to which this information must be reported to the Office of Personnel Management. The Executive Agents shall maintain discretion to determine the scope of information needed for record keeping and reciprocity purposes. The Office of Personnel Management shall regularly provide this information to the Director of National Intelligence for national security purposes.

(vii) ensure that all actions taken under this order take account of the counterintelligence interests of the United States, as appropriate; and

(viii) ensure that actions taken under this order are consistent with the President's constitutional authority to:

(A) conduct the foreign affairs of the United States;

(B) withhold information the disclosure of which could impair the foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties;

(C) recommend for congressional consideration such measures as the President may judge necessary or expedient; and

(D) supervise the unitary executive branch.

(c) All investigations being conducted by agencies that develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information that the individual may pose a counterintelligence or terrorist threat, or as otherwise provided by law, shall be referred to the Federal Bureau of Investigation for potential investigation, and may also be referred to other agencies where appropriate.

PART 3—MISCELLANEOUS

SEC. 3. *General Provisions*. (a) Executive Order 13381 of June 27, 2005 [amending Ex. Ord. No. 12171, set out as a note under section 7103 of Title 5, Government Organization and Employees], as amended, and Executive Order 10450 of April 27, 1953 [formerly set out as a note under section 7311 of Title 5], as amended, are revoked. By revoking Executive Order 10450 of April 27, 1953, as amended, there is no intent to alter the requirement for an investigation for national security purposes or the ''clearly consistent with the interest of national security'' standard prescribed by that Executive Order for making the determinations referenced in section 2.7(b)(ii). Further, suitability, fitness, credentialing, and national security eligibility regulations, standards and guidance issued by, or interagency agreements entered into by, the Council, the Executive Agents, or any agency pursuant to Executive Order 10450 of April 27, 1953, as amended, shall remain valid until superseded. Nothing in this order shall:

(i) supersede, impede, or otherwise affect:

(A) Executive Order 10577 of November 23, 1954, as amended;

(B) Executive Order 12333 of December 4, 1981, as amended;

(C) Executive Order 12829 of January 6, 1993, as amended; or

(D) Executive Order 13526 of December 29, 2009; or

(ii) diminish or otherwise affect the denial and revocation procedures provided to individuals covered by Executive Order 10865 of February 20, 1960, as amended; or

(iii) be applied in such a way as to affect any administrative proceeding pending on the date of this order.

(b) [Amended Ex. Ord. No. 12968, set out as a note above.]

(c) Provisions of Executive Order 12968 of August 2, 1995, as amended, that apply to eligibility for access to classified information shall apply to eligibility to hold any sensitive position regardless of whether that sensitive position requires access to classified information, subject to the Security Executive Agent issuing implementing or clarifying guidance regarding requirements for sensitive positions. Nothing in this order shall supersede, impede, or otherwise affect the remainder of Executive Order 12968 of August 2, 1995, as amended.

(d) Nothing in this order shall be construed to impair or otherwise affect the:

(i) authority granted by law to a department or agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(e) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(f) Existing delegations of authority made pursuant to Executive Order 13381 of June 27, 2005, as amended, to any agency relating to granting eligibility for access to classified information shall remain in effect, subject to the exercise of authorities pursuant to this order to revise or revoke such delegation.

(g) Existing delegations of authority made by the Office of Personnel Management to any agency relating to suitability or fitness shall remain in effect, subject to the exercise of authorities to revise or revoke such delegations.

(h) 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.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

EX. ORD. NO. 13526. CLASSIFIED NATIONAL SECURITY INFORMATION

Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, 1013, provided:

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. 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 both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, 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. *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 1.4 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, which includes defense against transnational terrorism, 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.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

SEC. 1.2. *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. 1.3. *Classification Authority*. (a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(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, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) ''Secret'' or ''Confidential'' original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, 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.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority 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.

SEC. 1.4. *Classification Categories*. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

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

(b) foreign government information;

(c) intelligence activities (including covert action), 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;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (h) the development, production, or use of weapons of mass destruction.

SEC. 1.5. *Duration of Classification*. (a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(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, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as ''Originating Agency's Determination Required,'' or classified information that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part 3 of this order.

SEC. 1.6. *Identification and Markings.* (a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name and position, or by personal identifier, 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 1.5(a);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, 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 and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia 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. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(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 or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

SEC. 1.7. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified 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 the national security.

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

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(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), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 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 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that 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.

SEC. 1.8. *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) of this section.

