

**TITLE 6 - DOMESTIC SECURITY**

**CHAPTER 1 - HOMELAND SECURITY ORGANIZATION**

**SUBCHAPTER II - INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION**

**Part A - Information and Analysis and Infrastructure Protection; Access to Information**

**§ 121. Information and Analysis and Infrastructure Protection**

**(a) Intelligence and analysis and infrastructure protection**

There shall be in the Department an Office of Intelligence and Analysis and an Office of Infrastructure Protection.

**(b) Under Secretary for Intelligence and Analysis and Assistant Secretary for Infrastructure Protection**

**(1) Office of Intelligence and Analysis**

The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

**(2) Chief Intelligence Officer**

The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

**(3) Office of Infrastructure Protection**

The Office of Infrastructure Protection shall be headed by an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

**(c) Discharge of responsibilities**

The Secretary shall ensure that the responsibilities of the Department relating to information analysis and infrastructure protection, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis or the Assistant Secretary for Infrastructure Protection, as appropriate.

**(d) Responsibilities of Secretary relating to intelligence and analysis and infrastructure protection**

The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection shall be as follows:

**(1)** To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o), in order to—

**(A)** identify and assess the nature and scope of terrorist threats to the homeland;

**(B)** detect and identify threats of terrorism against the United States; and

**(C)** understand such threats in light of actual and potential vulnerabilities of the homeland.

**(2)** To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

**(3)** To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in

order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

(4) To ensure, pursuant to section 122 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

(7) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 485 of this title, including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

(8) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(9) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(10) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(11) To ensure that—

(A) any material received pursuant to this chapter is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this chapter is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(12) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(13) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

- (14) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—
- (A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and
  - (B) treat information in such databases in a manner that complies with applicable Federal law on privacy.
- (15) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.
- (16) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.
- (17) To provide intelligence and information analysis and support to other elements of the Department.
- (18) To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.
- (19) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence.
- (20) To establish a structure and process to support the missions and goals of the intelligence components of the Department.
- (21) To ensure that, whenever possible, the Department—
- (A) produces and disseminates unclassified reports and analytic products based on open-source information; and
  - (B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.
- (22) To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.
- (23) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—
- (A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and
  - (B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.
- (24) To perform such other duties relating to such responsibilities as the Secretary may provide.
- (25) To prepare and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security in the House of Representatives, and to other appropriate congressional committees having jurisdiction over the critical infrastructure or key resources, for each sector identified in the National Infrastructure Protection Plan, a report on the comprehensive assessments carried out by the Secretary of the critical infrastructure and key resources of the United States, evaluating threat, vulnerability, and consequence, as required under this subsection. Each such report—
- (A) shall contain, if applicable, actions or countermeasures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in the assessments;

(B) shall be required for fiscal year 2007 and each subsequent fiscal year and shall be submitted not later than 35 days after the last day of the fiscal year covered by the report; and

(C) may be classified.

**(e) Staff**

**(1) In general**

The Secretary shall provide the Office of Intelligence and Analysis and the Office of Infrastructure Protection with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section.

**(2) Private sector analysts**

Analysts under this subsection may include analysts from the private sector.

**(3) Security clearances**

Analysts under this subsection shall possess security clearances appropriate for their work under this section.

**(f) Detail of personnel**

**(1) In general**

In order to assist the Office of Intelligence and Analysis and the Office of Infrastructure Protection in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

**(2) Covered agencies**

The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

**(3) Cooperative agreements**

The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

**(4) Basis**

The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

**(g) Functions transferred**

In accordance with subchapter XII of this chapter, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscript.html>).

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

(Pub. L. 107–296, title II, § 201, Nov. 25, 2002, 116 Stat. 2145; Pub. L. 110–53, title V, §§ 501(a)(2)(A), (b), 531 (a), title X, § 1002(a), Aug. 3, 2007, 121 Stat. 309, 332, 374; Pub. L. 110–417, [div. A], title IX, § 931(b)(5), Oct. 14, 2008, 122 Stat. 4575.)

