

the matter being considered by the Advisory Committee shall constitute a quorum.

**(g) Conflict of interest rules**

The Advisory Committee shall establish rules for determining when 1 of its members has a conflict of interest in a matter being considered by the Advisory Committee.

**(h) Reports**

**(1) Annual report**

The Advisory Committee shall render an annual report to the Under Secretary for Science and Technology for transmittal to Congress on or before January 31 of each year. Such report shall describe the activities and recommendations of the Advisory Committee during the previous year.

**(2) Additional reports**

The Advisory Committee may render to the Under Secretary for transmittal to Congress such additional reports on specific policy matters as it considers appropriate.

**(i) Exemption from chapter 10 of title 5**

Section 1013 of title 5 shall not apply to the Advisory Committee.

**(j) Termination**

The Department of Homeland Security Science and Technology Advisory Committee shall terminate on December 31, 2008.

(Pub. L. 107–296, title III, §311, Nov. 25, 2002, 116 Stat. 2174; Pub. L. 108–334, title V, §520, Oct. 18, 2004, 118 Stat. 1318; Pub. L. 109–347, title III, §302(a), Oct. 13, 2006, 120 Stat. 1920; Pub. L. 117–286, §4(a)(14), Dec. 27, 2022, 136 Stat. 4306.)

**Editorial Notes**

AMENDMENTS

2022—Subsec. (i). Pub. L. 117–286 substituted “Exemption from chapter 10 of title 5” for “Federal Advisory Committee Act exemption” in heading and “Section 1013 of title 5” for “Section 14 of the Federal Advisory Committee Act” in text.

2006—Subsec. (j). Pub. L. 109–347 substituted “on December 31, 2008” for “3 years after the effective date of this chapter”.

2004—Subsec. (c)(2). Pub. L. 108–334 amended heading and text of par. (2) generally. Prior to amendment, text read as follows: “The original members of the Advisory Committee shall be appointed to three classes of three members each. One class shall have a term of 1 year, 1 a term of 2 years, and the other a term of 3 years.”

**Statutory Notes and Related Subsidiaries**

EFFECTIVE DATE OF 2006 AMENDMENT

Pub. L. 109–347, title III, §302(b), Oct. 13, 2006, 120 Stat. 1921, provided that: “The amendment made by subsection (a) [amending this section] shall be effective as if enacted on the date of the enactment of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) [Nov. 25, 2002].”

**§ 192. Homeland Security Institute**

**(a) Establishment**

The Secretary shall establish a federally funded research and development center to be known as the “Homeland Security Institute” (in this section referred to as the “Institute”).

**(b) Administration**

The Institute shall be administered as a separate entity by the Secretary.

**(c) Duties**

The duties of the Institute shall be determined by the Secretary, and may include the following:

(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation’s critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities.

(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.

(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.

(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.

(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.

(7) Design of and support for the conduct of homeland security-related exercises and simulations.

(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation’s critical infrastructure and key resources.

**(d) Consultation on Institute activities**

In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, nonprofit institutions, other Government agencies, and federally funded research and development centers.

**(e) Use of centers**

The Institute shall utilize the capabilities of the National Infrastructure Simulation and Analysis Center.

**(f) Annual reports**

The Institute shall transmit to the Secretary and Congress an annual report on the activities of the Institute under this section.

**(g) Termination**

The Homeland Security Institute shall terminate 5 years after its establishment.

(Pub. L. 107–296, title III, §312, Nov. 25, 2002, 116 Stat. 2176; Pub. L. 108–334, title V, §519, Oct. 18, 2004, 118 Stat. 1318.)

**Editorial Notes**

AMENDMENTS

2004—Subsec. (g). Pub. L. 108–334 amended heading and text of subsec. (g) generally. Prior to amendment,

text read as follows: “The Homeland Security Institute shall terminate 3 years after the effective date of this chapter.”

**§ 193. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security**

**(a) Establishment of program**

The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 111 of this title).

**(b) Elements of program**

The program described in subsection (a) shall include the following components:

(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private sector entities for additional review, purchase, or use.

(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.

(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private sector efforts to evaluate and implement the use of technologies described in paragraph (1) or (2).

(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.

**(c) Miscellaneous provisions**

**(1) In general**

Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology to be used by the Department, any other executive agency, any State or local government entity, or any private sector entity.

**(2) Certain proposals**

The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

**(3) Coordination**

In carrying out this section, the Secretary shall coordinate with the Technical Support Working Group (organized under the April 1982 National Security Decision Directive Numbered 30).

(Pub. L. 107–296, title III, §313, Nov. 25, 2002, 116 Stat. 2176.)

**§ 194. Enhancement of public safety communications interoperability**

**(a) Coordination of public safety interoperable communications programs**

**(1) Program**

The Secretary of Homeland Security, in consultation with the Secretary of Commerce and the Chairman of the Federal Communications Commission, shall establish a program to enhance public safety interoperable communications at all levels of government. Such program shall—

(A) establish a comprehensive national approach to achieving public safety interoperable communications;

(B) coordinate with other Federal agencies in carrying out subparagraph (A);

(C) develop, in consultation with other appropriate Federal agencies and State and local authorities, appropriate minimum capabilities for communications interoperability for Federal, State, and local public safety agencies;

(D) accelerate, in consultation with other Federal agencies, including the National Institute of Standards and Technology, the private sector, and nationally recognized standards organizations as appropriate, the development of national voluntary consensus standards for public safety interoperable communications, recognizing—

(i) the value, life cycle, and technical capabilities of existing communications infrastructure;

(ii) the need for cross-border interoperability between States and nations;

(iii) the unique needs of small, rural communities; and

(iv) the interoperability needs for daily operations and catastrophic events;

(E) encourage the development and implementation of flexible and open architectures incorporating, where possible, technologies that currently are commercially available, with appropriate levels of security, for short-term and long-term solutions to public safety communications interoperability;

(F) assist other Federal agencies in identifying priorities for research, development, and testing and evaluation with regard to public safety interoperable communications;

(G) identify priorities within the Department of Homeland Security for research, development, and testing and evaluation with regard to public safety interoperable communications;

(H) establish coordinated guidance for Federal grant programs for public safety interoperable communications;

(I) provide technical assistance to State and local public safety agencies regarding planning, acquisition strategies, interoperability architectures, training, and other functions necessary to achieve public safety communications interoperability;

(J) develop and disseminate best practices to improve public safety communications interoperability; and

(K) develop appropriate performance measures and milestones to systematically meas-