(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, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure 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 (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

SEC. 1.9. *Fundamental Classification Guidance Review.* (a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

PART 2—DERIVATIVE CLASSIFICATION

SEC. 2.1. *Use of Derivative Classification.* (a) Persons who reproduce, extract, or summarize classified information, or who 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) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) 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, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

SEC. 2.2. *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 ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

(1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

SEC. 3.1. *Authority for Declassification.* (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

(1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

(2) the originator's current successor in function, if that individual has original classification authority;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) 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 the 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.

(e) 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 National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) 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.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

SEC. 3.2. *Transferred Records.*

(a) In the case of classified records 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 records that are not officially transferred as described in paragraph (a) of this section, 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 records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives 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 classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone 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 section 3.3 of this order.

SEC. 3.3 *Automatic Declassification.*

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified 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. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

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

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, 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 formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

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

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) 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

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declas-

sification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) 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.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification 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 Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

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

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

SEC. 3.4. *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 for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records:

(1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

SEC. 3.5. *Mandatory Declassification Review.*

(a) Except as provided in paragraph (b) of this section, 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 document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent

President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or 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) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. 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 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) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) 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 Panel.

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

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

SEC. 3.6. *Processing Requests and Reviews.* Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

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

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 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 or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

(1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of this order.

SEC. 3.7. *National Declassification Center.* (a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

(1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

(2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;

(3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

(4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

(5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

(6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

(7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

(1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

(2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that re-

late to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

PART 4—SAFEGUARDING

SEC. 4.1. *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) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

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

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

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, 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:

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, 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.

(h) 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 U.S. ''Confidential'' information, including modified handling and transmission and 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.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the purposes of this section, ''foreign government'' includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

SEC. 4.2 *Distribution Controls.*

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

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

SEC. 4.3. *Special Access Programs.* (a) Establishment of special access programs. Unless otherwise authorized

by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or 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.

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access 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 5.4(d) 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 of the Information Security Oversight Office 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 head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term ''agency head'' refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each.

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

SEC. 4.4. *Access by Historical Researchers and Certain Former Government Personnel.*

(a) The requirement in section 4.1(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;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice 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 the 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 or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

PART 5—IMPLEMENTATION AND REVIEW

SEC. 5.1. *Program Direction.* (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification, declassification, and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

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

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

SEC. 5.2. *Information Security Oversight Office.* (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, 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 prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;

(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 and 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 President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;

(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 National Security Advisor;

(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. 5.3. *Interagency Security Classification Appeals Panel.*

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(6) 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.

(7) 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 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and

(4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. 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 shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The 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 changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

SEC. 5.4. *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;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) 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 regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying 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) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(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;

(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; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

SEC. 5.5. *Sanctions*. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has 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) of this section occurs; and

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

PART 6—GENERAL PROVISIONS

SEC. 6.1. *Definitions*. For purposes of this order:

(a) ''Access'' means the ability or opportunity to gain knowledge of classified information.

(b) ''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.

(c) ''Authorized holder'' of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(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) ''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.

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

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

(h) ''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.

(i) ''Classified national security information'' or ''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.

(j) ''Compilation'' means an aggregation of preexisting unclassified items of information.

(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, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

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

(n) ''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.

(*o*) ''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.

(p) ''Document'' means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) ''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.

(r) ''File series'' means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) ''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 Government 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.

(t) ''Information'' means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) ''Infraction'' means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a ''violation,'' as defined below.

(v) ''Integral file block'' means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

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

(x) ''Intelligence'' includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) ''Intelligence activities'' means all activities that elements of the Intelligence Community are authorized

to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) ''Intelligence Community'' means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) ''Mandatory declassification review'' means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

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

(cc) ''National security'' means the national defense or foreign relations of the United States.

(dd) ''Need-to-know'' means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

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

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

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

(hh) ''Records'' means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) ''Records having permanent historical value'' means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) ''Records management'' means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) ''Safeguarding'' means measures and controls that are prescribed to protect classified information.

(*ll*) ''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.

(mm) ''Senior agency official'' means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

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

(*oo*) ''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.

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

(qq) ''Telecommunications'' means the preparation, transmission, or communication of information by electronic means.

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

(ss) ''U.S. entity'' includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) ''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.

(uu) ''Weapons of mass destruction'' means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

SEC. 6.2. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. ''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 Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) 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.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.

(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

SEC. 6.3. *Effective Date*. This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

SEC. 6.4. *Publication*. The Archivist of the United States shall publish this Executive Order in the Federal Register.