## References in Text

This chapter, referred to in subsec. (d)(11), was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The National Security Act of 1947, referred to in subsec. (d)(11)(B), is act July 26, 1947, ch. 343, 61 Stat. 495, as amended. For complete classification of this Act to the Code, see Short Title note set out under section 401 of Title 50, War and National Defense, and Tables.

## Codification

Section is comprised of section 201 of Pub. L. 107–296. Subsec. (h) of section 201 of Pub. L. 107–296 amended section 401a of Title 50, War and National Defense.

## Amendments

2008—Subsec. (f)(2)(E). Pub. L. 110–417, which directed substitution of “National Geospatial-Intelligence Agency” for “National Imagery and Mapping Agency” in subsec. (e)(2), was executed by making the substitution in subsec. (f)(2)(E) to reflect the probable intent of Congress, because the language to be stricken did not appear in subsec. (e)(2).

2007—Pub. L. 110–53, § 531(a)(1), substituted “Information and” for “Directorate for Information” in section catchline.

Subsecs. (a) to (c). Pub. L. 110–53, § 531(a)(2), added subsecs. (a) to (c) and struck out former subsecs. (a) to (c) which related to, in subsec. (a), establishment and responsibilities of Directorate for Information Analysis and Infrastructure Protection, in subsec. (b), positions of Assistant Secretary for Information Analysis and Assistant Secretary for Infrastructure Protection, and, in subsec. (c), Secretary’s duty to ensure that responsibilities regarding information analysis and infrastructure protection would be carried out through the Under Secretary for Information Analysis and Infrastructure Protection.

Subsec. (d). Pub. L. 110–53, § 531(a)(3), substituted “Secretary relating to intelligence and analysis and infrastructure protection” for “Under Secretary” in heading and “The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection” for “Subject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection” in introductory provisions.

Subsec. (d)(1). Pub. L. 110–53, § 501(b)(1), inserted “, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o),” after “to integrate such information” in introductory provisions.

Subsec. (d)(7). Pub. L. 110–53, § 501(b)(2), added par. (7) and struck out former par. (7) which read as follows: “To review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities.”

Pub. L. 110–53, § 501(a)(2)(A), redesignated par. (8) as (7) and struck out former par. (7) which read as follows: “To administer the Homeland Security Advisory System, including—

“(A) exercising primary responsibility for public advisories related to threats to homeland security; and

“(B) in coordination with other agencies of the Federal Government, providing specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public.”

Subsec. (d)(8). Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (9) as (8). Former par. (8) redesignated (7).

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscprint.html>).*

Subsec. (d)(9). Pub. L. 110–53, § 531(a)(3)(C), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (10) as (9). Former par. (9) redesignated (8).

Subsec. (d)(10). Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (11) as (10). Former par. (10) redesignated (9).

Subsec. (d)(11). Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (12) as (11). Former par. (11) redesignated (10).

Subsec. (d)(11)(B). Pub. L. 110–53, § 531(a)(3)(D), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Subsec. (d)(12) to (17). Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated pars. (13) to (18) as (12) to (17), respectively. Former par. (12) redesignated (11).

Subsec. (d)(18). Pub. L. 110–53, § 531(a)(3)(E), (F), added par. (18) and redesignated former par. (18) as (24).

Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (19) as (18). Former par. (18) redesignated (17).

Subsec. (d)(19). Pub. L. 110–53, § 531(a)(3)(F), added par. (19).

Pub. L. 110–53, § 501(a)(2)(A)(ii), redesignated par. (19) as (18).

Subsec. (d)(20) to (23). Pub. L. 110–53, § 531(a)(3)(F), added pars. (20) to (23).

Subsec. (d)(24). Pub. L. 110–53, § 531(a)(3)(E), redesignated par. (18) as (24).

Subsec. (d)(25). Pub. L. 110–53, § 1002(a), added par. (25).

Subsec. (e)(1). Pub. L. 110–53, § 531(a)(4), substituted “provide the Office of Intelligence and Analysis and the Office of Infrastructure Protection” for “provide the Directorate” and “assist such offices in discharging” for “assist the Directorate in discharging”.

Subsec. (f)(1). Pub. L. 110–53, § 531(a)(5), substituted “Office of Intelligence and Analysis and the Office of Infrastructure Protection” for “Directorate”.

