

Sec.
3227c. Continued applicability of the Federal Advisory Committee Act to the Board of Visitors.

SUBCHAPTER IX—ADDITIONAL MISCELLANEOUS PROVISIONS

- 3231. Applicability to United States intelligence activities of Federal laws implementing international treaties and agreements.
- 3232. Counterintelligence initiatives.
- 3232a. Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware.
- 3233. Misuse of the Office of the Director of National Intelligence name, initials, or seal.
- 3234. Prohibited personnel practices in the intelligence community.
- 3235. Semiannual reports on investigations of unauthorized disclosures of classified information.
- 3236. Inspector General external review panel.
- 3237. Annual reports on influence operations and campaigns in the United States by the Chinese Communist Party.
- 3237a. Repealed.
- 3238. Annual reports on influence operations and campaigns in the United States by the Russian Federation.
- 3239. Requirement to buy certain satellite component from American sources.
- 3240. Report on best practices to protect privacy, civil liberties, and civil rights of Chinese Americans.
- 3241. Biennial reports on foreign biological threats.
- 3242. Annual reports on certain cyber vulnerabilities procured by intelligence community and foreign commercial providers of cyber vulnerabilities.
- 3243. Periodic reports on technology strategy of intelligence community.

Editorial Notes

CODIFICATION

Chapter is comprised of act July 26, 1947, ch. 343, 61 Stat. 495, the National Security Act of 1947, which was formerly classified principally as part of chapter 15 of this title, prior to editorial reclassification and renumbering as chapter 44 of this title. For complete classification of the National Security Act of 1947, see Tables.

§ 3001. Short title

This chapter may be cited as the “National Security Act of 1947”.

(July 26, 1947, ch. 343, § 1, 61 Stat. 495.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning act July 26, 1947, ch. 343, 61 Stat. 495, known as the National Security Act of 1947, which is classified principally to this chapter. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was formerly classified as a note under section 401 of this title prior to editorial reclassification as this section.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Pub. L. 108–458, title I, § 1081, Dec. 17, 2004, 118 Stat. 3696, provided that:

“(a) DIRECTOR OF CENTRAL INTELLIGENCE AS HEAD OF INTELLIGENCE COMMUNITY.—Any reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the intelligence community in any law, regulation, document, paper, or other record of the United States shall be deemed to be a reference to the Director of National Intelligence.

“(b) DIRECTOR OF CENTRAL INTELLIGENCE AS HEAD OF CIA.—Any reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the Central Intelligence Agency in any law, regulation, document, paper, or other record of the United States shall be deemed to be a reference to the Director of the Central Intelligence Agency.

“(c) COMMUNITY MANAGEMENT STAFF.—Any reference to the Community Management Staff in any law, regulation, document, paper, or other record of the United States shall be deemed to be a reference to the staff of the Office of the Director of National Intelligence.”

EFFECTIVE DATE OF 2004 AMENDMENT; TRANSITION PROVISIONS

Pub. L. 108–458, title I, subtitle H, Dec. 17, 2004, 118 Stat. 3697, as amended by Pub. L. 109–13, div. A, title I, § 1009, May 11, 2005, 119 Stat. 244; Pub. L. 117–263, div. F, title LXIV, § 6403, Dec. 23, 2022, 136 Stat. 3525, provided that:

“SEC. 1091. TRANSFER OF COMMUNITY MANAGEMENT STAFF.

“(a) TRANSFER.—There shall be transferred to the Office of the Director of National Intelligence such staff of the Community Management Staff as of the date of the enactment of this Act [Dec. 17, 2004] as the Director of National Intelligence determines to be appropriate, including all functions and activities discharged by the Community Management Staff as of that date.

“(b) ADMINISTRATION.—The Director of National Intelligence shall administer the Community Management Staff after the date of the enactment of this Act [Dec. 17, 2004] as a component of the Office of the Director of National Intelligence under section 103 of the National Security Act of 1947 [50 U.S.C. 3025], as amended by section 1011(a) of this Act.

“SEC. 1092. TRANSFER OF TERRORIST THREAT INTEGRATION CENTER.

“(a) TRANSFER.—There shall be transferred to the National Counterterrorism Center the Terrorist Threat Integration Center (TTIC) or its successor entity, including all functions and activities discharged by the Terrorist Threat Integration Center or its successor entity as of the date of the enactment of this Act [Dec. 17, 2004].

“(b) ADMINISTRATION.—The Director of the National Counterterrorism Center shall administer the Terrorist Threat Integration Center after the date of the enactment of this Act [Dec. 17, 2004] as a component of the Directorate of Intelligence of the National Counterterrorism Center under section 119(i) of the National Security Act of 1947 [50 U.S.C. 3056(i)], as added by section 1021(a) [1021] of this Act.

“SEC. 1093. TERMINATION OF POSITIONS OF ASSISTANT DIRECTORS OF CENTRAL INTELLIGENCE.

“(a) TERMINATION.—The positions referred to in subsection (b) are hereby abolished.

“(b) COVERED POSITIONS.—The positions referred to in this subsection are as follows:

“(1) The Assistant Director of Central Intelligence for Collection.

“(2) The Assistant Director of Central Intelligence for Analysis and Production.

“(3) The Assistant Director of Central Intelligence for Administration.

“SEC. 1094. IMPLEMENTATION PLAN.

“The President shall transmit to Congress a plan for the implementation of this title [see Tables for classi-

fication] and the amendments made by this title. The plan shall address, at a minimum, the following:

“(1) The transfer of personnel, assets, and obligations to the Director of National Intelligence pursuant to this title.

“(2) Any consolidation, reorganization, or streamlining of activities transferred to the Director of National Intelligence pursuant to this title.

“(3) The establishment of offices within the Office of the Director of National Intelligence to implement the duties and responsibilities of the Director of National Intelligence as described in this title.

“(4) Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations to be transferred to the Director of National Intelligence.

“(5) Recommendations for additional legislative or administrative action as the President considers appropriate.

“SEC. 1095. DIRECTOR OF NATIONAL INTELLIGENCE REPORT ON IMPLEMENTATION OF INTELLIGENCE COMMUNITY REFORM.

“(a) REPORT.—Not later than one year after the effective date of this Act [probably means the effective date of title I of Pub. L. 108-458, see below], the Director of National Intelligence shall submit to the congressional intelligence committees a report on the progress made in the implementation of this title [see Tables for classification], including the amendments made by this title. The report shall include a comprehensive description of the progress made, and may include such recommendations for additional legislative or administrative action as the Director considers appropriate.

“(b) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, the term ‘congressional intelligence committees’ means—

“(1) the Select Committee on Intelligence of the Senate; and

“(2) the Permanent Select Committee on Intelligence of the House of Representatives.

“SEC. 1096. TRANSITIONAL AUTHORITIES.

“(a) IN GENERAL.—(1) Upon the request of the Director of National Intelligence, the head of any executive agency may, on a reimbursable basis, provide services or detail personnel to the Director of National Intelligence. Any records of the Office of the Director of National Intelligence that are maintained by the agency as a service for the Office of the Director of National Intelligence under section 1535 of title 31, United States Code, (popularly known as the ‘Economy Act’) may be treated as the records of the agency when dispositioned as required by law, and any disclosure of such records between the two agencies shall not be subject to any otherwise applicable legal consent requirements or disclosure accounting requirements.

“(2) The records of the Office of the Director of National Intelligence may not be dispositioned pursuant to paragraph (1) without the authorization of the Director of National Intelligence.

“(b) TRANSFER OF PERSONNEL.—In addition to any other authorities available under law for such purposes, in the fiscal years 2005 and 2006, the Director of National Intelligence—

“(1) is authorized within the Office of the Director of National Intelligence the total of 500 new personnel positions; and

“(2) with the approval of the Director of the Office of Management and Budget, may detail not more than 150 personnel funded within the National Intelligence Program to the Office of the Director of National Intelligence for a period of not more than 2 years.

“SEC. 1097. EFFECTIVE DATES.

“(a) IN GENERAL.—Except as otherwise expressly provided in this Act [see Tables for classification], this title [see Tables for classification] and the amendments made by this title shall take effect not later than six months after the date of the enactment of this Act

[Dec. 17, 2004] [For determination by the President that certain sections of title I of Pub. L. 108-458 take effect earlier than six months after the date of enactment, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note below.]

“(b) SPECIFIC EFFECTIVE DATES.—(1)(A) Not later than 60 days after the date of the appointment of the first Director of National Intelligence, the Director of National Intelligence shall first appoint individuals to positions within the Office of the Director of National Intelligence.

“(B) Subparagraph (A) shall not apply with respect to the Principal Deputy Director of National Intelligence.

“(2) Not later than 180 days after the effective date of this Act [probably means the effective date of title I of Pub. L. 108-458, see above], the President shall transmit to Congress the implementation plan required by section 1094.

“(3) Not later than one year after the date of the enactment of this Act [Dec. 17, 2004], the Director of National Intelligence shall prescribe regulations, policies, procedures, standards, and guidelines required under section 102A of the National Security Act of 1947 [50 U.S.C. 3024], as amended by section 1011(a) of this Act.”

[Functions of President under section 1094 of Pub. L. 108-458, set out in a note above, assigned to the Director of National Intelligence by section 3 of Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 48633, set out as a note under section 301 of Title 3, The President.]

SHORT TITLE OF 2018 AMENDMENT

Pub. L. 115-173, §1, May 22, 2018, 132 Stat. 1291, provided that: “This Act [enacting provisions set out as a note under section 3161 of this title] may be cited as the ‘Securely Expediting Clearances Through Reporting Transparency Act of 2018’ or the ‘SECRET Act of 2018’.”

SHORT TITLE OF 2012 AMENDMENT

Pub. L. 112-235, §1, Dec. 28, 2012, 126 Stat. 1626, provided that: “This Act [amending provisions set out as a note under section 3161 of this title] may be cited as the ‘Public Interest Declassification Board Reauthorization Act of 2012’.”

SHORT TITLE OF 2004 AMENDMENT

Pub. L. 108-458, §1(a), Dec. 17, 2004, 118 Stat. 3638, provided that: “This Act [see Tables for classification] may be cited as the ‘Intelligence Reform and Terrorism Prevention Act of 2004’.”

Pub. L. 108-458, title I, §1001, Dec. 17, 2004, 118 Stat. 3643, provided that: “This title [see Tables for classification] may be cited as the ‘National Security Intelligence Reform Act of 2004’.”

SHORT TITLE OF 1996 AMENDMENT

Pub. L. 104-293, title VIII, §801, Oct. 11, 1996, 110 Stat. 3474, provided that: “This title [see Tables for classification] may be cited as the ‘Intelligence Renewal and Reform Act of 1996’.”

SHORT TITLE OF 1994 AMENDMENT

Pub. L. 103-359, title VIII, §801, Oct. 14, 1994, 108 Stat. 3434, provided that: “This title [see Tables for classification] may be cited as the ‘Counterintelligence and Security Enhancements Act of 1994’.”