BARACK OBAMA.

EX. ORD. NO. 13549. CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM FOR STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR ENTITIES

Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, in order to ensure the proper safeguarding of information shared with State, local, tribal, and private sector entities, it is hereby ordered as follows:

SECTION 1. *Establishment and Policy*.

SEC. 1.1. There is established a Classified National Security Information Program (Program) designed to safeguard and govern access to classified national security information shared by the Federal Government with State, local, tribal, and private sector (SLTPS) entities.

SEC. 1.2. The purpose of this order is to ensure that security standards governing access to and safeguarding of classified material are applied in accordance with Executive Order 13526 of December 29, 2009 (''Classified National Security Information''), Executive Order 12968 of August 2, 1995, as amended (''Access to Classified Information''), Executive Order 13467 of June 30, 2008 (''Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information''), and Executive Order 12829 of January 6, 1993, as amended (''National Industrial Security Program''). Procedures for uniform implementation of these standards by SLTPS entities shall be set forth in an implementing directive to be issued by the Secretary of Homeland Security within 180 days of the date of this order, in consultation with affected executive departments and agencies (agencies), and with the concurrence of the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Director of the Information Security Oversight Office.

SEC. 1.3. Additional policy provisions for access to and safeguarding of classified information shared with SLTPS personnel include the following:

(a) Eligibility for access to classified information by SLTPS personnel shall be determined by a sponsoring agency. The level of access granted shall not exceed the Secret level, unless the sponsoring agency determines on a case-by-case basis that the applicant has a demonstrated and foreseeable need for access to Top Secret, Special Access Program, or Sensitive Compartmented Information.

(b) Upon the execution of a non-disclosure agreement prescribed by the Information Security Oversight Office or the Director of National Intelligence, and absent disqualifying conduct as determined by the clearance granting official, a duly elected or appointed Governor of a State or territory, or an official who has succeeded to that office under applicable law, may be granted access to classified information without a background investigation in accordance with the implementing directive for this order. This authorization of access may not be further delegated by the Governor to any other person.

(c) All clearances granted to SLTPS personnel, as well as accreditations granted to SLTPS facilities without a waiver, shall be accepted reciprocally by all agencies and SLTPS entities.

(d) Physical custody of classified information by State, local, and tribal (SLT) entities shall be limited to Secret information unless the location housing the information is under the full-time management, control, and operation of the Department of Homeland Security or another agency. A standard security agreement, established by the Department of Homeland Security in consultation with the SLTPS Advisory Committee, shall be executed between the head of the SLT entity and the U.S. Government for those locations where the SLT entity will maintain physical custody of classified information.

(e) State, local, and tribal facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with established standards, in accordance with Executive Order 13526 and the implementing directive for this order, by the Department of Homeland Security or another agency that has entered into an agreement with the Department of Homeland Security to perform such inspection, accreditation, and monitoring.

(f) Private sector facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with standards established pursuant to Executive Order 12829, as amended, by the Department of Defense or the cognizant security agency under Executive Order 12829, as amended.

(g) Access to information systems that store, process, or transmit classified information shall be enforced by the rules established by the agency that controls the system and consistent with approved dissemination and handling markings applied by originators, separate from and in addition to criteria for determining eligibility for access to classified information. Access to information within restricted portals shall be based on criteria applied by the agency that controls the portal and consistent with approved dissemination and handling markings applied by originators.

(h) The National Industrial Security Program established in Executive Order 12829, as amended, shall govern the access to and safeguarding of classified information that is released to contractors, licensees, and grantees of SLT entities.

(i) All access eligibility determinations and facility security accreditations granted prior to the date of this order that do not meet the standards set forth in this order or its implementing directive shall be reconciled with those standards within a reasonable period.

(j) Pursuant to section 4.1(i)(3) of Executive Order 13526, documents created prior to the effective date of Executive Order 13526 shall not be re-disseminated to other entities without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

SEC. 2. *Policy Direction*. With policy guidance from the National Security Advisor and in consultation with the Director of the Information Security Oversight Office, the Director of the Office of Management and Budget, and the heads of affected agencies, the Secretary of Homeland Security shall serve as the Executive Agent for the Program. This order does not displace any authorities provided by law or Executive Order and the Executive Agent shall, to the extent practicable, make use of existing structures and authorities to preclude duplication and to ensure efficiency.