Subsec. (g). Pub. L. 110–53, § 531(a)(6), substituted “Office of Intelligence and Analysis and the Office of Infrastructure Protection” for “Under Secretary for Information Analysis and Infrastructure Protection” in introductory provisions.

## Regulations

Pub. L. 109–295, title V, § 550, Oct. 4, 2006, 120 Stat. 1388, as amended by Pub. L. 110–161, div. E, title V, § 534, Dec. 26, 2007, 121 Stat. 2075, provided that:

“(a) No later than six months after the date of enactment of this Act [Oct. 4, 2006], the Secretary of Homeland Security shall issue interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for chemical facilities: Provided, That such regulations shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk: Provided further, That such regulations shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility: Provided further, That the Secretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section: Provided further, That the Secretary may approve alternative security programs established by private sector entities, Federal, State, or local authorities, or other applicable laws if the Secretary determines that the requirements of such programs meet the requirements of this section and the interim regulations: Provided further, That the Secretary shall review and approve each vulnerability assessment and site security plan required under this section: Provided further, That the Secretary shall not apply regulations issued pursuant to this section to facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Public Law 107–295, as amended [see Tables for classification]; Public Water Systems, as defined by section 1401 of the Safe Drinking Water Act, Public Law 93–523, as amended [42 U.S.C. 300f]; Treatment Works as defined in section 212 of the Federal Water Pollution Control Act, Public Law 92–500, as amended [33 U.S.C. 1292]; any facility owned or operated by the Department of Defense or the Department of Energy, or any facility subject to regulation by the Nuclear Regulatory Commission.

“(b) Interim regulations issued under this section shall apply until the effective date of interim or final regulations promulgated under other laws that establish requirements and standards referred to in subsection (a) and expressly supersede this section: Provided, That the authority provided by this section shall terminate three years after the date of enactment of this Act [Oct. 4, 2006].

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscp.html>).*

“(c) Notwithstanding any other provision of law and subsection (b), information developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title 46, United States Code: Provided, That this subsection does not prohibit the sharing of such information, as the Secretary deems appropriate, with State and local government officials possessing the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this section, provided that such information may not be disclosed pursuant to any State or local law: Provided further, That in any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material.

“(d) Any person who violates an order issued under this section shall be liable for a civil penalty under section 70119 (a) of title 46, United States Code: Provided, That nothing in this section confers upon any person except the Secretary a right of action against an owner or operator of a chemical facility to enforce any provision of this section.

“(e) The Secretary of Homeland Security shall audit and inspect chemical facilities for the purposes of determining compliance with the regulations issued pursuant to this section.

“(f) Nothing in this section shall be construed to supersede, amend, alter, or affect any Federal law that regulates the manufacture, distribution in commerce, use, sale, other treatment, or disposal of chemical substances or mixtures.

“(g) If the Secretary determines that a chemical facility is not in compliance with this section, the Secretary shall provide the owner or operator with written notification (including a clear explanation of deficiencies in the vulnerability assessment and site security plan) and opportunity for consultation, and issue an order to comply by such date as the Secretary determines to be appropriate under the circumstances: Provided, That if the owner or operator continues to be in noncompliance, the Secretary may issue an order for the facility to cease operation, until the owner or operator complies with the order.

“(h) This section shall not preclude or deny any right of any State or political subdivision thereof to adopt or enforce any regulation, requirement, or standard of performance with respect to chemical facility security that is more stringent than a regulation, requirement, or standard of performance issued under this section, or otherwise impair any right or jurisdiction of any State with respect to chemical facilities within that State, unless there is an actual conflict between this section and the law of that State.”

### **Treatment of Incumbent Under Secretary for Intelligence and Analysis**

Pub. L. 110–53, title V, § 531(c), Aug. 3, 2007, 121 Stat. 335, provided that: “The individual administratively performing the duties of the Under Secretary for Intelligence and Analysis as of the date of the enactment of this Act [Aug. 3, 2007] may continue to perform such duties after the date on which the President nominates an individual to serve as the Under Secretary pursuant to section 201 of the Homeland Security Act of 2002 [6 U.S.C. 121], as amended by this section, and until the individual so appointed assumes the duties of the position.”