SHORT TITLE OF 1992 AMENDMENT

Pub. L. 102-496, title VII, §701, Oct. 24, 1992, 106 Stat. 3188, provided that: “This title [see Tables for classification] may be cited as the ‘Intelligence Organization Act of 1992’.”

SHORT TITLE OF 1984 AMENDMENT

Pub. L. 98-477, §1, Oct. 15, 1984, 98 Stat. 2209, provided: “That this Act [see Tables for classification] may be cited as the ‘Central Intelligence Agency Information Act’.”

SHORT TITLE OF 1982 AMENDMENT

Pub. L. 97-200, §1, June 23, 1982, 96 Stat. 122, provided: “That this Act [see Tables for classification] may be cited as the ‘Intelligence Identities Protection Act of 1982’.”

SHORT TITLE OF 1949 AMENDMENT

Act Aug. 10, 1949, ch. 412, §1, 63 Stat. 578, provided that: “This Act [see Tables for classification] may be cited as the ‘National Security Act Amendments of 1949’.”

Sections of National Security Act of 1947, which were classified to former Title 5, were repealed and restated in Title 10, Armed Forces, except as noted, as follows:

<i>Section of former Title 5</i>	<i>Section of Title 10</i>
171	131, 133.
171a(a), (b)	133.
171a(c)	125, 136, 141, 3010, 3012, 5011, 5031, 8010, 8012.
171a(d)	133.
171a(e)	132.
171a(f)	133.
171a(g)-(i)	[Omitted].
171a(j)	124.
171c	134, 135, 136, 718, 2358.
171c-1, 171c-2	[Repealed].
171d	1580.
171e	171.
171f	141, 142.
171g	143.
171h	2201.
171i	2351.
171j	173.
172	136.
172a	3014, 5061, 8014.
172b	2203.
172c	2204.
172d	2208.
172e	2209.
172f	126.
172g	2205.
172h	2206.
172i	2701.
181-1	101, 3011, 3012, 3062, T. 50 § 409.
181-2	3012.
411a(a)	101; T. 50 § 409.
411a(b)	5012.
411a(c)	5013, 5402.
626(a)	8012.
626(b)	[Repealed].
626(c)	101; T. 50 § 409.
626(d)	8013.
626(e)	8012.
626(f)	8033.
626(g)	8011.
626a	8012.
626b	8013.
626c	743, 8062.

SAVINGS PROVISIONS

Pub. L. 108-487, title VIII, §803, Dec. 23, 2004, 118 Stat. 3962, provided that:

“(a) HEAD OF INTELLIGENCE COMMUNITY.—(1) During the period beginning on the date of the enactment of this Act [Dec. 23, 2004] and ending on the date of the appointment of the Director of National Intelligence [Apr. 21, 2005] under section 102 of the National Security Act of 1947, as amended by section 1011(a) of the National Security Intelligence Reform Act of 2004 [50 U.S.C. 3023], the Director of Central Intelligence may, acting as the head of the intelligence community, discharge the functions and authorities provided in this Act, and the amendments made by this Act [see Effective Date of 2004 Amendments note set out under section 2656f of Title 22, Foreign Relations and Intercourse], to the Director of National Intelligence.

“(2) During the period referred to in paragraph (1) any reference in this Act or the amendments made by this Act to the Director of National Intelligence shall be considered to be a reference to the Director of Central Intelligence, as the head of the intelligence community.

“(3) Upon the appointment of an individual as Director of National Intelligence under section 102 of the National Security Act of 1947, as so amended, any reference in this Act, or in the classified annex to accompany this Act, to the Director of Central Intelligence as head of the intelligence community shall be deemed to be a reference to the Director of National Intelligence.

“(b) HEAD OF CENTRAL INTELLIGENCE AGENCY.—(1) During the period beginning on the date of the enactment of this Act [Dec. 23, 2004] and ending on the date of the appointment of the Director of the Central Intelligence Agency under section 104A of the National Security Act of 1947, as amended by section 1011(a) of the National Security Intelligence Reform Act of 2004 [50 U.S.C. 3036], the Director of Central Intelligence may, acting as the head of the Central Intelligence Agency, discharge the functions and authorities provided in this Act, and the amendments made by this Act, to the Director of the Central Intelligence Agency.

“(2) Upon the appointment of an individual as Director of the Central Intelligence Agency under section 104A of the National Security Act of 1947, as so amended, any reference in this Act, or in the classified annex to accompany this Act, to the Director of Central Intelligence as head of the Central Intelligence Agency shall be deemed to be a reference to the Director of the Central Intelligence Agency.”

Act Aug. 10, 1949, ch. 412, §12(g), 63 Stat. 591, provided: “All laws, orders, regulations, and other actions relating to the National Military Establishment, the Departments of the Army, the Navy, or the Air Force, or to any officer or activity of such establishment or such departments, shall, except to the extent inconsistent with the provisions of this Act [see Tables for classification], have the same effect as if this Act had not been enacted; but, after the effective date of this Act [Aug. 10, 1949], any such law, order, regulation, or other action which vested functions in or otherwise related to any officer, department, or establishment, shall be deemed to have vested such function in or relate to the officer or department, executive or military, succeeding the officer, department, or establishment in which such function was vested. For purposes of this subsection the Department of Defense shall be deemed the department succeeding the National Military Establishment, and the military departments of Army, Navy, and Air Force shall be deemed the departments succeeding the Executive Departments of Army, Navy, and Air Force.”

SEPARABILITY

Pub. L. 108-458, title I, §1103, Dec. 17, 2004, 118 Stat. 3700, provided that: “If any provision of this Act [see Tables for classification], or an amendment made by this Act, or the application of such provision to any person or circumstance is held invalid, the remainder of this Act, or the application of such provision to persons or circumstances other those to which such provision is held invalid shall not be affected thereby.”

CONSTRUCTION OF REFERENCES TO DIRECTOR OF
CENTRAL INTELLIGENCE

Pub. L. 108-487, title VIII, §802, Dec. 23, 2004, 118 Stat. 3962, provided that: “Except as otherwise specifically provided or otherwise provided by context, any reference in this Act [see Effective Date of 2004 Amendments note set out under section 2656f of Title 22, Foreign Relations and Intercourse], or in the classified annex to accompany this Act, to the Director of Central Intelligence shall be deemed to be a reference to the Director of Central Intelligence as head of the intelligence community.”

ANOMALOUS HEALTH INCIDENTS INTERAGENCY
COORDINATOR

Pub. L. 117–81, div. F, title LXVI, § 6603, Dec. 27, 2021, 135 Stat. 2438, provided that:

“(a) ANOMALOUS HEALTH INCIDENTS INTERAGENCY COORDINATOR.—

“(1) DESIGNATION.—Not later than 30 days after the date of the enactment of this Act [Dec. 27, 2021], the President shall designate an appropriate senior official to be known as the Anomalous Health Incidents Interagency Coordinator (in this section referred to as the ‘Interagency Coordinator’).

“(2) DUTIES.—The Interagency Coordinator, working through the interagency national security process, shall, with respect to anomalous health incidents—

“(A) coordinate the response of the United States Government to such incidents;

“(B) coordinate among relevant Federal agencies to ensure equitable and timely access to assessment and care for affected United States Government personnel, dependents of such personnel, and other appropriate individuals;

“(C) ensure adequate training and education relating to such incidents for United States Government personnel;

“(D) ensure that information regarding such incidents is efficiently shared across relevant Federal agencies in a manner that provides appropriate protections for classified, sensitive, and personal information;

“(E) coordinate, in consultation with the Director of the White House Office of Science and Technology Policy, the technological and research efforts of the United States Government to address suspected attacks presenting as such incidents; and

“(F) develop policy options to prevent, mitigate, and deter suspected attacks presenting as such incidents.

“(b) DESIGNATION OF AGENCY COORDINATION LEADS.—

“(1) DESIGNATION; RESPONSIBILITIES.—The head of each relevant agency shall designate an official appointed by the President, by and with the advice and consent of the Senate, or other appropriate senior official, who shall—

“(A) serve as the Anomalous Health Incident Agency Coordination Lead (in this section referred to as the ‘Agency Coordination Lead’) for the relevant agency concerned;

“(B) report directly to the head of such relevant agency regarding activities carried out under this section;

“(C) perform functions specific to such relevant agency and related to anomalous health incidents, consistent with the directives of the Interagency Coordinator and the interagency national security process;

“(D) represent such relevant agency in meetings convened by the Interagency Coordinator; and

“(E) participate in interagency briefings to Congress regarding the response of the United States Government to anomalous health incidents, including briefings required under subsection (c).

“(2) DELEGATION PROHIBITED.—An Agency Coordination Lead may not delegate any of the responsibilities specified in paragraph (1).

“(c) BRIEFINGS.—

“(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and quarterly thereafter for the following two years, the Agency Coordination Leads shall jointly provide to the appropriate congressional committees a briefing on progress made in carrying out the duties under subsection (b)(2) [probably means subsec. (a)(2)].

“(2) ELEMENTS.—Each briefing required under paragraph (1) shall include—

“(A) an update on the investigation into anomalous health incidents affecting United States Government personnel and dependents of such per-

sonnel, including technical causation and suspected perpetrators;

“(B) an update on new or persistent anomalous health incidents;

“(C) a description of threat prevention and mitigation efforts with respect to anomalous health incidents, to include personnel training;

“(D) an identification of any changes to operational posture as a result of anomalous health threats;

“(E) an update on diagnosis and treatment efforts for individuals affected by anomalous health incidents, including patient numbers and wait times to access care;

“(F) a description of efforts to improve and encourage reporting of anomalous health incidents;

“(G) a detailed description of the roles and responsibilities of the Agency Coordination Leads;

“(H) information regarding additional authorities or resources needed to support the interagency response to anomalous health incidents; and

“(I) such other matters as the Interagency Coordinator or the Agency Coordination Leads may consider appropriate.

“(3) UNCLASSIFIED BRIEFING SUMMARY.—

“(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and quarterly thereafter for the following two years, the Agency Coordination Leads shall provide to the appropriate congressional committees a coordinated written summary of the briefings provided under paragraph (1).

“(B) FORM.—The summary under subparagraph (A) shall be submitted in an unclassified form to the extent practicable, consistent with the protection of intelligence sources and methods.

“(d) SECURE REPORTING MECHANISMS.—Not later than 90 days after the date of the enactment of this section, the Interagency Coordinator shall ensure that the head of each relevant agency—

“(1) develops a process to provide a secure mechanism for personnel of the relevant agency concerned, the dependents of such personnel, and other appropriate individuals, to self-report any suspected exposure that could be an anomalous health incident;

“(2) shares all relevant data reported through such mechanism in a timely manner with the Office of the Director of National Intelligence and other relevant agencies, through existing processes coordinated by the Interagency Coordinator; and

“(3) in developing the mechanism pursuant to paragraph (1), prioritizes secure information collection and handling processes to protect classified, sensitive, and personal information.