SEC. 3. *SLTPS Policy Advisory Committee*. (a) There is established an SLTPS Policy Advisory Committee (Committee) to discuss Program-related policy issues in dispute in order to facilitate their resolution and to otherwise recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of information under the Program. The Director of the Information Security Oversight Office shall serve as Chair of the Committee. An official designated by the Secretary of Homeland Security and a representative of SLTPS entities shall serve as Vice Chairs of the Committee. Members of the Committee shall include designees of the heads of the Departments of State, Defense, Justice, Transportation, and Energy, the Nuclear Regulatory Commission, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Federal Bureau of Investigation. Members shall also include employees of other

agencies and representatives of SLTPS entities, as nominated by any Committee member and approved by the Chair.

(b) Members of the Committee shall serve without compensation for their work on the Committee, except that any representatives of SLTPS entities 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).

(c) The Information Security Oversight Office shall provide staff support to the Committee.

(d) Insofar as the Federal Advisory Committee Act, as amended ([former] 5 App. U.S.C.) [see 5 U.S.C. 1001 et seq.] (the ''Act'') may apply to this order, any functions of the President under that Act, 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 guidelines and procedures established by the General Services Administration.

SEC. 4. *Operations and Oversight.* (a) The Executive Agent for the Program shall perform the following responsibilities:

(1) overall program management and oversight;

(2) accreditation, periodic inspection, and monitoring of all facilities owned or operated by SLT entities that have access to classified information, except when another agency has entered into an agreement with the Department of Homeland Security to perform some or all of these functions;

(3) processing of security clearance applications by SLTPS personnel, when requested by a sponsoring agency, on a reimbursable basis unless otherwise determined by the Department of Homeland Security and the sponsoring agency;

(4) documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management, the Department of Defense, and the Office of the Director of National Intelligence;

(5) developing and maintaining a security profile of SLT facilities that have access to classified information; and

(6) developing training, in consultation with the Committee, for all SLTPS personnel who have been determined eligible for access to classified information, which shall cover the proper safeguarding of classified information and sanctions for unauthorized disclosure of classified information.

(b) The Secretary of Defense, or the cognizant security agency under Executive Order 12829, as amended, shall provide program management, oversight, inspection, accreditation, and monitoring of all private sector facilities that have access to classified information.

(c) The Director of National Intelligence may inspect and monitor SLTPS programs and facilities that involve access to information regarding intelligence sources, methods, and activities.

(d) Heads of agencies that sponsor SLTPS personnel and facilities for access to and storage of classified information under section 1.3(a) of this order shall:

(1) ensure on a periodic basis that there is a demonstrated, foreseeable need for such access; and

(2) provide the Secretary of Homeland Security with information, as requested by the Secretary, about SLTPS personnel sponsored for security clearances and SLT facilities approved for use of classified information prior to and after the date of this order, except when the disclosure of the association of a specific individual with an intelligence or law enforcement agency must be protected in the interest of national security, as determined by the intelligence or law enforcement agency.

SEC. 5. *Definitions.* For purposes of this order:

(a) ''Access'' means the ability or opportunity to gain knowledge of classified information.

(b) ''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 possession of classified information.

(c) ''Classified National Security Information'' or ''classified information'' means information that has been determined pursuant to Executive Order 13526, or any predecessor or successor order, to require protection against unauthorized disclosure, and is marked to indicate its classified status when in documentary form.

(d) ''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.

(e) ''Intelligence activities'' means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(f) ''Local'' entities refers to ''(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; and (B) a rural community, unincorporated town or village, or other public entity'' as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(11) [now 101(13)]).

(g) ''Private sector'' means persons outside government who are critically involved in ensuring that public and private preparedness and response efforts are integrated as part of the Nation's Critical Infrastructure or Key Resources (CIKR), including:

(1) corporate owners and operators determined by the Secretary of Homeland Security to be part of the CIKR;

(2) subject matter experts selected to assist the Federal or State CIKR;

(3) personnel serving in specific leadership positions of CIKR coordination, operations, and oversight;

(4) employees of corporate entities relating to the protection of CIKR; or

(5) other persons not otherwise eligible for the granting of a personnel security clearance pursuant to Executive Order 12829, as amended, who are determined by the Secretary of Homeland Security to require a personnel security clearance.

(h) ''Restricted portal'' means a protected community of interest or similar area housed within an information system and to which access is controlled by a host agency different from the agency that controls the information system.

(i) ''Sponsoring Agency'' means an agency that recommends access to or possession of classified information by SLTPS personnel.

(j) ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States, as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(15) [now 101(17)]).