### **Reports To Be Submitted to Certain Committees**

Pub. L. 110–53, title XXIV, § 2403, Aug. 3, 2007, 121 Stat. 547, provided that: “The Committee on Commerce, Science, and Transportation of the Senate shall receive the reports required by the following provisions of law in the same manner and to the same extent that the reports are to be received by the Committee on Homeland Security and Governmental Affairs of the Senate:

“(1) Section 1016(j)(1) of the Intelligence Reform and Terrorist [Terrorism] Prevention Act of 2004 (6 U.S.C. 485 (j)(1)).

“(2) Section 511(d) of this Act [121 Stat. 323].

“(3) Subsection (a)(3)(D) of section 2022 of the Homeland Security Act of 2002 [6 U.S.C. 612 (a)(3)(D)], as added by section 101 of this Act.

“(4) Section 7215(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 123 (d)).

“(5) Section 7209(b)(1)(C) of the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458] (8 U.S.C. 1185 note ).

“(6) Section 804(c) of this Act [42 U.S.C. 2000ee–3 (c)].

“(7) Section 901(b) of this Act [121 Stat. 370].

“(8) Section 1002(a) of this Act [amending this section].

“(9) Title III of this Act [enacting sections 579 and 580 of this title and amending sections 194 and 572 of this title].”

## Security Management Systems Demonstration Project

Pub. L. 110–53, title XXIV, § 2404, Aug. 3, 2007, 121 Stat. 548, provided that:

“(a) Demonstration Project Required.—Not later than 120 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security shall—

“(1) establish a demonstration project to conduct demonstrations of security management systems that—

“(A) shall use a management system standards approach; and

“(B) may be integrated into quality, safety, environmental and other internationally adopted management systems; and

“(2) enter into one or more agreements with a private sector entity to conduct such demonstrations of security management systems.

“(b) Security Management System Defined.—In this section, the term ‘security management system’ means a set of guidelines that address the security assessment needs of critical infrastructure and key resources that are consistent with a set of generally accepted management standards ratified and adopted by a standards making body.”

## Ex. Ord. No. 13231. Critical Infrastructure Protection in the Information Age

Ex. Ord. No. 13231, Oct. 16, 2001, 66 F.R. 53063, as amended by Ex. Ord. No. 13284, § 2, Jan. 23, 2003, 68 F.R. 4075; Ex. Ord. No. 13286, § 7, Feb. 28, 2003, 68 F.R. 10620; Ex. Ord. No. 13385, § 5, Sept. 29, 2005, 70 F.R. 57990, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

Section 1. Policy. The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

Sec. 2. Continuing Authorities. This order does not alter the existing authorities or roles of United States Government departments and agencies. Authorities set forth in 44 U.S.C. chapter 35, and other applicable law, provide senior officials with responsibility for the security of Federal Government information systems.

(a) Executive Branch Information Systems Security. The Director of the Office of Management and Budget (OMB) has the responsibility to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, except those noted in section 2(b) of this order. The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices within the purview of this section in an executive branch department or agency.

(b) National Security Information Systems. The Secretary of Defense and the Director of Central Intelligence (DCI) shall have responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.

(i) Policies, principles, standards, and guidelines developed under this subsection may require more stringent protection than those developed in accordance with section 2(a) of this order.

(ii) The Assistant to the President for National Security Affairs shall advise the President and the appropriate department or agency when there is a critical deficiency in the security practices of a department or agency within the purview of this section.

(iii) National Security Systems. The National Security Telecommunications and Information Systems Security Committee, as established by and consistent with NSD–42 and chaired by the Department of Defense, shall be designated as the “Committee on National Security Systems.”

(c) Additional Responsibilities. The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscript.html>).*

preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

Sec. 3. The National Infrastructure Advisory Council. The National Infrastructure Advisory Council (NIAC), established on October 16, 2001, shall provide the President through the Secretary of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems.