“(e) WORKFORCE GUIDANCE.—

“(1) DEVELOPMENT AND DISSEMINATION.—The President shall direct the heads of the relevant agencies to develop and disseminate to employees of such relevant agencies who are determined to be at risk of exposure to anomalous health incidents updated workforce guidance that describes, at a minimum—

“(A) the threat posed by anomalous health incidents;

“(B) known defensive techniques with respect to anomalous health incidents; and

“(C) processes to self-report any suspected exposure that could be an anomalous health incident.

“(2) DEADLINE.—The workforce guidance specified under paragraph (1) shall be developed and disseminated pursuant to such paragraph by not later than 60 days after the date of the enactment of this Act.

“(f) RULE OF CONSTRUCTION.—Nothing in this section, including the designation of the Interagency Coordinator pursuant to subsection (a)(1), shall be construed to limit the authority of any Federal agency to independently perform the authorized functions of such agency.

“(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of State \$5,000,000 for fiscal year 2022, to be used to—

“(1) increase capacity and staffing for the Health Incident Response Task Force of the Department of State;

“(2) support the development and implementation of efforts by the Department of State to prevent and mitigate anomalous health incidents affecting the workforce of the Department;

“(3) investigate and characterize the cause of anomalous health incidents, including investigations of causation and attribution;

“(4) collect and analyze data related to anomalous health incidents;

“(5) coordinate with other relevant agencies and the National Security Council regarding anomalous health incidents; and

“(6) support other activities to understand, prevent, deter, and respond to suspected attacks presenting as anomalous health incidents, at the discretion of the Secretary of State.

“(h) DEFINITIONS.—In this section:

“(1) The term ‘appropriate congressional committees’ means—

“(A) the Committees on Armed Services, Foreign Relations, Homeland Security and Governmental Affairs, the Judiciary, and Appropriations, and the Select Committee on Intelligence, of the Senate; and

“(B) the Committees on Armed Services, Foreign Affairs, Homeland Security, the Judiciary, and Appropriations, and the Permanent Select Committee on Intelligence, of the House of Representatives.

“(2) The term ‘relevant Federal agencies’ means—

“(A) the Department of Defense;

“(B) the Department of State;

“(C) the Office of the Director of National Intelligence;

“(D) the Central Intelligence Agency;

“(E) the Department of Justice;

“(F) the Department of Homeland Security; and

“(G) such other Federal departments or agencies as may be designated by the Interagency Coordinator.”

CONSIDERATION OF ADVERSARIAL TELECOMMUNICATIONS AND CYBERSECURITY INFRASTRUCTURE WHEN SHARING INTELLIGENCE WITH FOREIGN GOVERNMENTS AND ENTITIES

Pub. L. 116-92, div. E, title LXIII, § 6307, Dec. 20, 2019, 133 Stat. 2189, provided that: “Whenever the head of an element of the intelligence community enters into an intelligence-sharing agreement with a foreign government or any other foreign entity, the head of the element shall consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by adversaries of the United States, particularly China and Russia, or entities of such adversaries in the country or region of the foreign government or other foreign entity entering into the agreement.”

[For definition of “intelligence community” as used in section 6307 of Pub. L. 116-92, set out above, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.]

COMMITTEE TO COUNTER ACTIVE MEASURES BY THE RUSSIAN FEDERATION TO EXERT COVERT INFLUENCE OVER PEOPLES AND GOVERNMENTS

Pub. L. 115-31, div. N, title V, § 501, May 5, 2017, 131 Stat. 823, which established an interagency committee to counter active measures by the Russian Federation to exert covert influence within the executive branch and was formerly set out as a note under this section, was transferred to section 3369d of this title.

CHARTER FOR THE NATIONAL RECONNAISSANCE OFFICE

Pub. L. 111-84, div. A, title X, § 1035, Oct. 28, 2009, 123 Stat. 2450, provided that: “Not later than February 1, 2010, the Director of National Intelligence and the Secretary of Defense shall jointly submit to the congres-

sional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate a revised charter for the National Reconnaissance Office (in this section referred to as the ‘NRO’). The charter shall include the following:

“(1) The organizational and governance structure of the NRO.

“(2) The role of the NRO in the development and generation of requirements and acquisition.

“(3) The scope of the capabilities of the NRO.

“(4) The roles and responsibilities of the NRO and the relationship of the NRO to other organizations and agencies in the intelligence and defense communities.”

INCORPORATION OF REPORTING REQUIREMENTS

Pub. L. 108-177, title I, § 106, Dec. 13, 2003, 117 Stat. 2604, provided that:

“(a) IN GENERAL.—Each requirement to submit a report to the congressional intelligence committees that is included in the joint explanatory statement to accompany the conference report on the bill H.R. 2417 of the One Hundred Eighth Congress [enacted as Pub. L. 108-177], or in the classified annex to this Act, is hereby incorporated into this Act, and is hereby made a requirement in law.

“(b) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, the term ‘congressional intelligence committees’ means—

“(1) the Select Committee on Intelligence of the Senate; and

“(2) the Permanent Select Committee on Intelligence of the House of Representatives.”

Similar provisions were contained in Pub. L. 107-306, title I, § 108, Nov. 27, 2002, 116 Stat. 2388.

NATIONAL COMMISSION FOR REVIEW OF RESEARCH AND DEVELOPMENT PROGRAMS OF THE UNITED STATES INTELLIGENCE COMMUNITY

Pub. L. 111-259, title VII, § 701(a)(3), Oct. 7, 2010, 124 Stat. 2745, provided that membership of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community established by section 1002(a) of Pub. L. 107-306 [formerly set out in a note below] should be considered vacant and new members should be appointed in accordance with such section 1002.

Pub. L. 107-306, title X, Nov. 27, 2002, 116 Stat. 2437, as amended by Pub. L. 108-177, title III, § 315(a), Dec. 13, 2003, 117 Stat. 2610; Pub. L. 111-259, title VII, § 701(a)(1), (4), (b)(3), (c), Oct. 7, 2010, 124 Stat. 2744, 2745; Pub. L. 112-277, title V, § 502, Jan. 14, 2013, 126 Stat. 2476, established the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community to review the status of research and development programs and activities within the intelligence community, including advanced research and development programs and activities, required the Commission to submit a final report of its review to the congressional intelligence committees, the Director of National Intelligence, and the Secretary of Defense not later than Mar. 31, 2013, and provided that the Commission would terminate at the end of the 120-day period beginning on the date that the final report was transmitted to the congressional intelligence committees.

NATIONAL COMMISSION FOR THE REVIEW OF THE NATIONAL RECONNAISSANCE OFFICE

Pub. L. 106-120, title VII, Dec. 3, 1999, 113 Stat. 1620, established the National Commission for the Review of the National Reconnaissance Office to review the current organization, practices, and authorities of the National Reconnaissance Office, directed the Commission to submit to the congressional intelligence committees, the Director of Central Intelligence, and the Sec-

retary of Defense a final report on such review not later than Nov. 1, 2000, provided that the Commission would terminate at the end of the 120-day period beginning on the date on which the final report was transmitted to the congressional intelligence committees, and directed the Director of Central Intelligence and the Secretary of Defense to each submit to the congressional intelligence committees an assessment of the final report not later than 60 days after receipt.

COMMISSION ON ROLES AND CAPABILITIES OF UNITED STATES INTELLIGENCE COMMUNITY

Pub. L. 103-359, title IX, Oct. 14, 1994, 108 Stat. 3456, related to establishment, composition, duties, reports, powers, payment of expenses, and termination, not later than Mar. 1, 1996, of the Commission on the Roles and Capabilities of the United States Intelligence Community.

NATIONAL COMMISSION ON DEFENSE AND NATIONAL SECURITY

Pub. L. 101-511, title VIII, §8104, Nov. 5, 1990, 104 Stat. 1898, as amended by Pub. L. 102-172, title VIII, §8078, Nov. 26, 1991, 105 Stat. 1189, provided that:

“SECTION 1. This section establishes the National Commission on Defense and National Security.

“SEC. 2. FINDINGS.

“The Congress makes the following findings:

“(1) Recent revolutionary world events require a fundamental reassessment of the defense and national security policies of the United States.

“(2) Emerging democracies around the world will require political, technical, and economic assistance, as well as military assistance, from the developed free nations in order to thrive and to become productive members of the world community.

“(3) Real and potential military threats to the United States and its allies will continue to exist for the foreseeable future from not just the Soviet Union but also from terrorism and from Third World nations.

“(4) Proliferation of both sophisticated conventional weapons and of nuclear weapons could produce a world more dangerous than we have faced in the past.

“(5) Ethnic rivalries as well as economic inequalities may produce instabilities that could spark serious conflict.

“(6) In order to formulate coherent national policies to meet these challenges of a new world environment, it is essential for the United States to achieve a bipartisan consensus such as that which emerged following World War II.

“(7) Such a consensus can be fostered by the development of policy recommendations from a highly respected group of individuals who do not bear a partisan label and who possess critical expertise and experience.

“SEC. 3. ESTABLISHMENT.

“There is established a commission to be known as [the] National Commission on Defense and National Security (hereinafter in this Act referred to as the ‘Commission’). The Commission is established until 30 days following submission of the final report required by section 6 of this section.

“SEC. 4. DUTIES OF COMMISSION.

“(a) IN GENERAL.—The Commission shall analyze and make recommendations to the President and Congress concerning the national security and national defense policies of the United States.

“(b) MATTERS TO BE ANALYZED.—Matters to be analyzed by the Commission shall include the following:

“(1) The world-wide interests, goals, and objectives of the United States that are vital to the national security of the United States.

“(2) The political, economic, and military developments around the world and the implications of those

developments for United States national security interests, including—

“(A) the developments in Eastern Europe and the Soviet Union;

“(B) the question of German unification;

“(C) the future of NATO and European economic integration;

“(D) the future of the Pacific Basin; and

“(E) potential instability resulting from regional conflicts or economic problems in the developing world.

“(3) The foreign policy, world-wide commitments, and national defense capabilities of the United States necessary to deter aggression and implement the national security strategy of the United States, including the contribution that can be made by bilateral and multilateral political and economic associations in promoting interests that the United States shares with other members of the world community.

“(4) The proposed short-term uses of the political, economic, military, and other elements of national power for the United States to protect or promote the interests and to achieve the goals and objectives referred to in paragraph (1).

“(5) Long-term options that should be considered further for a number of potential courses of world events over the remainder of the century and into the next century.

“SEC. 5. MEMBERSHIP.

“(a) NUMBER AND APPOINTMENT.—The Commission shall be composed of 10 members, as follows:

“(1) Three appointed by the President.

“(2) Three appointed by the Speaker of the House of Representatives.

“(3) One appointed by the minority leader of the House of Representatives.

“(4) Two appointed by the majority leader of the Senate.

“(5) One appointed by the minority leader of the Senate.

“(b) QUALIFICATIONS.—Persons appointed to the Commission shall be persons who are not officers or employees of the Federal Government (including Members of Congress) and who are specially qualified to serve on the Commission by virtue of their education, training, or experience.