(k) ''State, local, and tribal personnel'' means any of the following persons:

(1) Governors, mayors, tribal leaders, and other elected or appointed officials of a State, local government, or tribe;

(2) State, local, and tribal law enforcement personnel and firefighters;

(3) public health, radiological health, and medical professionals of a State, local government, or tribe; and

(4) regional, State, local, and tribal emergency management agency personnel, including State Adjutants General and other appropriate public safety personnel and those personnel providing support to a Federal CIKR mission.

(l) ''Tribe'' means any Indian or Alaska Native tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian tribe as defined in the Federally Recognized [In-

dian] Tribe List Act of 1994 (25 U.S.C. 479a(2)) [now 25 U.S.C. 5130(2)].

(m) ''United States'' when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States and any waters within the territorial jurisdiction of the United States.

SEC. 6. *General Provisions.* (a) This order does not change the requirements of Executive Orders 13526, 12968, 13467, or 12829, as amended, and their successor orders and directives.

(b) Nothing in this order shall be construed to supersede or change the authorities 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.*); the Secretary of Defense under Executive Order 12829, as amended; the Director of the Information Security Oversight Office under Executive Order 13526 and Executive Order 12829, as amended; the Attorney General under title 18, United States Code, and the Foreign Intelligence Surveillance Act [of 1978] (50 U.S.C. 1801 *et seq.*); the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; or the Director of National Intelligence under the National Security Act of 1947, as amended, Executive Order 12333, as amended, Executive Order 12968, as amended, Executive Order 13467, and Executive Order 13526.

(c) Nothing in this order shall limit the authority of an agency head, or the agency head's designee, to authorize in an emergency and when necessary to respond to an imminent threat to life or in defense of the homeland, in accordance with section 4.2(b) of Executive Order 13526, the disclosure of classified information to an individual or individuals who are otherwise not eligible for access in accordance with the provisions of Executive Order 12968.

(d) Consistent with section 892(a)(4) of the Homeland Security Act of 2002 (6 U.S.C. 482(a)(4)), nothing in this order shall be interpreted as changing the requirements and authorities to protect sources and methods.

(e) Nothing in this order shall supersede measures established under the authority of law or Executive Order to protect the security and integrity of specific activities and associations that are in direct support of intelligence operations.

(f) Pursuant to section 892(e) of the Homeland Security Act of 2002 (6 U.S.C. 482(e)), all information provided to an SLTPS entity from an agency shall remain under the control of the Federal Government. Any State or local law authorizing or requiring disclosure shall not apply to such information.

(g) Nothing in this order limits the protection afforded any classified information by other provisions of law. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(h) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(i) This order shall be implemented subject to the availability of appropriations and consistent with procedures approved by the Attorney General pursuant to Executive Order 12333, as amended.

SEC. 7. *Effective Date.* This order is effective 180 days from the date of this order with the exception of section 3, which is effective immediately.

BARACK OBAMA.

EXTENSION OF TERM OF STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE

Term of State, Local, Tribal, and Private Sector Policy Advisory Committee extended until Sept. 30, 2025, by Ex. Ord. No. 14109, Sept. 29, 2023, 88 F.R. 68447, set out as a note under section 1013 of Title 5, Government Organization and Employees.

Previous extensions of term of State, Local, Tribal, and Private Sector Policy Advisory Committee were contained in the following prior Executive Orders:

Ex. Ord. No. 14048, Sept. 30, 2021, 86 F.R. 55465, extended term until Sept. 30, 2023.

Ex. Ord. No. 13889, Sept. 27, 2019, 84 F.R. 52743, extended term until Sept. 30, 2021.

Ex. Ord. No. 13811, Sept. 29, 2017, 82 F.R. 46363, extended term until Sept. 30, 2019.

Ex. Ord. No. 13708, Sept. 30, 2015, 80 F.R. 60271, extended term until Sept. 30, 2017.

Ex. Ord. No. 13652, Sept. 30, 2013, 78 F.R. 61817, extended term until Sept. 30, 2015.

Ex. Ord. No. 13591, Nov. 23, 2011, 76 F.R. 74623, extended term until Sept. 30, 2013.

EX. ORD. NO. 13587. STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

Ex. Ord. No. 13587, Oct. 7, 2011, 76 F.R. 63811, 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 ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

SECTION 1. *Policy.* Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

SEC. 2. *General Responsibilities of Agencies.*

SEC. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer

Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

SEC. 3. *Senior Information Sharing and Safeguarding Steering Committee.*

SEC. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

SEC. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

SEC. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM–ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD–1 of February 13, 2009 (Organization of the National Security Council System).

SEC. 4. *Classified Information Sharing and Safeguarding Office.*

SEC. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM–ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

SEC. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

SEC. 5. *Executive Agent for Safeguarding Classified Information on Computer Networks.*

SEC. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the ''Executive Agent''), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD–42 of July 5, 1990, as supplemented by and subject to this order.

SEC. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD–42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

SEC. 6. *Insider Threat Task Force.*

SEC. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

SEC. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

SEC. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

SEC. 7. *General Provisions*. (a) For the purposes of this order, the word ''agencies'' shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM–ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD–42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD–42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA.

[Reference to the National Security Staff deemed to be a reference to the National Security Council staff, see Ex. Ord. No. 13657, set out as a note under section 3021 of this title.]

EX. ORD. NO. 14040. DECLASSIFICATION REVIEWS OF CERTAIN DOCUMENTS CONCERNING THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001

Ex. Ord. No. 14040, Sept. 3, 2021, 86 F.R. 50439, provided:

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. *Policy*. Many Americans continue to seek full accountability for the horrific attacks of September 11, 2001 (9/11), including 9/11 survivors and victims' family members. As the 20th anniversary of 9/11 approaches, the American people deserve to have a fuller picture of what their Government knows about those attacks. Although the indiscriminate release of classified information could jeopardize the national security—including the United States Government's efforts to protect against future acts of terrorism—information should not remain classified when the public interest in disclosure outweighs any damage to the national security that might reasonably be expected from disclosure. The significant events in question occurred two decades ago or longer, and they concern a tragic moment that continues to resonate in American history and in the lives of so many Americans. It is therefore critical to ensure that the United States Government maximizes transparency, relying on classification only when narrowly tailored and necessary. Thus, information collected and generated in the United States Government's investigation of the 9/11 terrorist attacks should now be disclosed, except when the strongest possible reasons counsel otherwise.

SEC. 2. *Declassification Reviews*. The Attorney General and the heads of any other executive departments and agencies (agencies) that originated relevant information shall complete declassification reviews:

(a) not later than September 11, 2021, of the Federal Bureau of Investigation (FBI) electronic communication dated April 4, 2016, from the subfile investigation described in chapter V of the 2015 Report of the Congressionally-directed 9/11 Review Commission to the Director of the FBI (subfile investigation), which was identified but withheld in full during discovery in *In re Terrorist Attacks on September 11, 2001*, MDL No. 03–1570 (S.D.N.Y.);

(b) not later than 60 days after the date of this order [Sept. 3, 2021], of:

(i) all other records that previously were withheld as classified, in full or in part, during discovery in *In re Terrorist Attacks on September 11, 2001*; and

(ii) the 2021 FBI electronic communication closing the subfile investigation;

(c) not later than 120 days after the date of this order, of all interview reports, analytical documents, documents reporting investigative findings, or other substantive records (including phone records and banking records, if any) from the FBI's initial investigation of the 9/11 terrorist attacks—known as the Pentagon/Twin Towers Bombings (PENTTBOM) investigation—that reference the individual subjects of the subfile investigation and may be found through search terms, keyword identifiers, and other diligent means; and

(d) not later than 180 days after the date of this order, of all records from any separate FBI investigation other than the PENTTBOM investigation or the subfile investigation of any individual subjects of the subfile investigation that are relevant to the 9/11 terrorist attacks or to any of the individual subjects' connection to an agency relationship with a foreign government.

SEC. 3. *Standards for Declassification.* (a) Consistent with Executive Order 13526 of December 29, 2009 (Classified National Security Information) [set out above], the Attorney General or the head of any other agency that originated the information, as the case may be, shall be responsible for conducting the declassification reviews and making declassification determinations for information that originated within their respective agency. Information may remain classified only if it still requires protection in the interest of the national security and disclosure of the information reasonably could be expected to result in damage to the national security. Information shall not remain classified if there is significant doubt about the need to maintain its classified status. Nor shall information remain classified in order to conceal violations of law, inefficiency, or administrative error or to prevent embarrassment to a person, organization, or agency.

(b) Even when information requires continued protection in the interest of the national security, the Attorney General or the head of any other agency that originated the information, as the case may be, should determine, as an exercise of discretion, whether the public interest in disclosure of the information outweighs the damage to the national security that might reasonably be expected from disclosure.

(c) Upon the completion of the declassification reviews under section 2 of this order, the Attorney General and the heads of any other agencies that originated relevant information shall ensure that, as to all information subject to such reviews but not declassified pursuant to such reviews:

(i) such information meets the requirements for classification, in accordance with Executive Order 13526;

(ii) all non-classified information is disentangled from any classified information and, to the extent practicable, made available to the public under section 5 of this order; and

(iii) all information is nonetheless declassified, in accordance with section 3.1 of Executive Order 13526, or any successor order, when the Attorney General or the head of any other agency that originated the information, as the case may be, determines that the United States Government's interest in classification is outweighed by the public's interest in disclosure.

SEC. 4. *Report to the President and the Congressional Intelligence Committees.* Upon completion of each review, the Attorney General, in consultation with the heads of any other agencies that originated relevant information, shall submit to the President, through the Assistant to the President for National Security Affairs, and to the congressional intelligence committees, reports on the results of the declassification reviews completed under section 2 of this order, including a justification for each decision not to declassify information pursuant to such reviews.

SEC. 5. *Public Release.* Upon completion of each review, the Attorney General, in consultation with the heads of any other agencies that originated relevant information, shall make publicly available information declassified as a result of the declassification reviews completed under section 2 of this order, except for information the disclosure of which would materially impair confidential executive branch deliberations.

SEC. 6. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law, including the Privacy Act [5 U.S.C. 552a], and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

J.R. BIDEN, JR.

IMPLEMENTATION OF THE EXECUTIVE ORDER, ''CLASSIFIED NATIONAL SECURITY INFORMATION''

Memorandum of President of the United States, Dec. 29, 2009, 75 F.R. 733, provided:

Memorandum for the Heads of Executive Departments and Agencies

Today I have signed an executive order [Ex. Ord. No. 13526, set out above] entitled, ''Classified National Security Information'' (the ''order''), which substantially advances my goals for reforming the security classification and declassification processes. I expect that the order will produce measurable progress towards greater openness and transparency in the Government's classification and declassification programs while protecting the Government's legitimate interests, and I will closely monitor the results. I also look forward to reviewing recommendations from the study that the National Security Advisor will undertake in cooperation with the Public Interest Declassification Board to design a more fundamental transformation of the security classification system. To further assist in fulfilling the goal of measurable progress toward greater openness and transparency, I hereby direct the following actions.

1. *Initial Implementation Efforts.*

Successful implementation of the order requires personal commitment from the heads of departments and agencies, as well as their senior officials. It also requires effective security education and training programs, self-inspection programs, and measures designed to hold personnel accountable.

In accordance with section 5.4 of the order, the head of each department and agency that creates or handles classified information shall provide the Director of the Information Security Oversight Office (ISOO) a copy of the department or agency regulations implementing the requirements of the order. Such regulations shall be issued in final form within 180 days of ISOO's publication of its implementing directive for the order. The Director of ISOO shall consider agency actions to implement the requirements of section 5.4 of the order as a key element in planning oversight of agencies. Each senior agency official designated under section 5.4(d) of the order shall provide ISOO with updates concerning agency plans and other actions to implement the requirements of the order. The Director of ISOO shall publish a periodic status report on agency implementation.

2. *Declassification of Records of Permanent Historical Value.*

Under the direction of the National Declassification Center (NDC), and utilizing recommendations of an ongoing Business Process Review in support of the NDC, referrals and quality assurance problems within a backlog of more than 400 million pages of accessioned Federal records previously subject to automatic declassification shall be addressed in a manner that will permit public access to all declassified records from this backlog no later than December 31, 2013. In order to

promote the efficient and effective utilization of finite resources available for declassification, further referrals of these records are not required except for those containing information that would clearly and demonstrably reveal: (a) the identity of a confidential human source or a human intelligence source; or (b) key design concepts of weapons of mass destruction.

The Secretaries of State, Defense, and Energy, and the Director of National Intelligence shall provide the Archivist of the United States with sufficient guidance to complete this task. The Archivist shall make public a report on the status of the backlog every 6 months.

3. *Delegation of Original Classification Authority*.

Delegations of original classification authority shall be limited to the minimum necessary to implement the order and only those individuals or positions with a demonstrable and continuing need to exercise such authority shall be delegated original classification authority.

Accordingly, heads of departments and agencies with original classification authority shall commence a review to ensure that all delegations of original classification authority are so limited and otherwise in accordance with section 1.3(c) of the order. Each department and agency shall submit a report on the results of this review to the Director of ISOO within 120 days of the date of this memorandum.

4. *Promotion of New Technologies to Support Declassification*.

Striking the critical balance between openness and secrecy is a difficult but necessary part of our democratic form of government. Striking this balance becomes more difficult as the volume and complexity of the information increases. Improving the capability of departments and agencies to identify still-sensitive information and to make declassified information available to the public are integral parts of the classification system.

Therefore, I am directing that the Secretary of Defense and the Director of National Intelligence each support research to assist the NDC in addressing the cross-agency challenges associated with declassification.

5. *Publication*. The Archivist of the United States is authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA.

ORIGINAL CLASSIFICATION AUTHORITY

Order of President of the United States, dated Dec. 29, 2009, 75 F.R. 735, provided:

Pursuant to the provisions of section 1.3 of the Executive Order issued today [Ex. Ord. No. 13526, set out above], entitled ''Classified National Security Information'' (Executive Order), I hereby designate the following officials to classify information originally as ''Top Secret'' or ''Secret'':

TOP SECRET

Executive Office of the President:

The Assistant to the President and Chief of Staff

The Assistant to the President for National Security Affairs (National Security Advisor)

The Assistant to the President for Homeland Security and Counterterrorism

The Director of National Drug Control Policy

The Director, Office of Science and Technology Policy

The Chair or Co-Chairs, President's Intelligence Advisory Board

Departments and Agencies:

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Attorney General

The Secretary of Energy

The Secretary of Homeland Security

The Director of National Intelligence

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Chairman, Nuclear Regulatory Commission

The Director of the Central Intelligence Agency

The Administrator of the National Aeronautics and Space Administration

The Director, Information Security Oversight Office

SECRET

Executive Office of the President:

The United States Trade Representative

Departments and Agencies:

The Secretary of Agriculture

The Secretary of Commerce

The Secretary of Health and Human Services

The Secretary of Transportation

The Administrator of the United States Agency for International Development

The Administrator of the Environmental Protection Agency

Any delegation of this authority shall be in accordance with section 1.3(c) of the Executive Order, except that the Director of the Information Security Oversight Office, the Secretary of Agriculture, and the Administrator of the Environmental Protection Agency may not delegate the authority granted in this order. If an agency head without original classification authority under this order, or otherwise delegated in accordance with section 1.3(c) of the Executive Order, has an exceptional need to classify information originated by their agency, the matter shall be referred to the agency head with appropriate subject matter interest and classification authority in accordance with section 1.3(e) of the Executive Order. If the agency with appropriate subject matter interest and classification authority cannot readily be determined, the matter shall be referred to the Director of the Information Security Oversight Office.

Presidential designations ordered prior to the issuance of the Executive Order are revoked as of the date of this order. However, delegations of authority to classify information originally that were made in accordance with the provisions of section 1.4 of Executive Order 12958 of April 17, 1995 [formerly set out above], as amended, by officials designated under this order shall continue in effect, provided that the authority of such officials is delegable under this order.

This order shall be published in the Federal Register.

BARACK OBAMA.

PRIOR PRESIDENTIAL DESIGNATIONS TO CLASSIFY NATIONAL SECURITY INFORMATION WERE CONTAINED IN THE FOLLOWING:

Ex. Ord. No. 13010, § 7(b), July 15, 1996, 61 F.R. 37347, as amended, set out as a note under section 5195 of Title 42, The Public Health and Welfare.

Order of President of the United States, dated Oct. 13, 1995, 60 F.R. 53845, formerly set out as a note under this section.

Order of President of the United States, dated Feb. 27, 1996, 61 F.R. 7977, formerly set out as a note under this section.

Order of President of the United States, dated Feb. 26, 1997, 62 F.R. 9349, formerly set out as a note under this section.

Order of President of the United States, dated Dec. 10, 2001, 66 F.R. 64347, formerly set out as a note under this section.

Order of President of the United States, dated May 6, 2002, 67 F.R. 31109, formerly set out as a note under this section.

Order of President of the United States, dated Sept. 26, 2002, 67 F.R. 61465, formerly set out as a note under this section.

Order of President of the United States, dated Sept. 17, 2003, 68 F.R. 55257, formerly set out as a note under this section.

Order of President of the United States, dated Apr. 21, 2005, 70 F.R. 21609, formerly set out as a note under this section.

§ 3162. 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).

(b) Prohibition of certain disclosure

(1) Prohibition

(A) In general

If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

(B) Certification

The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) Exception

(A) In general

A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

(B) Application

A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) Notice

Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) Identification of disclosure recipients

At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i)