(a) Membership. The NIAC shall be composed of not more than 30 members appointed by the President, taking appropriate account of the benefits of having members (i) from the private sector, including but not limited to banking and finance, transportation, energy, communications, and emergency services organizations and institutions of higher learning, and State, local, and tribal governments, (ii) with senior leadership responsibilities for the reliability and availability, which include security, of the critical infrastructure and key resource sectors, (iii) with expertise relevant to the functions of the NIAC, and (iv) with experience equivalent to that of a chief executive of an organization. Unless otherwise determined by the President, no full-time officer or employee of the executive branch shall be appointed to serve as a member of the NIAC. The President shall designate from among the members of the NIAC a Chair and a Vice Chair, who shall perform the functions of the Chair if the Chair is absent, disabled, or in the instance of a vacancy in the Chair.

(b) Functions of the NIAC. The NIAC shall meet periodically to:

(i) enhance the partnership of the public and private sectors in protecting critical infrastructures and their information systems and provide reports on this issue to the President through the Secretary of Homeland Security, as appropriate;

(ii) propose and develop ways to encourage private industry to perform periodic risk assessments;

(iii) monitor the development and operations of private sector coordinating councils and their information sharing mechanisms and provide recommendations to the President through the Secretary of Homeland Security on how these organizations can best foster improved cooperation among the sectors, the Department of Homeland Security, and other Federal Government entities;

(iv) report to the President through the Secretary of Homeland Security, who shall ensure appropriate coordination with the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs under the terms of this order; and

(v) advise sector specific agencies with critical infrastructure responsibilities to include issues pertaining to sector and government coordinating councils and their information sharing mechanisms.

(c) Administration of the NIAC.

(i) The NIAC may hold hearings, conduct inquiries, and establish subcommittees, as appropriate.

(ii) Upon request of the Chair, and to the extent permitted by law, the heads of the executive departments and agencies shall provide the NIAC with information and advice relating to its functions.

(iii) Senior Federal Government officials may participate in the meetings of the NIAC, as appropriate.

(iv) Members shall serve without compensation for their work on the NIAC. However, members may be reimbursed for travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service (5 U.S.C. 5701–5707).

(v) To the extent permitted by law and subject to the availability of appropriations, the Department of Homeland Security shall provide the NIAC with administrative services, staff, and other support services, and such funds as may be necessary for the performance of the NIAC's functions.

Sec. 4. Judicial Review. This order does not create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush.

### **Extension of Term of National Infrastructure Advisory Council**

Term of the National Infrastructure Advisory Council extended until Sept. 30, 2005, by Ex. Ord. No. 13316, Sept. 17, 2003, 68 F.R. 55255, formerly set out as a note under section 14 of the Federal Advisory Committee Act in the Appendix to Title 5, Government Organizations and Employees.

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscprint.html>).*

Term of the National Infrastructure Advisory Council extended until Sept. 30, 2007, by Ex. Ord. No. 13385, Sept. 29, 2005, 70 F.R. 57989, formerly set out as a note under section 14 of the Federal Advisory Committee Act in the Appendix to Title 5.

Term of the National Infrastructure Advisory Council extended until Sept. 30, 2009, by Ex. Ord. No. 13446, Sept. 28, 2007, 72 F.R. 56175, set out as a note under section 14 of the Federal Advisory Committee Act in the Appendix to Title 5.

### **Ex. Ord. No. 13284. Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security**

Ex. Ord. No. 13284, Jan. 23, 2003, 68 F.R. 4075, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Homeland Security Act of 2002 (Public Law 107–296) [see Tables for classification], and the National Security Act of 1947, as amended (50 U.S.C. 401 et seq.), and in order to reflect responsibilities vested in the Secretary of Homeland Security and take other actions in connection with the establishment of the Department of Homeland Security, it is hereby ordered as follows:

Section 1. [Amended Ex. Ord. No. 13234.]

Sec. 2. [Amended Ex. Ord. No. 13231, set out above.]