“(c) TERMS.—Members shall be appointed for the life of the Commission. A vacancy in the Commission shall be filled in the manner in which the original appointment was made.

“(d) BASIC PAY.—Members of the Commission shall serve without pay.

“(e) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number may hold hearings.

“(f) CHAIRMAN AND VICE CHAIRMAN.—The Chairman of the Commission shall be designated by the President from among the members appointed by the President. The Vice Chairman of the Commission shall be designated by the Speaker of the House of Representatives from among the members appointed by the Speaker.

“(g) MEETINGS.—The Commission shall meet at the call of the Chairman or a majority of its members.

“(h) DEADLINE FOR APPOINTMENTS.—Members of the Commission shall be appointed not later than the end of the 30-day period beginning on the date of the enactment of this Act [Nov. 5, 1990].

“SEC. 6. REPORTS.

“(a) INITIAL REPORT.—The Commission shall transmit to the President and to Congress an initial report not later than six months after the date on which the Commission is first constituted with a quorum.

“(b) FINAL REPORT.—The Commission shall transmit to the President and to Congress a final report one year following submission of the initial report under subsection (a).

“(c) CONTENTS OF REPORTS.—The report under subsection (b) shall contain a detailed statement of the findings and conclusions of the Commission concerning

the matters to be studied by the Commission under section 4, together with its recommendations for such legislation and administrative actions as it considers appropriate. Such report shall include a comprehensive description and discussion of the matters set forth in section 4.

“(d) REPORTS TO BE UNCLASSIFIED.—Each such report shall be submitted in unclassified form.

“(e) ADDITIONAL AND MINORITY VIEWS.—Each report may include such additional and minority views as individual members of the Commission may request be included.

“SEC. 7. DIRECTOR AND STAFF OF COMMISSION; EXPERTS AND CONSULTANTS.

“(a) DIRECTOR.—The Commission shall, without regard to section 5311(b) of title 5, United States Code, have a Director who shall be appointed by the Chairman and who shall be paid at a rate not to exceed the maximum rate of basic pay payable for GS-18 of the General Schedule.

“(b) STAFF.—The Chairman may appoint and fix the pay of such additional personnel as the Chairman considers appropriate.

“(c) APPLICABILITY OF CERTAIN CIVIL SERVICE LAWS.—The Director and staff of the Commission may be appointed without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and may be paid without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no individual so appointed may receive pay in excess of the annual rate of basic pay payable for GS-18 of the General Schedule.

“(d) EXPERTS AND CONSULTANTS.—Subject to such rules as may be prescribed by the Commission, the Chairman may procure temporary and intermittent services under section 3109(b) of title 5 of the United States Code, but at rates for individuals not to exceed the daily equivalent of the maximum annual rate of basic pay payable for GS-18 of the General Schedule.

“(e) STAFF OF FEDERAL AGENCIES.—Upon request of the Commission, the head of any Federal agency may detail, on a reimbursable basis, any of the personnel of such agency to the Commission to assist the Commission in carrying out its duties under this Act.

“SEC. 8. POWERS OF COMMISSION

“(a) HEARINGS AND SESSIONS.—The Commission may, for the purpose of carrying out this Act, hold such hearings, sit and act at such times and places, take such testimony, and receive such evidence, as the Commission considers appropriate.

“(b) POWERS OF MEMBERS AND AGENTS.—Any member or agent of the Commission may, if so authorized by the Commission, take any action which the Commission is authorized to take by this section.

“(c) OBTAINING OFFICIAL DATA.—The Chairman or a designee on behalf of the Chairman may request information necessary to enable the Commission to carry out this Act directly from any department or agency of the United States.

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

“(e) MAILS.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the United States.

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

“SEC. 9. INITIAL FUNDING OF COMMISSION.

“If funds are not otherwise available for the necessary expenses of the Commission for fiscal year 1991, the Secretary of Defense shall make available to the Commission, from funds available to the Secretary for the fiscal year concerned, such funds as the Commission requires. When funds are specifically appropriated for the expenses of the Commission, the Commission

shall reimburse the Secretary from such funds for any funds provided to it under the preceding sentence.”

[References in laws to the rates of pay for GS-16, 17, or 18, or to maximum rates of pay under the General Schedule, to be considered references to rates payable under specified sections of Title 5, Government Organization and Employees, see section 529 [title I, § 101(c)(1)] of Pub. L. 101-509, set out in a note under section 5376 of Title 5.]

INTELLIGENCE PRIORITIES AND REORGANIZATION

Pub. L. 101-510, div. A, title IX, § 907, Nov. 5, 1990, 104 Stat. 1622, required the Secretary of Defense and Director of Central Intelligence to conduct a joint review of all intelligence and intelligence-related activities in the Tactical Intelligence and Related Activities programs and the National Foreign Intelligence Program and reduce by not less than 5 percent the number of personnel detailed to such programs during each of fiscal years 1992 through 1996.

CHANGE OF TITLES OF SECRETARY OF DEFENSE, ET AL.; REAPPOINTMENT

Act Aug. 10, 1949, ch. 412, § 12(f), 63 Stat. 591, provided in part that: “The titles of the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, the Secretary of the Air Force, the Under Secretaries and the Assistant Secretaries of the Departments of the Army, Navy, and Air Force, the Chairman of the Munitions Board, and the Chairman of the Research and Development Board, shall not be changed by virtue of this Act [see Tables for classification] and the reappointment of the officials holding such titles on the effective date of this Act [Aug. 10, 1949] shall not be required.”

Executive Documents

REORGANIZATION PLAN NO. 8 OF 1949

Act Aug. 10, 1949, ch. 412, § 12(i), 63 Stat. 592, provided that: “Reorganization Plan Numbered 8 of 1949, which was transmitted to the Congress by the President on July 18, 1949 [set out in Appendix to Title 5, Government Organization and Employees] pursuant to the provisions of the Reorganization Act of 1949, shall not take effect, notwithstanding the provisions of section 6 of such Reorganization Act of 1949.”

EX. ORD. NO. 10431. NATIONAL SECURITY MEDAL

Ex. Ord. No. 10431, Jan. 19, 1953, 18 F.R. 437, as amended by Ex. Ord. No. 13709, § 1, Oct. 2, 2015, 80 F.R. 60793, provided:

1. There is hereby established a medal to be known as the National Security Medal with accompanying ribbons and appurtenances. The medal and its appurtenances shall be of appropriate design, approved by the Executive Secretary of the National Security Council.

2. The National Security Medal may be awarded to any person, without regard to nationality, including members of the Armed Forces of the United States, for distinguished achievement or outstanding contribution made on or after July 26, 1947, in the field of national security through either exceptionally meritorious service performed in a position of high responsibility or through an act of heroism requiring personal courage of a high degree and complete disregard of personal safety.

3. The decoration established by this order shall be awarded by the President of the United States or, under regulations approved by him, by such person or persons as he may designate.

4. No more than one National Security Medal shall be awarded to any one person, but for subsequent services justifying an award, a suitable device may be awarded to be worn with the Medal.

5. Members of the armed forces of the United States who are awarded the decoration established by this order are authorized to wear the medal and the ribbon

symbolic of the award, as may be authorized by uniform regulations approved by the Secretary of Defense.

6. The decoration established by this order may be awarded posthumously.

7. Any individual having personal knowledge of the facts of a potential recipient's exceptionally meritorious service or act of heroism, either as an eyewitness or from the testimony of others who have personal knowledge or were eyewitnesses, may recommend the potential recipient as a candidate for the award to the Executive Secretary of the National Security Council. Any recommendations shall be made with the concurrence of the department or agency employing the proposed recipient, if appropriate, and be accompanied by complete documentation, including, where necessary, certificates, affidavits, or sworn transcripts of testimony. Each recommendation for an award shall show the exact status, at the time of the rendition of the service on which the recommendation is based, with respect to citizenship, employment, and all other material factors of the person who is being recommended for the National Security Medal. Each recommendation shall contain a draft of an appropriate citation to accompany the award of the National Security Medal.

8. Upon a determination by the Executive Secretary of the National Security Council that the National Security Medal is warranted, and following approval by the President, the Executive Secretary shall notify the Office of the Director of National Intelligence, which will then process the award recommendation, prepare the National Security Medal, with any appropriate devices, and deliver the National Security Medal to the National Security Council for presentation to the recipient.

REGULATIONS GOVERNING THE AWARD OF THE NATIONAL SECURITY MEDAL

Ex. Ord. No. 13709, §2, Oct. 2, 2015, 80 F.R. 60793, provided that the regulations governing the award of the National Security Medal that were issued pursuant to par. 2 of Ex. Ord. No. 10431 (prior to amendment by Ex. Ord. No. 13709) and published with that order were superseded by Ex. Ord. No. 13709.

EXECUTIVE ORDER No. 11905

Ex. Ord. No. 11905, Feb. 18, 1976, 41 F.R. 7703, as amended by Ex. Ord. No. 11985, May 13, 1977, 42 F.R. 25487; Ex. Ord. No. 11994, June 1, 1977, 42 F.R. 28869, which related to United States foreign intelligence activities, was superseded by Ex. Ord. No. 12036, Jan. 24, 1978, 43 F.R. 3674, formerly set out below.

EXECUTIVE ORDER No. 12036

Ex. Ord. No. 12036, Jan. 24, 1978, 43 F.R. 3674, as amended by Ex. Ord. No. 12139, May 23, 1979, 44 F.R. 30311, which related to United States foreign intelligence activities, was revoked by Ex. Ord. No. 12333, §3.6, Dec. 4, 1981, 46 F.R. 59954, prior to Ex. Ord. No. 12333 being amended by Ex. Ord. No. 13470, §4(j), July 30, 2008, 73 F.R. 45341.

FOREIGN INTELLIGENCE ELECTRONIC SURVEILLANCE

For provisions relating to the exercise of certain authority respecting foreign intelligence electronic surveillance, see Ex. Ord. No. 12139, May 23, 1979, 44 F.R. 30311, set out under section 1802 of this title.

EX. ORD. No. 12333. UNITED STATES INTELLIGENCE ACTIVITIES

Ex. Ord. No. 12333, Dec. 4, 1981, 46 F.R. 59941, as amended by Ex. Ord. No. 13284, §18, Jan. 23, 2003, 68 F.R. 4077; Ex. Ord. No. 13355, §§2, 3, 6, Aug. 27, 2004, 69 F.R. 53593; Ex. Ord. No. 13470, §§1–4, July 30, 2008, 73 F.R. 45325, provided:

TABLE OF CONTENTS [Omitted.]

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of for-

eign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended (Act) [50 U.S.C. 3001 et seq.], and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1—GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS

1.1 GOALS

The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 THE NATIONAL SECURITY COUNCIL

(a) *Purpose.* The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) *Covert Action and Other Sensitive Intelligence Operations.* The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 DIRECTOR OF NATIONAL INTELLIGENCE

Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head [sic] of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or

through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a

vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security]; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security]. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 THE INTELLIGENCE COMMUNITY

Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad

necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 DUTIES AND RESPONSIBILITIES OF THE HEADS OF EXECUTIVE BRANCH DEPARTMENTS AND AGENCIES

The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence col-

lected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 HEADS OF ELEMENTS OF THE INTELLIGENCE COMMUNITY

The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 INTELLIGENCE COMMUNITY ELEMENTS

Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 THE DEPARTMENT OF STATE

In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 THE DEPARTMENT OF THE TREASURY

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 THE DEPARTMENT OF DEFENSE

The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and in-

telligence and be responsive to collection tasking and advisory tasking by the Director;

(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in [sub]sections (a) through [sic] (i) above, and to support the Intelligence Community elements of the Department of Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense, (h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 THE DEPARTMENT OF HOMELAND SECURITY

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 THE DEPARTMENT OF ENERGY

In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 THE FEDERAL BUREAU OF INVESTIGATION

In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2—CONDUCT OF INTELLIGENCE ACTIVITIES

2.1 NEED

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 PURPOSE

This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 COLLECTION OF INFORMATION

Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 COLLECTION TECHNIQUES

Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element concerned and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a nonintelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 ATTORNEY GENERAL APPROVAL

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 ASSISTANCE TO LAW ENFORCEMENT AND OTHER CIVIL AUTHORITIES

Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element within the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 CONTRACTING

Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 CONSISTENCY WITH OTHER LAWS

Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 UNDISCLOSED PARTICIPATION IN ORGANIZATIONS WITHIN THE UNITED STATES

No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 HUMAN EXPERIMENTATION

No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 PROHIBITION ON ASSASSINATION

No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination.

2.12 INDIRECT PARTICIPATION

No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 LIMITATION ON COVERT ACTION

No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3—GENERAL PROVISIONS

3.1 CONGRESSIONAL OVERSIGHT

The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act [50 U.S.C. 3091 et seq.]. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 IMPLEMENTATION

The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 PROCEDURES

The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 REFERENCES AND TRANSITION

References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or other

Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 DEFINITIONS

For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community and elements of the Intelligence Community* refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 REVOCATION

Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 GENERAL PROVISIONS

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

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

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

(c) This order is intended only to improve the internal management of the executive branch and 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.

[For provisions relating to consideration of Commandant and Assistant Commandant for Intelligence of the Coast Guard as a "Senior Official of the Intelligence Community" for purposes of Ex. Ord. No. 12333, set out above, and all other relevant authorities, see Ex. Ord. No. 13286, § 87, Feb. 28, 2003, 68 F.R. 10632, set out as a note under section 111 of Title 6, Domestic Security.]

EXECUTIVE ORDER NO. 12334

Ex. Ord. No. 12334, Dec. 4, 1981, 46 F.R. 59955, as amended by Ex. Ord. No. 12701, Feb. 14, 1990, 55 F.R. 5953, which established the President's Intelligence Oversight Board, was revoked by Ex. Ord. No. 12863, § 3.3, Sept. 13, 1993, 58 F.R. 48441, formerly set out below.

EXECUTIVE ORDER NO. 12863

Ex. Ord. No. 12863, Sept. 13, 1993, 58 F.R. 48441, as amended by Ex. Ord. No. 13070, Dec. 15, 1997, 62 F.R. 66493; Ex. Ord. No. 13301, May 14, 2003, 68 F.R. 26981; Ex. Ord. No. 13376, Apr. 13, 2005, 70 F.R. 20261, which established the President's Foreign Intelligence Advisory Board, was revoked by Ex. Ord. No. 13462, § 10, Feb. 29, 2008, 73 F.R. 11808, set out below.

EX. ORD. NO. 13434. NATIONAL SECURITY PROFESSIONAL DEVELOPMENT

Ex. Ord. No. 13434, May 17, 2007, 72 F.R. 28583, 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 enhance the national security, it is hereby ordered as follows:

SECTION 1. Policy. In order to enhance the national security of the United States, including preventing, protecting against, responding to, and recovering from natural and manmade disasters, such as acts of terrorism, it is the policy of the United States to promote the education, training, and experience of current and future professionals in national security positions (security professionals) in executive departments and agencies (agencies).

SEC. 2. National Strategy for Professional Development. Not later than 60 days after the date of this order, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT), in coordination with the Assistant to the President for National Security Affairs (APNSA), shall submit to the President for approval a National Strategy for the Development of Security Professionals (National Strategy). The National Strategy shall set forth a framework that will provide to security professionals access to integrated education, training, and professional experience opportunities for the purpose of enhancing their mission-related knowledge, skills, and experience and thereby improve their capability to safeguard the security of the Nation. Such opportunities shall be provided across organizations, levels of government, and incident management disciplines, as appropriate.

SEC. 3. Executive Steering Committee. (a) There is established the Security Professional Development Executive Steering Committee (Steering Committee), which shall facilitate the implementation of the National Strategy. Not later than 120 days after the approval of the National Strategy by the President, the Steering Committee shall submit to the APHS/CT and the APNSA an implementation plan (plan) for the National Strategy, and annually thereafter shall submit to the APHS/CT and the APNSA a status report on the implementation of the plan and any recommendations for changes to the National Strategy.

(b) The Steering Committee shall consist exclusively of the following members (or their designees who shall be full-time officers or employees of the members' respective agencies):

- (i) the Director of the Office of Personnel Management, who shall serve as Chair;
- (ii) the Secretary of State;
- (iii) the Secretary of the Treasury;
- (iv) the Secretary of Defense;
- (v) the Attorney General;
- (vi) the Secretary of Agriculture;
- (vii) the Secretary of Labor;
- (viii) the Secretary of Health and Human Services;
- (ix) the Secretary of Housing and Urban Development;
- (x) the Secretary of Transportation;
- (xi) the Secretary of Energy;

(xii) the Secretary of Education;
 (xiii) the Secretary of Homeland Security;
 (xiv) the Director of National Intelligence;
 (xv) the Director of the Office of Management and Budget; and
 (xvi) such other officers of the United States as the Chair of the Steering Committee may designate from time to time.

(c) The Steering Committee shall coordinate, to the maximum extent practicable, national security professional development programs and guidance issued by the heads of agencies in order to ensure an integrated approach to such programs.

(d) The Chair of the Steering Committee shall convene and preside at the meetings of the Steering Committee, set its agenda, coordinate its work, and, as appropriate to deal with particular subject matters, establish subcommittees of the Steering Committee that shall consist exclusively of members of the Steering Committee (or their designees under subsection (b) of this section), and such other full-time or permanent part-time officers or employees of the Federal Government as the Chair may designate.

SEC. 4. *Responsibilities.* The head of each agency with national security functions shall:

(a) identify and enhance existing national security professional development programs and infrastructure, and establish new programs as necessary, in order to fulfill their respective missions to educate, train, and employ security professionals consistent with the National Strategy and, to the maximum extent practicable, the plan and related guidance from the Steering Committee; and

(b) cooperate with the Steering Committee and provide such information, support, and assistance as the Chair of the Steering Committee may request from time to time.

SEC. 5. *Additional Responsibilities.* (a) Except for employees excluded by law, and subject to subsections (b), (c), and (d) of this section, the Director of the Office of Personnel Management, after consultation with the Steering Committee, shall:

(i) consistent with applicable merit-based hiring and advancement principles, lead the establishment of a national security professional development program in accordance with the National Strategy and the plan that provides for interagency and intergovernmental assignments and fellowship opportunities and provides for professional development guidelines for career advancement; and

(ii) issue to agencies rules and guidance or apply existing rules and guidance relating to the establishment of national security professional development programs to implement the National Strategy and the plan;

(b) The Secretary of Defense shall issue rules or guidance on professional development programs for Department of Defense military personnel, including interagency and intergovernmental assignments and fellowship opportunities, to implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee;

(c) The Secretary of State shall issue rules or guidance on national security professional development programs for the Foreign Service, including interagency and intergovernmental exchanges and fellowship opportunities, to implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee;

(d) The Director of National Intelligence, in coordination with the heads of agencies of which elements of the intelligence community are a part, shall issue rules or guidance on national security professional development programs for the intelligence community, including interagency and intergovernmental assignments and fellowship opportunities, to implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee; and

(e) The Secretary of Homeland Security shall develop a program to provide to Federal, State, local, and tribal government officials education in disaster preparedness, response, and recovery plans and authorities, and training in crisis decision-making skills, consistent with applicable presidential guidance.

SEC. 6. *General Provisions.* This order:

(a) shall be implemented consistent with applicable law and authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the authorities of any agency, instrumentality, officer, or employee of the United States under applicable law, including the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals, or the functions assigned by the President to the Director of the Office of Personnel Management; and

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

GEORGE W. BUSH.

EX. ORD. NO. 13462. PRESIDENT'S INTELLIGENCE ADVISORY BOARD AND INTELLIGENCE OVERSIGHT BOARD

Ex. Ord. No. 13462, Feb. 29, 2008, 73 F.R. 11805, as amended by Ex. Ord. No. 13516, §1, Oct. 28, 2009, 74 F.R. 56521, 57241, 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 as follows:

SECTION 1. *Policy.* It is the policy of the United States to ensure that the President and other officers of the United States with responsibility for the security of the Nation and the advancement of its interests have access to accurate, insightful, objective, and timely information concerning the capabilities, intentions, and activities of foreign powers.

SEC. 2. *Definitions.* As used in this order:

(a) “department concerned” means an executive department listed in section 101 of title 5, United States Code, that contains an organization listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended ([former] 50 U.S.C. 401a(4)) [now 50 U.S.C. 3003(4)];

(b) “intelligence activities” has the meaning specified in section 3.5 of Executive Order 12333 of December 4, 1981, as amended; and

(c) “intelligence community” means the organizations listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended.

SEC. 3. *Establishment of the President's Intelligence Advisory Board.* (a) There is hereby established, within the Executive Office of the President and exclusively to advise and assist the President as set forth in this order, the President's Intelligence Advisory Board (PIAB).

(b) The PIAB shall consist of not more than 16 members appointed by the President from among individuals who are not full-time employees of the Federal Government.

(c) The President shall designate a Chair or Co-Chairs from among the members of the PIAB, who shall convene and preside at meetings of the PIAB, determine its agenda, and direct its work.

(d) Members of the PIAB and the Intelligence Oversight Board (IOB) established in section 5 of this order:

(i) shall serve without any compensation for their work on the PIAB or the IOB; and

(ii) while engaged in the work of the PIAB or the IOB, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government (5 U.S.C. 5701–5707).

(e) The PIAB shall utilize such full-time professional and administrative staff as authorized by the Chair and

approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the PIAB, appointed by the President, whom the President may designate to serve also as the Executive Director of the IOB.

SEC. 4. *Functions of the PIAB.* Consistent with the policy set forth in section 1 of this order, the PIAB shall have the authority to, as the PIAB determines appropriate, or shall, when directed by the President:

(a) assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities, assess the adequacy of management, personnel and organization in the intelligence community, and review the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy and report the results of such assessments or reviews:

(i) to the President, as necessary but not less than twice each year; and

(ii) to the Director of National Intelligence (DNI) and the heads of departments concerned when the PIAB determines appropriate; and

(b) consider and make appropriate recommendations to the President, the DNI, or the head of the department concerned with respect to matters identified to the PIAB by the DNI or the head of a department concerned.

SEC. 5. *Establishment of Intelligence Oversight Board.*

(a) There is hereby established a committee of the PIAB to be known as the Intelligence Oversight Board.

(b) The IOB shall consist of not more than five members of the PIAB who are designated by the President from among members of the PIAB to serve on the IOB. The IOB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the IOB, appointed by the President, whom the President may designate to serve also as the Executive Director of the PIAB.

(c) The President shall designate a Chair from among the members of the IOB, who shall convene and preside at meetings of the IOB, determine its agenda, and direct its work.

SEC. 6. *Functions of the IOB.* Consistent with the policy set forth in section 1 of this order, the IOB shall:

(a) issue criteria on the thresholds for reporting matters to the IOB, to the extent consistent with section 1.6(c) of Executive Order 12333, as amended[,] or the corresponding provision of any successor order;

(b) inform the President of intelligence activities that the IOB believes:

(i)(A) may be unlawful or contrary to Executive Order or presidential directive; and

(B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or

(ii) should be immediately reported to the President.[]

(c) forward to the Attorney General information concerning intelligence activities that involve possible violations of Federal criminal laws or otherwise implicate the authority of the Attorney General;

(d) review and assess the effectiveness, efficiency, and sufficiency of the processes by which the DNI and the heads of departments concerned perform their respective functions under this order and report thereon as necessary, together with any recommendations, to the President and, as appropriate, the DNI and the head of the department concerned;

(e) receive and review information submitted by the DNI under subsection 7(c) of this order and make recommendations thereon, including for any needed corrective action, with respect to such information, and the intelligence activities to which the information relates, as necessary, but not less than twice each year, to the President, the DNI, and the head of the department concerned; and

(f) conduct, or request that the DNI or the head of the department concerned, as appropriate, carry out and report to the IOB the results of, investigations of intelligence activities that the IOB determines are necessary to enable the IOB to carry out its functions under this order.

SEC. 7. *Functions of the Director of National Intelligence.* Consistent with the policy set forth in section 1 of this order, the DNI shall:

(a) with respect to guidelines applicable to organizations within the intelligence community that concern reporting of intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) review and ensure that such guidelines are consistent with section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order, and this order; and

(ii) issue for incorporation in such guidelines instructions relating to the format and schedule of such reporting as necessary to implement this order;

(b) with respect to intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) receive reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order;

(ii) forward to the Attorney General information in such reports relating to such intelligence activities to the extent that such activities involve possible violations of Federal criminal laws or implicate the authority of the Attorney General unless the DNI or the head of the department concerned has previously provided such information to the Attorney General; and

(iii) monitor the intelligence community to ensure that the head of the department concerned has directed needed corrective actions and that such actions have been taken and report to the IOB and the head of the department concerned, and as appropriate the President, when such actions have not been timely taken; and

(c) submit to the IOB as necessary and no less than twice each year:

(i) an analysis of the reports received under subsection (b)(i) of this section, including an assessment of the gravity, frequency, trends, and patterns of occurrences of intelligence activities described in subsection 6(b)(i)(A) of this order;

(ii) a summary of direction under subsection (b)(iii) of this section and any related recommendations; and

(iii) an assessment of the effectiveness of corrective action taken by the DNI or the head of the department concerned with respect to intelligence activities described in subsection 6(b)(i)(A) of this order.

SEC. 8. *Functions of Heads of Departments Concerned and Additional Functions of the Director of National Intelligence.*

(a) To the extent permitted by law, the DNI and the heads of departments concerned shall provide such information and assistance as the PIAB and the IOB determine is needed to perform their functions under this order.

(b) The heads of departments concerned shall:

(i) ensure that the DNI receives:

(A) copies of reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order; and

(B) such information and assistance as the DNI may need to perform functions under this order; and

(ii) designate the offices within their respective organizations that shall submit reports to the IOB required by Executive Order and inform the DNI and the IOB of such designations; and

(iii) ensure that departments concerned comply with instructions issued by the DNI under subsection 7(a)(ii) of this order.

(c) The head of a department concerned who does not implement a recommendation to that head of department from the PIAB under subsection 4(b) of this order or from the IOB under subsections 6(c) or 6(d) of this order shall promptly report through the DNI to the

Board that made the recommendation, or to the President, the reasons for not implementing the recommendation.

(d) The DNI shall ensure that the Director of the Central Intelligence Agency performs the functions with respect to the Central Intelligence Agency under this order that a head of a department concerned performs with respect to organizations within the intelligence community that are part of that department.

SEC. 9. *References and Transition.* (a) References in Executive Orders other than this order, or in any other presidential guidance, to the “President’s Foreign Intelligence Advisory Board” shall be deemed to be references to the President’s Intelligence Advisory Board established by this order.

(b) Individuals who are members of the President’s Foreign Intelligence Advisory Board under Executive Order 12863 of September 13, 1993, as amended, immediately prior to the signing of this order shall be members of the President’s Intelligence Advisory Board immediately upon the signing of this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(c) Individuals who are members of the Intelligence Oversight Board under Executive Order 12863 immediately prior to the signing of this order shall be members of the Intelligence Oversight Board under this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(d) The individual serving as Executive Director of the President’s Foreign Intelligence Advisory Board immediately prior to the signing of this order shall serve as the Executive Director of the PIAB until such person resigns, dies, or is removed, or upon appointment of a successor under this order and shall serve as the Executive Director of the IOB until an Executive Director of the IOB is appointed or designated under this order.

SEC. 10. *Revocation.* Executive Order 12863 is revoked.

SEC. 11. *General Provisions.*

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

(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 budget, administrative, or legislative proposals.

(b) Any person who is a member of the PIAB or the IOB, or who is granted access to classified national security information in relation to the activities of the PIAB or the IOB, as a condition of access to such information, shall sign and comply with appropriate agreements to protect such information from unauthorized disclosure. This order shall be implemented in a manner consistent with Executive Order 12958 of April 17, 1995, as amended, and Executive Order 12968 of August 2, 1995, as amended.

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

(d) This order is intended only to improve the internal management of the executive branch and 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.

GEORGE W. BUSH.

EX. ORD. NO. 13732. UNITED STATES POLICY ON PRE- AND POST-STRIKE MEASURES TO ADDRESS CIVILIAN CASUALTIES IN U.S. OPERATIONS INVOLVING THE USE OF FORCE

Ex. Ord. No. 13732, July 1, 2016, 81 F.R. 44485, as amended by Ex. Ord. No. 13862, §2, Mar. 6, 2019, 84 F.R. 8789, provided:

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

SECTION 1. *Purpose.* United States policy on civilian casualties resulting from U.S. operations involving the use of force in armed conflict or in the exercise of the Nation’s inherent right of self-defense is based on our national interests, our values, and our legal obligations. As a Nation, we are steadfastly committed to complying with our obligations under the law of armed conflict, including those that address the protection of civilians, such as the fundamental principles of necessity, humanity, distinction, and proportionality.

The protection of civilians is fundamentally consistent with the effective, efficient, and decisive use of force in pursuit of U.S. national interests. Minimizing civilian casualties can further mission objectives; help maintain the support of partner governments and vulnerable populations, especially in the conduct of counterterrorism and counterinsurgency operations; and enhance the legitimacy and sustainability of U.S. operations critical to our national security. As a matter of policy, the United States therefore routinely imposes certain heightened policy standards that are more protective than the requirements of the law of armed conflict that relate to the protection of civilians.

Civilian casualties are a tragic and at times unavoidable consequence of the use of force in situations of armed conflict or in the exercise of a state’s inherent right of self-defense. The U.S. Government shall maintain and promote best practices that reduce the likelihood of civilian casualties, take appropriate steps when such casualties occur, and draw lessons from our operations to further enhance the protection of civilians.

SEC. 2. *Policy.* In furtherance of U.S. Government efforts to protect civilians in U.S. operations involving the use of force in armed conflict or in the exercise of the Nation’s inherent right of self-defense, and with a view toward enhancing such efforts, relevant departments and agencies (agencies) shall continue to take certain measures in present and future operations.

(a) In particular, relevant agencies shall, consistent with mission objectives and applicable law, including the law of armed conflict:

(i) train personnel, commensurate with their responsibilities, on compliance with legal obligations and policy guidance that address the protection of civilians and on implementation of best practices that reduce the likelihood of civilian casualties, including through exercises, pre-deployment training, and simulations of complex operational environments that include civilians;

(ii) develop, acquire, and field intelligence, surveillance, and reconnaissance systems that, by enabling more accurate battlespace awareness, contribute to the protection of civilians;

(iii) develop, acquire, and field weapon systems and other technological capabilities that further enable the discriminate use of force in different operational contexts;

(iv) take feasible precautions in conducting attacks to reduce the likelihood of civilian casualties, such as providing warnings to the civilian population (unless the circumstances do not permit), adjusting the timing of attacks, taking steps to ensure military objectives and civilians are clearly distinguished, and taking other measures appropriate to the circumstances; and

(v) conduct assessments that assist in the reduction of civilian casualties by identifying risks to civilians and evaluating efforts to reduce risks to civilians.

(b) In addition to the responsibilities above, relevant agencies shall also, as appropriate and consistent with mission objectives and applicable law, including the law of armed conflict:

(i) review or investigate incidents involving civilian casualties, including by considering relevant and credible information from all available sources, such as other agencies, partner governments, and nongovernmental organizations, and take measures to mitigate the likelihood of future incidents of civilian casualties;

(ii) acknowledge U.S. Government responsibility for civilian casualties and offer condolences, including ex

gratia payments, to civilians who are injured or to the families of civilians who are killed;

(iii) engage with foreign partners to share and learn best practices for reducing the likelihood of and responding to civilian casualties, including through appropriate training and assistance; and

(iv) maintain channels for engagement with the International Committee of the Red Cross and other nongovernmental organizations that operate in conflict zones and encourage such organizations to assist in efforts to distinguish between military objectives and civilians, including by appropriately marking protected facilities, vehicles, and personnel, and by providing updated information on the locations of such facilities and personnel.

SEC. 3. *Report on Strikes Undertaken by the U.S. Government Against Terrorist Targets Outside Areas of Active Hostilities.* [Revoked by Ex. Ord. No. 13862, §2, Mar. 6, 2019, 84 F.R. 8789.]

SEC. 4. *Periodic Consultation.* In furtherance of the policies and practices set forth in this order, the Assistant to the President for National Security Affairs, through the National Security Council staff, will convene agencies with relevant defense, counterterrorism, intelligence, legal, civilian protection, and technology expertise to consult on civilian casualty trends, consider potential improvements to U.S. Government civilian casualty mitigation efforts, and, as appropriate, report to the Deputies and Principals Committees, consistent with Presidential Policy Directive 1 or its successor. Specific incidents will not be considered in this context, and will continue to be examined within relevant chains of command.

SEC. 5. *General Provisions.* (a) The policies and practices set forth above are not intended to alter, and shall be implemented consistent with, the authority and responsibility of commanders and other U.S. personnel to execute their mission as directed by the President or other appropriate authorities, which necessarily includes the inherent right of self-defense and the maintenance of good order and discipline among U.S. personnel. No part of this order modifies the chain of command of the U.S. Armed Forces or the authority of U.S. commanders.

(b) No part of this order modifies priorities in the collection of intelligence or the development, acquisition, or fielding of weapon systems and other technological capabilities.

(c) No part of this order shall prejudice or supplant established procedures pertaining to administrative or criminal investigative or judicial processes in the context of the military justice system or other applicable law and regulation.

(d) The policies set forth in this order are consistent with existing U.S. obligations under international law and are not intended to create new international legal obligations; nor shall anything in this order be construed to derogate from obligations under applicable law, including the law of armed conflict.

(e) 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. 14086. ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

Ex. Ord. No. 14086, Oct. 7, 2022, 87 F.R. 62283, 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 as follows:

SECTION 1. *Purpose.* The United States collects signals intelligence so that its national security decision-makers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United

States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.

SEC. 2. *Signals Intelligence Activities.*

(a) *Principles.* Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:

(A) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

(B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(iii) Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

(b) *Objectives.* Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

(i) *Legitimate objectives.*

(A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

(1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

(2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

(4) protecting against foreign military capabilities and activities;

(5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted

by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) protecting against threats to the personnel of the United States or of its allies or partners;

(10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section;

(11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section.

(B) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (Director) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(ii) *Prohibited objectives.*

(A) Signals intelligence collection activities shall not be conducted for the purpose of:

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

(2) suppressing or restricting legitimate privacy interests;

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

(B) It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

(iii) *Validation of signals intelligence collection priorities.*

(A) Under section 102A of the National Security Act of 1947, as amended (50 U.S.C. 3024), the Director must establish priorities for the Intelligence Community to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence. The Director does this through the National Intelligence Priorities Framework (NIPF), which the Director maintains and presents to the President, through the Assistant to the President for National Security Affairs, on a regular basis. In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with re-

gard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

(1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section;

(2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and

(3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(B) If the Director disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor framework, the Director shall include the CLPO's assessment and the Director's views when presenting the NIPF to the President.

(c) *Privacy and civil liberties safeguards.* The following safeguards shall fulfill the principles contained in subsections (a)(ii) and (a)(iii) of this section.

(i) *Collection of signals intelligence.*

(A) The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information. In determining whether to collect signals intelligence consistent with this principle, the United States—through an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

(B) Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

(C) For purposes of subsection (c)(i) of this section, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate.

(ii) *Bulk collection of signals intelligence.*

(A) Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination—by an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection. When it is determined to be necessary to engage in bulk collection in order to advance a validated intel-

ligence priority, the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.

(B) Each element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of the following objectives:

(1) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(5) protecting against threats to the personnel of the United States or of its allies or partners; and

(6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (c)(ii) of this section.

(C) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that bulk collection may be used. The Director shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(D) In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific identifiers or selection terms) shall be subject to the safeguards described in this subsection, unless such data is:

(1) used only to support the initial technical phase of the targeted signals intelligence collection activity;

(2) retained for only the short period of time required to complete this phase; and

(3) thereafter deleted.

(iii) *Handling of personal information collected through signals intelligence.*

(A) *Minimization.* Each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

(1) *Dissemination.* Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended [50 U.S.C. 3001 note], states may be disseminated in the case of information concerning United States persons;

(b) shall not disseminate personal information collected through signals intelligence solely because of a person's nationality or country of residence;

(c) shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;

(d) shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States Government, including to a foreign government or international organization; and

(e) shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

(2) *Retention.* Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall retain non-United States persons' personal information collected through signals intelligence only if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

(b) shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(c) shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

(B) *Data security and access.* Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(1) shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community directives, and associated policies;

(2) shall limit access to such personal information to authorized personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of applicable United States law, as described in policies and procedures issued under subsection (c)(iv) of this section; and

(3) shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

(C) *Data quality.* Each element of the Intelligence Community that handles personal information collected through signals intelligence shall include such personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity, with a focus on applying standards relating to the quality and reliability of the information, consideration of alter-

native sources of information and interpretations of data, and objectivity in performing analysis.

(D) *Queries of bulk collection.* Each element of the Intelligence Community that conducts queries of unminimized signals intelligence obtained by bulk collection shall do so consistent with the permissible uses of signals intelligence obtained by bulk collection identified in subsection (c)(ii)(B) of this section and according to policies and procedures issued under subsection (c)(iv) of this section, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(E) *Documentation.* In order to facilitate the oversight processes set forth in subsection (d) of this section and the redress mechanism set forth in section 3 of this order, each element of the Intelligence Community that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the Intelligence Community, based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.

(iv) *Update and publication of policies and procedures.* The head of each element of the Intelligence Community:

(A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD-28), until they are updated pursuant to subsection (c)(iv)(B) of this section;

(B) shall, within 1 year of the date of this order [Oct. 7, 2022], in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order; and

(C) shall, within 1 year of the date of this order, release these policies and procedures publicly to the maximum extent possible, consistent with the protection of intelligence sources and methods, in order to enhance the public's understanding of, and to promote public trust in, the safeguards pursuant to which the United States conducts signals intelligence activities.

(v) *Review by the PCLOB.*

(A) *Nature of review.* Consistent with applicable law, the PCLOB is encouraged to conduct a review of the updated policies and procedures described in subsection (c)(iv)(B) of this section once they have been issued to ensure that they are consistent with the enhanced safeguards contained in this order.

(B) *Consideration of review.* Within 180 days of completion of any review by the PCLOB described in subsection (c)(v)(A) of this section, the head of each element of the Intelligence Community shall carefully consider and shall implement or otherwise address all recommendations contained in such review, consistent with applicable law.

(d) *Subjecting signals intelligence activities to rigorous oversight.* The actions directed in this subsection are designed to build on the oversight mechanisms that elements of the Intelligence Community already have in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

(i) *Legal, oversight, and compliance officials.* Each element of the Intelligence Community that collects signals intelligence:

(A) shall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of

and ensure compliance with applicable United States law;

(B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities under this subsection.

(ii) *Training.* Each element of the Intelligence Community shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law.

(iii) *Significant incidents of non-compliance.*

(A) Each element of the Intelligence Community shall ensure that, if a legal, oversight, or compliance official, as described in subsection (d)(i) of this section, or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the Intelligence Community, the head of the executive department or agency (agency) containing the element of the Intelligence Community (to the extent relevant), and the Director.

(B) Upon receipt of such report, the head of the element of the Intelligence Community, the head of the agency containing the element of the Intelligence Community (to the extent relevant), and the Director shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(e) *Savings clause.* Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive.

SEC. 3. *Signals Intelligence Redress Mechanism.*

(a) *Purpose.* This section establishes a redress mechanism to review qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation.

(b) *Process for submission of qualifying complaints.* Within 60 days of the date of this order, the Director, in consultation with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence, shall establish a process for the submission of qualifying complaints transmitted by the appropriate public authority in a qualifying state.

(c) *Initial investigation of qualifying complaints by the CLPO.*

(i) *Establishment.* The Director, in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. This process shall govern how the CLPO will review qualifying complaints in a manner that protects classified or otherwise privileged or protected information and shall ensure, at a minimum, that for each qualifying complaint the CLPO shall:

(A) review information necessary to investigate the qualifying complaint;

(B) exercise its statutory and delegated authority to determine whether there was a covered violation by:

- (i) [sic] taking into account both relevant national security interests and applicable privacy protections;
- (ii) giving appropriate deference to any relevant determinations made by national security officials; and
- (iii) applying the law impartially;
- (C) determine the appropriate remediation for any covered violation;
- (D) provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure;
- (E) after the review is completed, inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:
 - (1) “the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation”;
 - (2) the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General pursuant to section 3(d)(i) of this order, apply for review of the CLPO’s determinations by the Data Protection Review Court described in subsection (d) of this section; and
 - (3) if either the complainant or an element of the Intelligence Community applies for review by the Data Protection Review Court, a special advocate will be selected by the Data Protection Review Court to advocate regarding the complainant’s interest in the matter;
- (F) maintain appropriate documentation of its review of the qualifying complaint and produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation, consistent with its statutory and delegated authority;
- (G) prepare a classified ex parte record of review, which shall consist of the appropriate documentation of its review of the qualifying complaint and the classified decision described in subsection (c)(i)(F) of this section; and
- (H) provide any necessary support to the Data Protection Review Court.
- (ii) *Binding effect.* Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by the CLPO to undertake appropriate remediation pursuant to subsection (c)(i)(C) of this section, subject to any contrary determination by the Data Protection Review Court.
- (iii) *Assistance.* Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the reviews described in subsection (c)(i) of this section, consistent with the protection of intelligence sources and methods, and shall not take any actions designed to impede or improperly influence the CLPO’s reviews. Privacy and civil liberties officials within elements of the Intelligence Community shall also support the CLPO as it performs the reviews described in subsection (c)(i) of this section.
- (iv) *Independence.* The Director shall not interfere with a review by the CLPO of a qualifying complaint under subsection (c)(i) of this section; nor shall the Director remove the CLPO for any actions taken pursuant to this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity.
- (d) *Data Protection Review Court.*
 - (i) *Establishment.* The Attorney General is authorized to and shall establish a process to review determina-

tions made by the CLPO under subsection (c)(i) of this section. In exercising that authority, the Attorney General shall, within 60 days of the date of this order, promulgate regulations establishing a Data Protection Review Court to exercise the Attorney General’s authority to review such determinations. These regulations shall, at a minimum, provide that:

(A) The Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB, shall appoint individuals to serve as judges on the Data Protection Review Court, who shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government. During their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.

(B) Upon receipt of an application for review filed by the complainant or an element of the Intelligence Community of a determination made by the CLPO under subsection (c) of this section, a three-judge panel of the Data Protection Review Court shall be convened to review the application. Service on the Data Protection Review Court panel shall require that the judge hold the requisite security clearances to access classified national security information.

(C) Upon being convened, the Data Protection Review Court panel shall select a special advocate through procedures prescribed in the Attorney General’s regulations. The special advocate shall assist the panel in its consideration of the application for review, including by advocating regarding the complainant’s interest in the matter and ensuring that the Data Protection Review Court panel is well informed of the issues and the law with respect to the matter. Service as a special advocate shall require that the special advocate hold the requisite security clearances to access classified national security information and to adhere to restrictions prescribed in the Attorney General’s regulations on communications with the complainant to ensure the protection of classified or otherwise privileged or protected information.

(D) The Data Protection Review Court panel shall impartially review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation. The review shall be based at a minimum on the classified ex parte record of review described in subsection (c)(i)(F) of this section and information or submissions provided by the complainant, the special advocate, or an element of the Intelligence Community. In reviewing determinations made by the CLPO, the Data Protection Review Court panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

(E) In the event that the Data Protection Review Court panel disagrees with any of the CLPO’s determinations with respect to whether a covered violation occurred or the appropriate remediation in the event there was such a violation, the panel shall issue its own determinations.

(F) The Data Protection Review Court panel shall provide a classified report on information indicating a violation of any authority subject to the oversight of the FISC to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure.

(G) After the review is completed, the CLPO shall be informed of the Data Protection Review Court panel’s determinations through procedures prescribed by the Attorney General’s regulations.

(H) After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

(ii) *Binding effect.* Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

(iii) *Assistance.* Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the review described in subsection (d)(i) of this section, consistent with the protection of intelligence sources and methods, that a Data Protection Review Court panel requests from the CLPO and shall not take any actions for the purpose of impeding or improperly influencing a panel's review.

(iv) *Independence.* The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act [probably means the Judicial Improvements Act of 2002] (28 U.S.C. 351 et seq.).

(v) *Record of determinations.* For each qualifying complaint transmitted by the appropriate public authority in a qualifying state, the Secretary of Commerce shall:

(A) maintain a record of the complainant who submitted such complaint;

(B) not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint by the CLPO has been declassified and whether information pertaining to the review of any application for review submitted to the Data Protection Review Court has been declassified, including whether an element of the Intelligence Community filed an application for review with the Data Protection Review Court; and

(C) if informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or to the review of any application for review submitted to the Data Protection Review Court may be available under applicable law.

(e) *Annual review by PCLOB of redress process.*

(i) *Nature of review.* Consistent with applicable law, the PCLOB is encouraged to conduct an annual review of the processing of qualifying complaints by the redress mechanism established by section 3 of this order, including whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner; whether the CLPO and the Data Protection Review Court are obtaining full access to necessary information; whether the CLPO and the Data Protection Review Court are operating consistent with this order; whether the safeguards established by section 2 of this order are properly considered in the processes of the CLPO and the Data Protection Review Court; and whether the elements of the Intelligence Community have fully complied with determinations made by the CLPO and the Data Protection Review Court.

(ii) *Assistance.* The Attorney General, the CLPO, and the elements of the Intelligence Community shall provide the PCLOB with access to information necessary to conduct the review described in subsection (e)(i) of this section, consistent with the protection of intelligence sources and methods.

(iii) *Report and certification.* Within 30 days of completing any review described in subsection (e)(i) of this section, the PCLOB is encouraged to:

(A) provide the President, the Attorney General, the Director, the heads of elements of the Intelligence Community, the CLPO, and the congressional intelligence committees with a classified report detailing the results of its review;

(B) release to the public an unclassified version of the report; and

(C) make an annual public certification as to whether the redress mechanism established pursuant to section 3 of this order is processing complaints consistent with this order.

(iv) *Consideration of review.* Within 180 days of receipt of any report by the PCLOB described in subsection (e)(iii)(A) of this section, the Attorney General, the Director, the heads of elements of the Intelligence Community, and the CLPO shall carefully consider and shall implement or otherwise address all recommendations contained in such report, consistent with applicable law.

(f) *Designation of qualifying state.*

(i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and

(C) such designation would advance the national interests of the United States.

(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or

(C) such designation is not in the national interests of the United States.

SEC. 4. *Definitions.* For purposes of this order:

(a) “Appropriate remediation” means lawful measures designed to fully redress an identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant’s complaint, taking into account the ways that a violation of the kind identified have customarily been addressed. Such measures may include, depending on the specific covered violation at issue, curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorized, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law. Appropriate remediation shall be narrowly tailored to redress the covered violation and to minimize adverse impacts on the operations of the Intelligence Community and the national security of the United States.

(b) “Bulk collection” means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).

(c) “Counterintelligence” shall have the same meaning as it has in Executive Order 12333 [50 U.S.C. 3001 note].

(d) “Covered violation” means a violation that:

(i) arises from signals intelligence activities conducted after the date of this order regarding data transferred to the United States from a qualifying state after the effective date of the Attorney General’s designation for such state, as provided in section 3(f)(i) of this order;

(ii) adversely affects the complainant’s individual privacy and civil liberties interests; and

(iii) violates one or more of the following:

(A) the United States Constitution;

(B) the applicable sections of FISA or any applicable FISC-approved procedures;

(C) Executive Order 12333 or any applicable agency procedures pursuant to Executive Order 12333;

(D) this order or any applicable agency policies and procedures issued or updated pursuant to this order (or the policies and procedures identified in section 2(c)(iv)(A) of this order before they are updated pursuant to section 2(c)(iv)(B) of this order);

(E) any successor statute, order, policies, or procedures to those identified in section 4(d)(iii)(B)–(D) of this order; or

(F) any other statute, order, policies, or procedures adopted after the date of this order that provides privacy and civil liberties safeguards with respect to United States signals intelligence activities within the scope of this order, as identified in a list published and updated by the Attorney General, in consultation with the Director of National Intelligence.

(e) “Foreign intelligence” shall have the same meaning as it has in Executive Order 12333.

(f) “Intelligence” shall have the same meaning as it has in Executive Order 12333.

(g) “Intelligence Community” and “elements of the Intelligence Community” shall have the same meaning as they have in Executive Order 12333.

(h) “National security” shall have the same meaning as it has in Executive Order 13526 of December 29, 2009 (Classified National Security Information) [50 U.S.C. 3161 note].

(i) “Non-United States person” means a person who is not a United States person.

(j) “Personnel of the United States or of its allies or partners” means any current or former member of the

Armed Forces of the United States, any current or former official of the United States Government, and any other person currently or formerly employed by or working on behalf of the United States Government, as well as any current or former member of the military, current or former official, or other person currently or formerly employed by or working on behalf of an ally or partner.

(k) “Qualifying complaint” means a complaint, submitted in writing, that:

(i) alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General’s designation for such state, as provided in section 3(f)(i) of this order;

(ii) includes the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant’s data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;

(iii) is not frivolous, vexatious, or made in bad faith;

(iv) is brought on behalf of the complainant, acting on that person’s own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(v) is transmitted by the appropriate public authority in a qualifying state, after it has verified the identity of the complainant and that the complaint satisfies the conditions of section 5(k)(i)–(iv) of this order.

(l) “Significant incident of non-compliance” shall mean a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.

(m) “United States person” shall have the same meaning as it has in Executive Order 12333.

(n) “Validated intelligence priority” shall mean, for most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrow circumstances (for example, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President or the head of an element of the Intelligence Community in accordance with the criteria described in section 2(b)(iii)(A)(1)–(3) of this order to the extent feasible.

(o) “Weapons of mass destruction” shall have the same meaning as it has in Executive Order 13526.

SEC. 5. *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, 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 orders of and procedures approved by the FISC, and subject to the availability of appropriations.

(c) Nothing in this order precludes the application of more privacy-protective safeguards for United States signals intelligence activities that would apply in the absence of this order. In the case of any conflict between this order and other applicable law, the more privacy-protective safeguards shall govern the conduct of

signals intelligence activities, to the maximum extent allowed by law.

(d) Nothing in this order prohibits elements of the Intelligence Community from disseminating information relating to a crime for law enforcement purposes; disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; notifying victims or warning potential victims of crime; or complying with dissemination obligations required by statute, treaty, or court order, including orders of and procedures approved by the FISC or other court orders.

(e) The collection, retention, and dissemination of information concerning United States persons is governed by multiple legal and policy requirements, such as those required by FISA and Executive Order 12333. This order is not intended to alter the rules applicable to United States persons adopted pursuant to FISA, Executive Order 12333, or other applicable law.

(f) This order shall apply to signals intelligence activities consistent with the scope of PPD-28's application to such activities prior to PPD-28's partial revocation by the national security memorandum issued concurrently with this order. To implement this subsection, the head of each agency containing an element of the Intelligence Community, in consultation with the Attorney General and the Director, is hereby delegated the authority to issue guidance, which may be classified, as appropriate, as to the scope of application of this order with respect to the element or elements of the Intelligence Community within their agency. The CLPO and the Data Protection Review Court, in carrying out the functions assigned to it under this order, shall treat such guidance as authoritative and binding.

(g) Nothing in this order confers authority to declassify or disclose classified national security information except as authorized pursuant to Executive Order 13526 or any successor order. Consistent with the requirements of Executive Order 13526, the CLPO, the Data Protection Review Court, and the special advocates shall not have authority to declassify classified national security information, nor shall they disclose any classified or otherwise privileged or protected information except to authorized and appropriately cleared individuals who have a need to know the information.

(h) This order creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO's decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of this order. This order is not intended to, and does not, create any other entitlement, 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. This order is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law.

J.R. BIDEN, JR.

EFFECTIVE DATES OF PROVISIONS IN TITLE I OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, provided:

Memorandum for 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 the Office of Management and Budget[, and] the Director of National Intelligence

Subsection 1097(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, December 17, 2004) (the Act) [set out in a note above] provides:

(a) IN GENERAL- Except as otherwise expressly provided in this Act, this title and the amendments made by this title shall take effect not later than 6 months after the date of the enactment of this Act.

Subsection 1097(a) clearly contemplates that one or more of the provisions in Title I of the Act may take effect earlier than the date that is 6 months after the date of enactment of the Act, but does not state explicitly the mechanism for determining when such earlier effect shall occur, leaving it to the President in the execution of the Act. Moreover, given that section 1097(a) evinces a legislative intent to afford the President flexibility, and such flexibility is constitutionally appropriate with respect to intelligence matters (see *United States v. Curtiss-Wright Export Corporation*, 299 U.S. 304 (1936)), the executive branch shall construe section 1097(a) to authorize the President to select different effective dates that precede the 6-month deadline for different provisions in Title I.

Therefore, pursuant to the Constitution and the laws of the United States of America, including subsection 1097(a) of the Act, I hereby determine and direct:

1. Sections 1097(a) and 1103 of the Act [set out in notes above], relating respectively to effective dates of provisions and to severability, shall take effect immediately upon the signing of this memorandum to any extent that they have not already taken effect.

2. Provisions in Title I of the Act other than those addressed in numbered paragraph 1 of this memorandum shall take effect immediately upon the signing of this memorandum, except:

(a) any provision in Title I of the Act for which the Act expressly provides the date on which the provision shall take effect; and

(b) sections 1021 and 1092 of the Act [enacting section 3056 of this title and provisions set out in a note above, respectively], relating to the National Counterterrorism Center.

The taking of effect of a provision pursuant to section 1097(a) of the Act and this memorandum shall not affect the construction of such provision by the executive branch as set forth in my Statement of December 17, 2004, upon signing the Act into law.

The Director of the Office of Management and Budget is authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

§ 3002. Congressional declaration of purpose

In enacting this chapter, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, for