Sec. 3. Executive Order 13228 of October 8, 2001 (“Establishing the Office of Homeland Security and the Homeland Security Council”) [50 U.S.C. 402 note ], is amended by inserting “the Secretary of Homeland Security,” after “the Secretary of Transportation,” in section 5 (b). Further, during the period from January 24, 2003, until March 1, 2003, the Secretary of Homeland Security shall have the responsibility for coordinating the domestic response efforts otherwise assigned to the Assistant to the President for Homeland Security pursuant to section 3(g) of Executive Order 13228.

Sec. 4. [Amended Ex. Ord. No. 13224, listed in a table under section 1701 of Title 50, War and National Defense.]

Sec. 5. [Amended Ex. Ord. No. 13151, set out as a note under section 5195 of Title 42, The Public Health and Welfare.]

Sec. 6. [Amended Ex. Ord. No. 13122, set out as a note under section 3121 of Title 42, The Public Health and Welfare.]

Sec. 7. [Amended Ex. Ord. No. 13048, set out as a note under section 501 of Title 31, Money and Finance.]

Sec. 8. [Amended Ex. Ord. No. 12992, set out as a note under section 1708 of Title 21, Food and Drugs.]

Sec. 9. [Amended Ex. Ord. No. 12881, set out as a note under section 6601 of Title 42, The Public Health and Welfare.]

Sec. 10. [Amended Ex. Ord. No. 12859, set out as a note preceding section 101 of Title 3, The President.]

Sec. 11. [Amended Ex. Ord. No. 12590, set out as a note under former section 1201 of Title 21, Food and Drugs.]

Sec. 12. [Amended Ex. Ord. No. 12260, set out as a note under section 2511 of Title 19, Customs Duties.]

Sec. 13. [Amended Ex. Ord. No. 11958, set out as a note under section 2751 of Title 22, Foreign Relations and Intercourse.]

Sec. 14. [Amended Ex. Ord. No. 11423, set out as a note under section 301 of Title 3, The President.]

Sec. 15. [Amended Ex. Ord. No. 10865, set out as a note under section 435 of Title 50, War and National Defense.]

Sec. 16. [Amended Ex. Ord. No. 13011, set out as a note under section 11101 of Title 40, Public Buildings, Property, and Works.]

Sec. 17. Those elements of the Department of Homeland Security that are supervised by the Department’s Under Secretary for Information Analysis and Infrastructure Protection through the Department’s Assistant Secretary for Information Analysis, with the exception of those functions that involve no analysis of foreign intelligence information, are designated as elements of the Intelligence Community under section 201(h) of the Homeland Security Act of 2002 [Pub. L. 107–296, amending 50 U.S.C. 401a] and section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4)).

Sec. 18. [Amended Ex. Ord. No. 12333, set out as a note under section 401 of title 50, War and National Defense.]

Sec. 19. Functions of Certain Officials in the Department of Homeland Security.

The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a “Senior Official of the Intelligence Community” for purposes of Executive Order 12333 [50 U.S.C. 401 note ], and all other relevant authorities, and shall:

*NB: This unofficial compilation of the U.S. Code is current as of Jan. 5, 2009 (see <http://www.law.cornell.edu/uscode/uscpri.html>).*

(a) recognize and give effect to all current clearances for access to classified information held by those who become employees of the Department of Homeland Security by operation of law pursuant to the Homeland Security Act of 2002 or by Presidential appointment;

(b) recognize and give effect to all current clearances for access to classified information held by those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities;

(c) make all clearance and access determinations pursuant to Executive Order 12968 of August 2, 1995 [50 U.S.C. 435 note ], or any successor Executive Order, as to employees of, and applicants for employment in, the Department of Homeland Security who do not then hold a current clearance for access to classified information; and

(d) ensure all clearance and access determinations for those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities are made in accordance with Executive Order 12829 of January 6, 1993 [50 U.S.C. 435 note ].

Sec. 20. Pursuant to the provisions of section 1.4 of Executive Order 12958 of April 17, 1995 (“Classified National Security Information”) [50 U.S.C. 435 note ], I hereby authorize the Secretary of Homeland Security to classify information originally as “Top Secret.” Any delegation of this authority shall be in accordance with section 1.4 of that order or any successor Executive Orders.

Sec. 21. This order shall become effective on January 24, 2003.

Sec. 22. This order does not create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush.