

ary and Judicial Procedure. For complete classification of title II to the Code, see Tables.

AMENDMENTS

2003—Subsec. (b). Pub. L. 108-7 inserted before period at end “: *Provided*, That any such transfer shall be carried out in accordance with section 605 of Public Law 107-77”.

§ 165. National Law Enforcement and Corrections Technology Centers

(a) In general

The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as “Centers”) and, to the extent necessary, establish new centers through a merit-based, competitive process.

(b) Purpose of Centers

The purpose of the Centers shall be to—

- (1) support research and development of law enforcement technology;
- (2) support the transfer and implementation of technology;
- (3) assist in the development and dissemination of guidelines and technological standards; and
- (4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

(c) Annual meeting

Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

(d) Report

Not later than 12 months after November 25, 2002, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

(Pub. L. 107-296, title II, § 235, Nov. 25, 2002, 116 Stat. 2162.)

SUBCHAPTER III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

§ 181. Under Secretary for Science and Technology

There shall be in the Department a Directorate of Science and Technology headed by an Under Secretary for Science and Technology.

(Pub. L. 107-296, title III, § 301, Nov. 25, 2002, 116 Stat. 2163.)

§ 182. Responsibilities and authorities of the Under Secretary for Science and Technology

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

- (1) advising the Secretary regarding research and development efforts and priorities in support of the Department’s missions;
- (2) developing, in consultation with other appropriate executive agencies, a national pol-

icy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government’s civilian efforts to identify and develop countermeasures to chemical, biological, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the Director of the Cybersecurity and Infrastructure Security Agency, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 8401 of title 7;

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as “select agents” in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 262a of title 42;

(10) supporting United States leadership in science and technology;

(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;

(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; and

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout

the Department, and for the dissemination of research conducted or sponsored by the Department.

(Pub. L. 107-296, title III, §302, Nov. 25, 2002, 116 Stat. 2163; Pub. L. 109-347, title V, §501(b)(2), Oct. 13, 2006, 120 Stat. 1935; Pub. L. 110-53, title V, §531(b)(1)(C), Aug. 3, 2007, 121 Stat. 334; Pub. L. 115-278, §2(g)(3)(A), Nov. 16, 2018, 132 Stat. 4178.)

Editorial Notes

AMENDMENTS

2018—Par. (2). Pub. L. 115-278, §2(g)(3)(A)(i), substituted “biological,” for “biological,,”.

Par. (3). Pub. L. 115-278, §2(g)(3)(A)(ii), substituted “Director of the Cybersecurity and Infrastructure Security Agency” for “Assistant Secretary for Infrastructure Protection”.

Par. (5)(A). Pub. L. 115-278, §2(g)(3)(A)(i), substituted “biological,” for “biological,,”.

2007—Par. (3). Pub. L. 110-53 substituted “Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection” for “Under Secretary for Information Analysis and Infrastructure Protection”.

2006—Pars. (2), (5)(A). Pub. L. 109-347 struck out “radiological, nuclear” after “biological,,”.

§ 183. Functions transferred

In accordance with subchapter XII, there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of the following entities:

(1) The following programs and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto (but not including programs and activities relating to the strategic nuclear defense posture of the United States):

(A) The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program.

(B) The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program. The programs and activities described in this subparagraph may be designated by the President either for transfer to the Department or for joint operation by the Secretary and the Secretary of Energy.

(C) The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program.

(D) Such life sciences activities of the biological and environmental research program related to microbial pathogens as may be designated by the President for transfer to the Department.

(E) The Environmental Measurements Laboratory.

(F) The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.

(2) The National Bio-Weapons Defense Analysis Center of the Department of Defense, including the functions of the Secretary of Defense related thereto.

(Pub. L. 107-296, title III, §303, Nov. 25, 2002, 116 Stat. 2164.)

§ 184. Conduct of certain public health-related activities

(a) In general

With respect to civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities, goals, objectives, and policies and develop a coordinated strategy for such activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed pursuant to section 182(2) of this title.

(b) Evaluation of progress

In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in such subsection.

(Pub. L. 107-296, title III, §304, Nov. 25, 2002, 116 Stat. 2165.)

Editorial Notes

CODIFICATION

Section is comprised of section 304 of Pub. L. 107-296. Subsec. (c) of section 304 of Pub. L. 107-296 amended section 233 of Title 42, The Public Health and Welfare.

§ 185. Federally funded research and development centers

The Secretary, acting through the Under Secretary for Science and Technology, shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this chapter, including coordinating and integrating both the extramural and intramural programs described in section 188 of this title.

(Pub. L. 107-296, title III, §305, Nov. 25, 2002, 116 Stat. 2168.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, 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.

§ 186. Miscellaneous provisions

(a) Classification

To the greatest extent practicable, research conducted or supported by the Department shall be unclassified.

(b) Construction

Nothing in this subchapter shall be construed to preclude any Under Secretary of the Depart-

ment from carrying out research, development, demonstration, or deployment activities, as long as such activities are coordinated through the Under Secretary for Science and Technology.

(c) Regulations

The Secretary, acting through the Under Secretary for Science and Technology, may issue necessary regulations with respect to research, development, demonstration, testing, and evaluation activities of the Department, including the conducting, funding, and reviewing of such activities.

(d) Notification of Presidential life sciences designations

Not later than 60 days before effecting any transfer of Department of Energy life sciences activities pursuant to section 183(1)(D) of this title, the President shall notify the appropriate congressional committees of the proposed transfer and shall include the reasons for the transfer and a description of the effect of the transfer on the activities of the Department of Energy.

(Pub. L. 107-296, title III, §306, Nov. 25, 2002, 116 Stat. 2168.)

§ 187. Homeland Security Advanced Research Projects Agency

(a) Definitions

In this section:

(1) Fund

The term “Fund” means the Acceleration Fund for Research and Development of Homeland Security Technologies established in subsection (c).

(2) Homeland security research

The term “homeland security research” means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.

(3) HSARPA

The term “HSARPA” means the Homeland Security Advanced Research Projects Agency established in subsection (b).

(4) Under Secretary

The term “Under Secretary” means the Under Secretary for Science and Technology.

(b) Homeland Security Advanced Research Projects Agency

(1) Establishment

There is established the Homeland Security Advanced Research Projects Agency.

(2) Director

HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary.

(3) Responsibilities

The Director shall administer the Fund to award competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including businesses, federally funded research and development centers, and universities. The Director shall administer the Fund to—

(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;

(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies;

(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities; and

(D) conduct research and development for the purpose of advancing technology for the investigation of child exploitation crimes, including child victim identification, trafficking in persons, and child pornography, and for advanced forensics.

(4) Targeted competitions

The Director may solicit proposals to address specific vulnerabilities identified by the Director.

(5) Coordination

The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies.

(6) Personnel

In hiring personnel for HSARPA, the Secretary shall have the hiring and management authorities described in section 1101¹ of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105-261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.

(7) Demonstrations

The Director, periodically, shall hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel.

(c) Fund

(1) Establishment

There is established the Acceleration Fund for Research and Development of Homeland Security Technologies, which shall be administered by the Director of HSARPA.

(2) Authorization of appropriations

There are authorized to be appropriated \$500,000,000 to the Fund for fiscal year 2003 and such sums as may be necessary thereafter.

(3) Coast Guard

Of the funds authorized to be appropriated under paragraph (2), not less than 10 percent of such funds for each fiscal year through fiscal year 2005 shall be authorized only for the Under Secretary, through joint agreement with the Commandant of the Coast Guard, to carry out research and development of improved ports, waterways and coastal security surveillance and perimeter protection capabilities for the purpose of minimizing the possibility that Coast Guard cutters, aircraft, helicopters, and personnel will be diverted

¹ See References in Text note below.

from non-homeland security missions to the ports, waterways and coastal security mission. (Pub. L. 107–296, title III, § 307, Nov. 25, 2002, 116 Stat. 2168; Pub. L. 114–22, title III, § 302(c), formerly § 302(d), May 29, 2015, 129 Stat. 255; renumbered § 302(d), Pub. L. 115–392, § 23(c)(2), Dec. 21, 2018, 132 Stat. 5264.)

Editorial Notes

REFERENCES IN TEXT

Section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, referred to in subsec. (b)(6), is section 1101 of Pub. L. 105–261, which was formerly set out as a note under section 3104 of Title 5, Government Organization and Employees, prior to repeal by Pub. L. 114–328, div. A, title XI, § 1121(b), Dec. 23, 2016, 130 Stat. 2452. See section 4092 of Title 10, Armed Forces.

AMENDMENTS

2015—Subsec. (b)(3)(D). Pub. L. 114–22 added subpar. (D).

§ 188. Conduct of research, development, demonstration, testing and evaluation

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the responsibilities under section 182(4) of this title through both extramural and intramural programs.

(b) Extramural programs

(1) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—

(A) ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practicable participate;

(B) ensure that the research funded is of high quality, as determined through merit review processes developed under section 182(14) of this title; and

(C) distribute funds through grants, cooperative agreements, and contracts.

(2) University-based centers for homeland security

(A) Designation

The Secretary, acting through the Under Secretary for Science and Technology, shall designate a university-based center or several university-based centers for homeland security. The purpose of the center or these centers shall be to establish a coordinated, university-based system to enhance the Nation's homeland security.

(B) Criteria for designation

Criteria for the designation of colleges or universities as a center for homeland security, shall include, but are not limited to, demonstrated expertise in—

- (i) The training of first responders.
- (ii) Responding to incidents involving weapons of mass destruction and biological warfare.

(iii) Emergency and diagnostic medical services.

(iv) Chemical, biological, radiological, and nuclear countermeasures or detection.

(v) Animal and plant health and diagnostics.

(vi) Food safety.

(vii) Water and wastewater operations.

(viii) Port and waterway security.

(ix) Multi-modal transportation.

(x) Information security and information engineering.

(xi) Engineering.

(xii) Educational outreach and technical assistance.

(xiii) Border transportation and security.

(xiv) The public policy implications and public dissemination of homeland security related research and development.

(C) Discretion of Secretary

To the extent that exercising such discretion is in the interest of homeland security, and with respect to the designation of any given university-based center for homeland security, the Secretary may except certain criteria as specified in subparagraph (B) and consider additional criteria beyond those specified in subparagraph (B). Upon designation of a university-based center for homeland security, the Secretary shall that day publish in the Federal Register the criteria that were excepted or added in the selection process and the justification for the set of criteria that were used for that designation.

(D) Report to Congress

The Secretary shall report annually, from the date of enactment, to Congress concerning the implementation of this section. That report shall indicate which center or centers have been designated and how the designation or designations enhance homeland security, as well as report any decisions to revoke or modify such designations.

(E) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this paragraph.

(c) Intramural programs

(1) Consultation

In carrying out the duties under section 182 of this title, the Secretary, acting through the Under Secretary for Science and Technology, may draw upon the expertise of any laboratory of the Federal Government, whether operated by a contractor or the Government.

(2) Laboratories

The Secretary, acting through the Under Secretary for Science and Technology, may establish a headquarters laboratory for the Department at any laboratory or site and may establish additional laboratory units at other laboratories or sites.

(3) Criteria for headquarters laboratory

If the Secretary chooses to establish a headquarters laboratory pursuant to paragraph (2), then the Secretary shall do the following:

- (A) Establish criteria for the selection of the headquarters laboratory in consultation

with the National Academy of Sciences, appropriate Federal agencies, and other experts.

(B) Publish the criteria in the Federal Register.

(C) Evaluate all appropriate laboratories or sites against the criteria.

(D) Select a laboratory or site on the basis of the criteria.

(E) Report to the appropriate congressional committees on which laboratory was selected, how the selected laboratory meets the published criteria, and what duties the headquarters laboratory shall perform.

(4) Limitation on operation of laboratories

No laboratory shall begin operating as the headquarters laboratory of the Department until at least 30 days after the transmittal of the report required by paragraph (3)(E).

(d) Preference for United States industry

(1) Definitions

In this subsection:

(A) Country of concern

The term “country of concern” means a country that—

(i) is a covered nation, as such term is defined in section 4872(d) of title 10; or

(ii) the Secretary determines is engaged in conduct that is detrimental to the national security of the United States.

(B) Nonprofit organization; small business firm; subject invention

The terms “nonprofit organization”, “small business firm”, and “subject invention” have the meanings given such terms in section 201 of title 35.

(C) Manufactured substantially in the United States

The term “manufactured substantially in the United States” means an item is a domestic end product.

(D) Domestic end product

The term “domestic end product” has the meaning given such term in section 25.003 of title 48, Code of Federal Regulations, or any successor thereto.

(3)¹ Waivers

(A) In general

Subject to subparagraph (B), in individual cases, the requirements under section 204 of title 35 may be waived by the Secretary upon a showing by the small business firm, nonprofit organization, or assignee that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that under the circumstances domestic manufacture is not commercially feasible.

(B) Conditions on waivers granted by Department

(i) Before grant of waiver

Before granting a waiver under subparagraph (A), the Secretary shall comply with

the procedures developed and implemented by the Department pursuant to section 70923(b)(2) of the Build America, Buy America Act (enacted as subtitle A of title IX of division G of Public Law 117-58).

(ii) Prohibition on granting certain waivers

The Secretary may not grant a waiver under subparagraph (A) if, as a result of such waiver, products embodying the applicable subject invention, or produced through the use of the applicable subject invention, would be manufactured substantially in a country of concern.

(Pub. L. 107-296, title III, § 308, Nov. 25, 2002, 116 Stat. 2170; Pub. L. 108-7, div. L, § 101(1), Feb. 20, 2003, 117 Stat. 526; Pub. L. 117-263, div. G, title LXXI, § 7114, Dec. 23, 2022, 136 Stat. 3633.)

Editorial Notes

REFERENCES IN TEXT

The date of enactment, referred to in subsec. (b)(2)(D), probably means the date of enactment of this section by Pub. L. 107-296, which was approved Nov. 25, 2002.

Section 70923(b)(2) of the Build America, Buy America Act, referred to in subsec. (d)(3)(B)(i), is section 70923(b)(2) of Pub. L. 117-58, div. G, title IX, Nov. 15, 2021, 135 Stat. 1306, which is not classified to the Code.

AMENDMENTS

2022—Subsec. (d). Pub. L. 117-263 added subsec. (d).

2003—Subsecs. (a) to (c)(1). Pub. L. 108-7 added subsecs. (a) to (c)(1) and struck out former subsecs. (a) to (c)(1) which related to the responsibilities of the Secretary, acting through the Under Secretary for Science and Technology, to carry out the responsibilities under section 182(4) of this title through both extramural and intramural programs, to operate extramural research, development, demonstration, testing, and evaluation programs, to establish a coordinated, university-based system to enhance the Nation's homeland security, and to draw upon the expertise of any laboratory of the Federal Government.

§ 189. Utilization of Department of Energy national laboratories and sites in support of homeland security activities

(a) Authority to utilize national laboratories and sites

(1) In general

In carrying out the missions of the Department, the Secretary may utilize the Department of Energy national laboratories and sites through any 1 or more of the following methods, as the Secretary considers appropriate:

(A) A joint sponsorship arrangement referred to in subsection (b).

(B) A direct contract between the Department and the applicable Department of Energy laboratory or site, subject to subsection (c).

(C) Any “work for others” basis made available by that laboratory or site.

(D) Any other method provided by law.

(2) Acceptance and performance by labs and sites

Notwithstanding any other law governing the administration, mission, use, or operations of any of the Department of Energy national laboratories and sites, such laboratories

¹ So in original. There is no par. (2).

and sites are authorized to accept and perform work for the Secretary, consistent with resources provided, and perform such work on an equal basis to other missions at the laboratory and not on a noninterference basis with other missions of such laboratory or site.

(b) Joint sponsorship arrangements

(1) Laboratories

The Department may be a joint sponsor, under a multiple agency sponsorship arrangement with the Department of Energy, of 1 or more Department of Energy national laboratories in the performance of work.

(2) Sites

The Department may be a joint sponsor of a Department of Energy site in the performance of work as if such site were a federally funded research and development center and the work were performed under a multiple agency sponsorship arrangement with the Department.

(3) Primary sponsor

The Department of Energy shall be the primary sponsor under a multiple agency sponsorship arrangement referred to in paragraph (1) or (2).

(4) Lead agent

The Secretary of Energy shall act as the lead agent in coordinating the formation and performance of a joint sponsorship arrangement under this subsection between the Department and a Department of Energy national laboratory or site.

(5) Federal Acquisition Regulation

Any work performed by a Department of Energy national laboratory or site under a joint sponsorship arrangement under this subsection shall comply with the policy on the use of federally funded research and development centers under the Federal Acquisition Regulations.

(6) Funding

The Department shall provide funds for work at the Department of Energy national laboratories or sites, as the case may be, under a joint sponsorship arrangement under this subsection under the same terms and conditions as apply to the primary sponsor of such national laboratory under section 3303(a)(1)(C) of title 41 or of such site to the extent such section applies to such site as a federally funded research and development center by reason of this subsection.

(c) Separate contracting

To the extent that programs or activities transferred by this chapter from the Department of Energy to the Department of Homeland Security are being carried out through direct contracts with the operator of a national laboratory or site of the Department of Energy, the Secretary of Homeland Security and the Secretary of Energy shall ensure that direct contracts for such programs and activities between the Department of Homeland Security and such operator are separate from the direct contracts of the Department of Energy with such operator.

(d) Authority with respect to cooperative research and development agreements and licensing agreements

In connection with any utilization of the Department of Energy national laboratories and sites under this section, the Secretary may permit the director of any such national laboratory or site to enter into cooperative research and development agreements or to negotiate licensing agreements with any person, any agency or instrumentality, of the United States, any unit of State or local government, and any other entity under the authority granted by section 3710a of title 15. Technology may be transferred to a non-Federal party to such an agreement consistent with the provisions of sections 3710 and 3710a of title 15.

(e) Reimbursement of costs

In the case of an activity carried out by the operator of a Department of Energy national laboratory or site in connection with any utilization of such laboratory or site under this section, the Department of Homeland Security shall reimburse the Department of Energy for costs of such activity through a method under which the Secretary of Energy waives any requirement for the Department of Homeland Security to pay administrative charges or personnel costs of the Department of Energy or its contractors in excess of the amount that the Secretary of Energy pays for an activity carried out by such contractor and paid for by the Department of Energy.

(f) Laboratory directed research and development by the Department of Energy

No funds authorized to be appropriated or otherwise made available to the Department in any fiscal year may be obligated or expended for laboratory directed research and development activities carried out by the Department of Energy unless such activities support the missions of the Department of Homeland Security.

(g) Office for National Laboratories

There is established within the Directorate of Science and Technology an Office for National Laboratories, which shall be responsible for the coordination and utilization of the Department of Energy national laboratories and sites under this section in a manner to create a networked laboratory system for the purpose of supporting the missions of the Department.

(h) Department of Energy coordination on homeland security related research

The Secretary of Energy shall ensure that any research, development, test, and evaluation activities conducted within the Department of Energy that are directly or indirectly related to homeland security are fully coordinated with the Secretary to minimize duplication of effort and maximize the effective application of Federal budget resources.

(Pub. L. 107-296, title III, § 309, Nov. 25, 2002, 116 Stat. 2172.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in subsec. (c), 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.

CODIFICATION

In subsec. (b)(6), “section 3303(a)(1)(C) of title 41” substituted for “section 303(b)(1)(C) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(b)(1)(C))” on authority of Pub. L. 111–350, §6(c), Jan. 4, 2011, 124 Stat. 3854, which Act enacted Title 41, Public Contracts.

Statutory Notes and Related Subsidiaries

SECURING ENERGY INFRASTRUCTURE

Pub. L. 116–92, div. E, title LVII, §5726, Dec. 20, 2019, 133 Stat. 2179, provided that:

“(a) DEFINITIONS.—In this section:

“(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ means—

“(A) the congressional intelligence committees [Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives];

“(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Energy and Natural Resources of the Senate; and

“(C) the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives.

“(2) COVERED ENTITY.—The term ‘covered entity’ means an entity identified pursuant to section 9(a) of Executive Order No. 13636 of February 12, 2013 (78 Fed. Reg. 11742) [6 U.S.C. 121 note], relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

“(3) EXPLOIT.—The term ‘exploit’ means a software tool designed to take advantage of a security vulnerability.

“(4) INDUSTRIAL CONTROL SYSTEM.—The term ‘industrial control system’ means an operational technology used to measure, control, or manage industrial functions, and includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

“(5) NATIONAL LABORATORY.—The term ‘National Laboratory’ has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

“(6) PROGRAM.—The term ‘Program’ means the pilot program established under subsection (b).

“(7) SECRETARY.—Except as otherwise specifically provided, the term ‘Secretary’ means the Secretary of Energy.

“(8) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

“(b) PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

“(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

“(2) evaluating technology and standards, in partnership with covered entities, to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

“(A) analog and nondigital control systems;

“(B) purpose-built control systems; and

“(C) physical controls.

“(c) WORKING GROUP TO EVALUATE PROGRAM STANDARDS AND DEVELOP STRATEGY.—

“(1) ESTABLISHMENT.—The Secretary shall establish a working group—

“(A) to evaluate the technology and standards used in the Program under subsection (b)(2); and

“(B) to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

“(2) MEMBERSHIP.—The working group established under paragraph (1) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

“(A) The Department of Energy.

“(B) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

“(C)(i) The Department of Homeland Security; or

“(ii) the Industrial Control Systems Cyber Emergency Response Team.

“(D) The North American Electric Reliability Corporation.

“(E) The Nuclear Regulatory Commission.

“(F)(i) The Office of the Director of National Intelligence; or

“(ii) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

“(G)(i) The Department of Defense; or

“(ii) the Assistant Secretary of Defense for Homeland Security and America’s Security Affairs.

“(H) A State or regional energy agency.

“(I) A national research body or academic institution.

“(J) The National Laboratories.

“(d) REPORTS ON THE PROGRAM.—

“(1) INTERIM REPORT.—Not later than 180 days after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees an interim report that—

“(A) describes the results of the Program;

“(B) includes an analysis of the feasibility of each method studied under the Program; and

“(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

“(2) FINAL REPORT.—Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees a final report that—

“(A) describes the results of the Program;

“(B) includes an analysis of the feasibility of each method studied under the Program; and

“(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

“(e) EXEMPTION FROM DISCLOSURE.—Information shared by or with the Federal Government or a State, Tribal, or local government under this section—

“(1) shall be deemed to be voluntarily shared information;

“(2) shall be exempt from disclosure under section 552 of title 5, United States Code, or any provision of any State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records; and

“(3) shall be withheld from the public, without discretion, under section 552(b)(3) of title 5, United States Code, and any provision of any State, Tribal, or local law requiring the disclosure of information or records.

“(f) PROTECTION FROM LIABILITY.—

“(1) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under subsection (b)—

“(A) shall not lie or be maintained in any court; and

“(B) shall be promptly dismissed by the applicable court.

“(2) VOLUNTARY ACTIVITIES.—Nothing in this section subjects any covered entity to liability for not engaging in the voluntary activities authorized under subsection (b).

“(g) NO NEW REGULATORY AUTHORITY FOR FEDERAL AGENCIES.—Nothing in this section authorizes the Secretary or the head of any other department or agency of the Federal Government to issue new regulations.

“(h) AUTHORIZATION OF APPROPRIATIONS.—

“(1) PILOT PROGRAM.—There is authorized to be appropriated \$10,000,000 to carry out subsection (b).

“(2) WORKING GROUP AND REPORT.—There is authorized to be appropriated \$1,500,000 to carry out subsections (c) and (d).

“(3) AVAILABILITY.—Amounts made available under paragraphs (1) and (2) shall remain available until expended.”

§ 190. Transfer of Plum Island Animal Disease Center, Department of Agriculture

(a) In general

In accordance with subchapter XII, the Secretary of Agriculture shall transfer to the Secretary of Homeland Security the Plum Island Animal Disease Center of the Department of Agriculture, including the assets and liabilities of the Center.

(b) Continued Department of Agriculture access

On completion of the transfer of the Plum Island Animal Disease Center under subsection (a), the Secretary of Homeland Security and the Secretary of Agriculture shall enter into an agreement to ensure that the Department of Agriculture is able to carry out research, diagnostic, and other activities of the Department of Agriculture at the Center.

(c) Direction of activities

The Secretary of Agriculture shall continue to direct the research, diagnostic, and other activities of the Department of Agriculture at the Center described in subsection (b).

(d) Notification

(1) In general

At least 180 days before any change in the biosafety level at the Plum Island Animal Disease Center, the President shall notify Congress of the change and describe the reasons for the change.

(2) Limitation

No change described in paragraph (1) may be made earlier than 180 days after the completion of the transition period (as defined in section 541 of this title).

(Pub. L. 107-296, title III, § 310, Nov. 25, 2002, 116 Stat. 2174.)

Statutory Notes and Related Subsidiaries

TRANSFER OF NATIONAL BIO AND AGRO-DEFENSE FACILITY

Pub. L. 117-328, div. A, title VII, § 775, Dec. 29, 2022, 136 Stat. 4509, provided that: “In this or any subsequent fiscal year, the Secretary of Homeland Security shall transfer to the Secretary of Agriculture the operation of and all property required to operate the National Bio- and Agro-Defense Facility in Manhattan, Kansas:

Provided, That, such transfer of function shall include the transfer of up to 40 full time equivalent positions, to be completed within 120 days of the effective date of the transfer of function, as jointly determined by the Secretaries.”

Similar provisions were contained in the following prior acts:

Pub. L. 117-103, div. A, title VII, § 730, Mar. 15, 2022, 136 Stat. 92.

Pub. L. 116-94, div. B, title VII, § 766, Dec. 20, 2019, 133 Stat. 2655.

DISPOSITION OF PLUM ISLAND PROPERTY AND TRANSPORTATION ASSETS

Pub. L. 116-260, div. FF, title V, § 501(c), Dec. 27, 2020, 134 Stat. 3136, provided that: “The Administrator of General Services shall ensure that—

“(1) Federal property commonly known as Plum Island, New York, including the Orient point facility, all real and personal property and transportation assets that support Plum Island operations and access to Plum Island, be disposed of as a single consolidated asset; and

“(2) such disposal is subject to conditions as may be necessary to protect Government interests and meet program requirements.”

Pub. L. 112-74, div. D, title V, § 538, Dec. 23, 2011, 125 Stat. 976, which related to disposition of property and transportation assets if the National Bio and Agro-Defense Facility were relocated from Plum Island, New York, was repealed by Pub. L. 116-260, div. FF, title V, § 501(b), Dec. 27, 2020, 134 Stat. 3136.

§ 191. Homeland Security Science and Technology Advisory Committee

(a) Establishment

There is established within the Department a Homeland Security Science and Technology Advisory Committee (in this section referred to as the “Advisory Committee”). The Advisory Committee shall make recommendations with respect to the activities of the Under Secretary for Science and Technology, including identifying research areas of potential importance to the security of the Nation.

(b) Membership

(1) Appointment

The Advisory Committee shall consist of 20 members appointed by the Under Secretary for Science and Technology, which shall include emergency first-responders or representatives of organizations or associations of emergency first-responders. The Advisory Committee shall also include representatives of citizen groups, including economically disadvantaged communities. The individuals appointed as members of the Advisory Committee—

(A) shall be eminent in fields such as emergency response, research, engineering, new product development, business, and management consulting;

(B) shall be selected solely on the basis of established records of distinguished service;

(C) shall not be employees of the Federal Government; and

(D) shall be so selected as to provide representation of a cross-section of the research, development, demonstration, and deployment activities supported by the Under Secretary for Science and Technology.

(2) National Research Council

The Under Secretary for Science and Technology may enter into an arrangement for the

National Research Council to select members of the Advisory Committee, but only if the panel used by the National Research Council reflects the representation described in paragraph (1).

(c) Terms of office

(1) In general

Except as otherwise provided in this subsection, the term of office of each member of the Advisory Committee shall be 3 years.

(2) Original appointments

The original members of the Advisory Committee shall be appointed to three classes. One class of six shall have a term of 1 year, one class of seven a term of 2 years, and one class of seven a term of 3 years.

(3) Vacancies

A member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of such term.

(d) Eligibility

A person who has completed two consecutive full terms of service on the Advisory Committee shall thereafter be ineligible for appointment during the 1-year period following the expiration of the second such term.

(e) Meetings

The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members so request in writing. Each member shall be given appropriate notice of the call of each meeting, whenever possible not less than 15 days before the meeting.

(f) Quorum

A majority of the members of the Advisory Committee not having a conflict of interest in 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 home-

land 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 measure the Nation's progress toward achieving public safety communications interoperability, including the development of national voluntary consensus standards.

(2) Office for Interoperability and Compatibility

(A) Establishment of Office

The Secretary may establish an Office for Interoperability and Compatibility within the Directorate of Science and Technology to carry out this subsection.

(B) Functions

If the Secretary establishes such office, the Secretary shall, through such office—

- (i) carry out Department of Homeland Security responsibilities and authorities relating to the SAFECOM Program; and
- (ii) carry out section 510¹ of the Homeland Security Act of 2002, as added by subsection (d).

(3) Authorization of appropriations

There are authorized to be appropriated to the Secretary to carry out this subsection—

- (A) \$22,105,000 for fiscal year 2005;
- (B) \$22,768,000 for fiscal year 2006;
- (C) \$23,451,000 for fiscal year 2007;
- (D) \$24,155,000 for fiscal year 2008; and
- (E) \$24,879,000 for fiscal year 2009.

(b) Report

Not later than 120 days after December 17, 2004, the Secretary shall report to the Congress on Department of Homeland Security plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications, a schedule of milestones for such development, and achievements of such development.

(c) International interoperability

Not later than 18 months after December 17, 2004, the President shall establish a mechanism for coordinating cross-border interoperability issues between—

- (1) the United States and Canada; and
- (2) the United States and Mexico.

(d) Omitted

(e) Multiyear interoperability grants

(1) Multiyear commitments

In awarding grants to any State, region, local government, or Indian tribe for the purposes of enhancing interoperable communications capabilities for emergency response providers, the Secretary may commit to obligate Federal assistance beyond the current fiscal year, subject to the limitations and restrictions in this subsection.

(2) Restrictions

(A) Time limit

No multiyear interoperability commitment may exceed 3 years in duration.

(B) Amount of committed funds

The total amount of assistance the Secretary has committed to obligate for any future fiscal year under paragraph (1) may not exceed \$150,000,000.

(3) Letters of intent

(A) Issuance

Pursuant to paragraph (1), the Secretary may issue a letter of intent to an applicant committing to obligate from future budget authority an amount, not more than the Federal Government's share of the project's cost, for an interoperability communications project (including interest costs and costs of formulating the project).

(B) Schedule

A letter of intent under this paragraph shall establish a schedule under which the Secretary will reimburse the applicant for the Federal Government's share of the project's costs, as amounts become available, if the applicant, after the Secretary issues the letter, carries out the project before receiving amounts under a grant issued by the Secretary.

(C) Notice to Secretary

An applicant that is issued a letter of intent under this subsection shall notify the

¹ See References in Text note below.

Secretary of the applicant's intent to carry out a project pursuant to the letter before the project begins.

(D) Notice to Congress

The Secretary shall transmit a written notification to the Congress no later than 3 days before the issuance of a letter of intent under this section.

(E) Limitations

A letter of intent issued under this section is not an obligation of the Government under section 1501 of title 31 and is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(F) Statutory construction

Nothing in this subsection shall be construed—

(i) to prohibit the obligation of amounts pursuant to a letter of intent under this subsection in the same fiscal year as the letter of intent is issued; or

(ii) to apply to, or replace, Federal assistance intended for interoperable communications that is not provided pursuant to a commitment under this subsection.

(f) Interoperable communications plans

Any applicant requesting funding assistance from the Secretary for interoperable communications for emergency response providers shall submit an Interoperable Communications Plan to the Secretary for approval. Such a plan shall—

(1) describe the current state of communications interoperability in the applicable jurisdictions among Federal, State, and local emergency response providers and other relevant private resources;

(2) describe the available and planned use of public safety frequency spectrum and resources for interoperable communications within such jurisdictions;

(3) describe how the planned use of spectrum and resources for interoperable communications is compatible with surrounding capabilities and interoperable communications plans of Federal, State, and local governmental entities, military installations, foreign governments, critical infrastructure, and other relevant entities;

(4) include a 5-year plan for the dedication of Federal, State, and local government and private resources to achieve a consistent, secure, and effective interoperable communications system, including planning, system design and engineering, testing and technology development, procurement and installation, training, and operations and maintenance;

(5) describe how such 5-year plan meets or exceeds any applicable standards and grant requirements established by the Secretary;

(6) include information on the governance structure used to develop the plan, including such information about all agencies and organizations that participated in developing the plan and the scope and timeframe of the plan; and

(7) describe the method by which multi-jurisdictional, multidisciplinary input is provided from all regions of the jurisdiction, including any high-threat urban areas located in the jurisdiction, and the process for continuing to incorporate such input.

(g) Definitions

In this section:

(1) Interoperable communications

The term “interoperable communications” means the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, and video with one another on demand, in real time, as necessary.

(2) Emergency response providers

The term “emergency response providers” has the meaning that term has under section 101 of this title.

(h) Omitted

(i) Sense of Congress regarding interoperable communications

(1) Finding

The Congress finds that—

(A) many first responders working in the same jurisdiction or in different jurisdictions cannot effectively and efficiently communicate with one another; and

(B) their inability to do so threatens the public's safety and may result in unnecessary loss of lives and property.

(2) Sense of Congress

It is the sense of Congress that interoperable emergency communications systems and radios should continue to be deployed as soon as practicable for use by the first responder community, and that upgraded and new digital communications systems and new digital radios must meet prevailing national, voluntary consensus standards for interoperability.

(Pub. L. 108-458, title VII, § 7303, Dec. 17, 2004, 118 Stat. 3843; Pub. L. 110-53, title III, § 301(c), Aug. 3, 2007, 121 Stat. 299.)

Editorial Notes

REFERENCES IN TEXT

Section 510 of the Homeland Security Act of 2002, as added by subsection (d), referred to in subsec. (a)(2)(B)(ii), means section 510 of Pub. L. 107-296, which was added by Pub. L. 108-458, title VII, § 7303(d), Dec. 17, 2004, 118 Stat. 3844, and was classified to section 321 of this title, prior to repeal by Pub. L. 109-295, title VI, § 611(5), Oct. 4, 2006, 120 Stat. 1395. See Prior Provisions note set out under section 321 of this title.

CODIFICATION

Section is comprised of section 7303 of Pub. L. 108-458. Subsec. (d) of section 7303 of Pub. L. 108-458 enacted section 321 of this title. Subsec. (h) of section 7303 of Pub. L. 108-458 amended sections 238 and 314 of this title.

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as

part of the 9/11 Commission Implementation Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Section 301(c) of Pub. L. 110-53, which directed the amendment of section 7303 of the “Intelligence Reform and Terrorist Prevention Act of 2004”, was executed to this section, which is section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004, to reflect the probable intent of Congress. See 2007 Amendment notes below.

AMENDMENTS

2007—Subsec. (f)(6), (7). Pub. L. 110-53, §301(c)(1), added pars. (6) and (7). See Codification note above.

Subsec. (g)(1). Pub. L. 110-53, §301(c)(2), substituted “and video” for “or video”. See Codification note above.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Pub. L. 108-458, title VII, §7308, Dec. 17, 2004, 118 Stat. 3849, provided that: “Notwithstanding any other provision of this Act [see Tables for classification], this subtitle [subtitle C (§§7301-7308) of title VII of Pub. L. 108-458, enacting this section and section 321 of this title, amending sections 238 and 312 of this title, and enacting provisions set out as notes under this section and section 5196 of Title 42, The Public Health and Welfare] shall take effect on the date of enactment of this Act [Dec. 17, 2004].”

TRANSFER OF FUNCTIONS

For transfer of the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards, to the Assistant Director for Emergency Communications, see section 571(d)(1) of this title.

DEPARTMENT OF HOMELAND SECURITY INTEROPERABLE COMMUNICATIONS

Pub. L. 114-120, title II, §212, Feb. 8, 2016, 130 Stat. 42, provided that:

“(a) IN GENERAL.—If the Secretary of Homeland Security determines that there are at least two communications systems described under paragraph (1)(B) and certified under paragraph (2), the Secretary shall establish and carry out a pilot program across not less than three components of the Department of Homeland Security to assess the effectiveness of a communications system that—

“(1) provides for—

“(A) multiagency collaboration and interoperability; and

“(B) wide-area, secure, and peer-invitation- and acceptance-based multimedia communications;

“(2) is certified by the Department of Defense Joint Interoperability Test Center; and

“(3) is composed of commercially available, off-the-shelf technology.

“(b) ASSESSMENT.—Not later than 6 months after the date on which the pilot program is completed, the Secretary shall submit to the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation and the Committee [on] Homeland Security and Governmental Affairs of the Senate an assessment of the pilot program, including the impacts of the program with respect to interagency and Coast Guard response capabilities.

“(c) STRATEGY.—The pilot program shall be consistent with the strategy required by the Department of Homeland Security Interoperable Communications Act (Public Law 114-29) [set out below].

“(d) TIMING.—The pilot program shall commence within 90 days after the date of the enactment of this Act [Feb. 8, 2016] or within 60 days after the completion of the strategy required by the Department of Home-

land Security Interoperable Communications Act (Public Law 114-29), whichever is later.”

Pub. L. 114-29, July 6, 2015, 129 Stat. 421, provided that:

“SECTION 1. SHORT TITLE.

“This Act may be cited as the ‘Department of Homeland Security Interoperable Communications Act’ or the ‘DHS Interoperable Communications Act’.

“SEC. 2. DEFINITIONS.

“In this Act—

“(1) the term ‘Department’ means the Department of Homeland Security;

“(2) the term ‘interoperable communications’ has the meaning given that term in section 701(d) [now 701(e)] of the Homeland Security Act of 2002 [6 U.S.C. 341(e)], as added by section 3; and

“(3) the term ‘Under Secretary for Management’ means the Under Secretary for Management of the Department of Homeland Security.

“SEC. 3. INCLUSION OF INTEROPERABLE COMMUNICATIONS CAPABILITIES IN RESPONSIBILITIES OF UNDER SECRETARY FOR MANAGEMENT.

[Amended section 341 of this title.]

“SEC. 4. STRATEGY.

“(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act [July 6, 2015], the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a strategy, which shall be updated as necessary, for achieving and maintaining interoperable communications among the components of the Department, including for daily operations, planned events, and emergencies, with corresponding milestones, that includes the following:

“(1) An assessment of interoperability gaps in radio communications among the components of the Department, as of the date of enactment of this Act.

“(2) Information on efforts and activities, including current and planned policies, directives, and training, of the Department since November 1, 2012, to achieve and maintain interoperable communications among the components of the Department, and planned efforts and activities of the Department to achieve and maintain such interoperable communications.

“(3) An assessment of obstacles and challenges to achieving and maintaining interoperable communications among the components of the Department.

“(4) Information on, and an assessment of, the adequacy of mechanisms available to the Under Secretary for Management to enforce and compel compliance with interoperable communications policies and directives of the Department.

“(5) Guidance provided to the components of the Department to implement interoperable communications policies and directives of the Department.

“(6) The total amount of funds expended by the Department since November 1, 2012, and projected future expenditures, to achieve interoperable communications, including on equipment, infrastructure, and maintenance.

“(7) Dates upon which Department-wide interoperability is projected to be achieved for voice, data, and video communications, respectively, and interim milestones that correspond to the achievement of each such mode of communication.

“(b) SUPPLEMENTARY MATERIAL.—Together with the strategy required under subsection (a), the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on—

“(1) any intra-agency effort or task force that has been delegated certain responsibilities by the Under Secretary for Management relating to achieving and maintaining interoperable communications among

the components of the Department by the dates referred to in subsection (a)(7); and

“(2) who, within each such component, is responsible for implementing policies and directives issued by the Under Secretary for Management to so achieve and maintain such interoperable communications.

“SEC. 5. REPORT.

“Not later than 100 days after the date on which the strategy required under section 4(a) is submitted, and every 2 years thereafter for 6 years, the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the status of efforts to implement the strategy required under section 4(a), including the following:

“(1) Progress on each interim milestone referred to in section 4(a)(7) toward achieving and maintaining interoperable communications among the components of the Department.

“(2) Information on any policies, directives, guidance, and training established by the Under Secretary for Management.

“(3) An assessment of the level of compliance, adoption, and participation among the components of the Department with the policies, directives, guidance, and training established by the Under Secretary for Management to achieve and maintain interoperable communications among the components.

“(4) Information on any additional resources or authorities needed by the Under Secretary for Management.

“SEC. 6. APPLICABILITY.

“Sections 4 and 5 shall only apply with respect to the interoperable communications capabilities within the Department and components of the Department to communicate within the Department.”

CROSS BORDER INTEROPERABILITY REPORTS

Pub. L. 110-53, title XXII, §2203, Aug. 3, 2007, 121 Stat. 541, provided that:

“(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Aug. 3, 2007], the Federal Communications Commission, in consultation with the Department of Homeland Security’s Office of Emergency Communications [now Emergency Communications Division], the Office of Management of [sic] Budget, and the Department of State shall report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce on—

“(1) the status of the mechanism established by the President under section 7303(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(c)) for coordinating cross border interoperability issues between—

“(A) the United States and Canada; and

“(B) the United States and Mexico;

“(2) the status of treaty negotiations with Canada and Mexico regarding the coordination of the rebanding of 800 megahertz radios, as required under the final rule of the Federal Communication Commission in the ‘Private Land Mobile Services; 800 MHz Public Safety Interface Proceeding’ (WT Docket No. 02-55; ET Docket No. 00-258; ET Docket No. 95-18, RM-9498; RM-10024; FCC 04-168) including the status of any outstanding issues in the negotiations between—

“(A) the United States and Canada; and

“(B) the United States and Mexico;

“(3) communications between the Commission and the Department of State over possible amendments to the bilateral legal agreements and protocols that govern the coordination process for license applications seeking to use channels and frequencies above Line A;

“(4) the annual rejection rate for the last 5 years by the United States of applications for new channels

and frequencies by Canadian private and public entities; and

“(5) any additional procedures and mechanisms that can be taken by the Commission to decrease the rejection rate for applications by United States private and public entities seeking licenses to use channels and frequencies above Line A.

“(b) UPDATED REPORTS TO BE FILED ON THE STATUS OF TREATY OF [sic] NEGOTIATIONS.—The Federal Communications Commission, in conjunction with the Department of Homeland Security, the Office of Management of Budget, and the Department of State shall continually provide updated reports to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives on the status of treaty negotiations under subsection (a)(2) until the appropriate United States treaty has been revised with each of—

“(1) Canada; and

“(2) Mexico.

“(c) INTERNATIONAL NEGOTIATIONS TO REMEDY SITUATION.—Not later than 90 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of the Department of State shall report to Congress on—

“(1) the current process for considering applications by Canada for frequencies and channels by United States communities above Line A;

“(2) the status of current negotiations to reform and revise such process;

“(3) the estimated date of conclusion for such negotiations;

“(4) whether the current process allows for automatic denials or dismissals of initial applications by the Government of Canada, and whether such denials or dismissals are currently occurring; and

“(5) communications between the Department of State and the Federal Communications Commission pursuant to subsection (a)(3).”

SUBMISSION OF REPORTS TO APPROPRIATE CONGRESSIONAL COMMITTEES

Pub. L. 110-53, title XXII, §2205, Aug. 3, 2007, 121 Stat. 543, provided that: “In addition to the committees specifically enumerated to receive reports under this title [enacting provisions set out as note under this section, section 701 of this title, and section 247d-3a of Title 42, The Public Health and Welfare, and amending provisions set out as a note under section 309 of Title 47, Telecommunications], any report transmitted under the provisions of this title shall also be transmitted to the appropriate congressional committees (as defined in section 2(2) of the Homeland Security Act of 2002 (6 U.S.C. 101(2))).”

REGIONAL MODEL STRATEGIC PLAN PILOT PROJECTS

Pub. L. 108-458, title VII, §7304, Dec. 17, 2004, 118 Stat. 3847, directed the Secretary of Homeland Security, not later than 90 days after Dec. 17, 2004, to establish not fewer than 2 pilot projects in high threat urban areas or regions likely to implement a national model strategic plan in order to develop a regional strategic plan to foster interagency communication and coordinate the gathering of all Federal, State, and local first responders in that area, consistent with the national strategic plan developed by the Department of Homeland Security, and to submit to Congress an interim report regarding the progress of the interagency communications pilot projects 6 months after Dec. 17, 2004, and a final report 18 months after Dec. 17, 2004.

§ 195. Office for Interoperability and Compatibility

(a) Clarification of responsibilities

The Director of the Office for Interoperability and Compatibility shall—

(1) assist the Secretary in developing and implementing the science and technology aspects of the program described in subpara-

graphs (D), (E), (F), and (G) of section 194(a)(1) of this title;

(2) in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies with responsibility for standards, support the creation of national voluntary consensus standards for interoperable emergency communications;

(3) establish a comprehensive research, development, testing, and evaluation program for improving interoperable emergency communications;

(4) establish, in coordination with the Director for Emergency Communications,¹ requirements for interoperable emergency communications capabilities, which shall be non-proprietary where standards for such capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance administered by the Department, excluding any alert and warning device, technology, or system;

(5) carry out the Department's responsibilities and authorities relating to research, development, testing, evaluation, or standards-related elements of the SAFECOM Program;

(6) evaluate and assess new technology in real-world environments to achieve interoperable emergency communications capabilities;

(7) encourage more efficient use of existing resources, including equipment, to achieve interoperable emergency communications capabilities;

(8) test public safety communications systems that are less prone to failure, support new nonvoice services, use spectrum more efficiently, and cost less than existing systems;

(9) coordinate with the private sector to develop solutions to improve emergency communications capabilities and achieve interoperable emergency communications capabilities; and

(10) conduct pilot projects, in coordination with the Director for Emergency Communications,¹ to test and demonstrate technologies, including data and video, that enhance—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications capabilities.

(b) Coordination

The Director of the Office for Interoperability and Compatibility shall coordinate with the Director for Emergency Communications¹ with respect to the SAFECOM program.

(c) Sufficiency of resources

The Secretary shall provide the Office for Interoperability and Compatibility the resources and staff necessary to carry out the responsibilities under this section.

(Pub. L. 107-296, title III, §314, as added Pub. L. 109-295, title VI, §672(a), Oct. 4, 2006, 120 Stat. 1441.)

¹ See Change of Name note below.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Reference to Director for Emergency Communications deemed to be a reference to Assistant Director for Emergency Communications, see section 2(c)(2) of Pub. L. 115-278, set out as a note under section 571 of this title.

§ 195a. Emergency communications interoperability research and development

(a) In general

The Under Secretary for Science and Technology, acting through the Director of the Office for Interoperability and Compatibility, shall establish a comprehensive research and development program to support and promote—

(1) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) interoperable emergency communications capabilities among emergency response providers and relevant government officials, including by—

(A) supporting research on a competitive basis, including through the Directorate of Science and Technology and Homeland Security Advanced Research Projects Agency; and

(B) considering the establishment of a Center of Excellence under the Department of Homeland Security Centers of Excellence Program focused on improving emergency response providers' communication capabilities.

(b) Purposes

The purposes of the program established under subsection (a) include—

(1) supporting research, development, testing, and evaluation on emergency communication capabilities;

(2) understanding the strengths and weaknesses of the public safety communications systems in use;

(3) examining how current and emerging technology can make emergency response providers more effective, and how Federal, State, local, and tribal government agencies can use this technology in a coherent and cost-effective manner;

(4) investigating technologies that could lead to long-term advancements in emergency communications capabilities and supporting research on advanced technologies and potential systemic changes to dramatically improve emergency communications; and

(5) evaluating and validating advanced technology concepts, and facilitating the development and deployment of interoperable emergency communication capabilities.

(c) Definitions

For purposes of this section, the term “interoperable”, with respect to emergency communications, has the meaning given the term in section 578 of this title.

(Pub. L. 107-296, title III, §315, as added Pub. L. 109-295, title VI, §673(a), Oct. 4, 2006, 120 Stat. 1443.)

§ 195b. National Biosurveillance Integration Center

(a) Establishment

The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall establish, operate, and maintain a National Biosurveillance Integration Center (referred to in this section as the “NBIC”), which shall be headed by a Directing Officer, under an office or directorate of the Department that is in existence as of August 3, 2007.

(b) Primary mission

The primary mission of the NBIC is to—

(1) enhance the capability of the Federal Government to—

(A) rapidly identify, characterize, localize, and track a biological event of national concern by integrating and analyzing data relating to human health, animal, plant, food, and environmental monitoring systems (both national and international); and

(B) disseminate alerts and other information to Member Agencies and, in coordination with (and where possible through) Member Agencies, to agencies of State, local, and tribal governments, as appropriate, to enhance the ability of such agencies to respond to a biological event of national concern; and

(2) oversee development and operation of the National Biosurveillance Integration System.

(c) Requirements

The NBIC shall detect, as early as possible, a biological event of national concern that presents a risk to the United States or the infrastructure or key assets of the United States, including by—

(1) consolidating data from all relevant surveillance systems maintained by Member Agencies to detect biological events of national concern across human, animal, and plant species;

(2) seeking private sources of surveillance, both foreign and domestic, when such sources would enhance coverage of critical surveillance gaps;

(3) using an information technology system that uses the best available statistical and other analytical tools to identify and characterize biological events of national concern in as close to real-time as is practicable;

(4) providing the infrastructure for such integration, including information technology systems and space, and support for personnel from Member Agencies with sufficient expertise to enable analysis and interpretation of data;

(5) working with Member Agencies to create information technology systems that use the minimum amount of patient data necessary and consider patient confidentiality and privacy issues at all stages of development and apprise the Privacy Officer of such efforts; and

(6) alerting Member Agencies and, in coordination with (and where possible through) Member Agencies, public health agencies of State, local, and tribal governments regarding

any incident that could develop into a biological event of national concern.

(d) Responsibilities of the Directing Officer of the NBIC

(1) In general

The Directing Officer of the NBIC shall—

(A) on an ongoing basis, monitor the availability and appropriateness of surveillance systems used by the NBIC and those systems that could enhance biological situational awareness or the overall performance of the NBIC;

(B) on an ongoing basis, review and seek to improve the statistical and other analytical methods used by the NBIC;

(C) receive and consider other relevant homeland security information, as appropriate; and

(D) provide technical assistance, as appropriate, to all Federal, regional, State, local, and tribal government entities and private sector entities that contribute data relevant to the operation of the NBIC.

(2) Assessments

The Directing Officer of the NBIC shall—

(A) on an ongoing basis, evaluate available data for evidence of a biological event of national concern; and

(B) integrate homeland security information with NBIC data to provide overall situational awareness and determine whether a biological event of national concern has occurred.

(3) Information sharing

(A) In general

The Directing Officer of the NBIC shall—

(i) establish a method of real-time communication with the National Operations Center;

(ii) in the event that a biological event of national concern is detected, notify the Secretary and disseminate results of NBIC assessments relating to that biological event of national concern to appropriate Federal response entities and, in coordination with relevant Member Agencies, regional, State, local, and tribal governmental response entities in a timely manner;

(iii) provide any report on NBIC assessments to Member Agencies and, in coordination with relevant Member Agencies, any affected regional, State, local, or tribal government, and any private sector entity considered appropriate that may enhance the mission of such Member Agencies, governments, or entities or the ability of the Nation to respond to biological events of national concern; and

(iv) share NBIC incident or situational awareness reports, and other relevant information, consistent with the information sharing environment established under section 485 of this title and any policies, guidelines, procedures, instructions, or standards established under that section.

(B) Consultation

The Directing Officer of the NBIC shall implement the activities described in subpara-

graph (A) consistent with the policies, guidelines, procedures, instructions, or standards established under section 485 of this title and in consultation with the Director of National Intelligence, the Under Secretary for Intelligence and Analysis, and other offices or agencies of the Federal Government, as appropriate.

(e) Responsibilities of the NBIC member agencies

(1)¹ In general

Each Member Agency shall—

(A) use its best efforts to integrate biosurveillance information into the NBIC, with the goal of promoting information sharing between Federal, State, local, and tribal governments to detect biological events of national concern;

(B) provide timely information to assist the NBIC in maintaining biological situational awareness for accurate detection and response purposes;

(C) enable the NBIC to receive and use biosurveillance information from member agencies to carry out its requirements under subsection (c);

(D) connect the biosurveillance data systems of that Member Agency to the NBIC data system under mutually agreed protocols that are consistent with subsection (c)(5);

(E) participate in the formation of strategy and policy for the operation of the NBIC and its information sharing;

(F) provide personnel to the NBIC under an interagency personnel agreement and consider the qualifications of such personnel necessary to provide human, animal, and environmental data analysis and interpretation support to the NBIC; and

(G) retain responsibility for the surveillance and intelligence systems of that department or agency, if applicable.

(f) Administrative authorities

(1) Hiring of experts

The Directing Officer of the NBIC shall hire individuals with the necessary expertise to develop and operate the NBIC.

(2) Detail of personnel

Upon the request of the Directing Officer of the NBIC, the head of any Federal department or agency may detail, on a reimbursable basis, any of the personnel of that department or agency to the Department to assist the NBIC in carrying out this section.

(g) NBIC interagency working group

The Directing Officer of the NBIC shall—

(1) establish an interagency working group to facilitate interagency cooperation and to advise the Directing Officer of the NBIC regarding recommendations to enhance the biosurveillance capabilities of the Department; and

(2) invite Member Agencies to serve on that working group.

¹ So in original. No par. (2) has been enacted.

(h) Relationship to other departments and agencies

The authority of the Directing Officer of the NBIC under this section shall not affect any authority or responsibility of any other department or agency of the Federal Government with respect to biosurveillance activities under any program administered by that department or agency.

(i) Authorization of appropriations

There are authorized to be appropriated such sums as are necessary to carry out this section.

(j) Definitions

In this section:

(1) The terms “biological agent” and “toxin” have the meanings given those terms in section 178 of title 18.

(2) The term “biological event of national concern” means—

(A) an act of terrorism involving a biological agent or toxin; or

(B) a naturally occurring outbreak of an infectious disease that may result in a national epidemic.

(3) The term “homeland security information” has the meaning given that term in section 482 of this title.

(4) The term “Member Agency” means any Federal department or agency that, at the discretion of the head of that department or agency, has entered a memorandum of understanding regarding participation in the NBIC.

(5) The term “Privacy Officer” means the Privacy Officer appointed under section 142 of this title.

(Pub. L. 107–296, title III, § 316, as added Pub. L. 110–53, title XI, § 1101(a), Aug. 3, 2007, 121 Stat. 375; amended Pub. L. 115–387, § 2(f)(2), Dec. 21, 2018, 132 Stat. 5168.)

Editorial Notes

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–387 substituted “Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall” for “Secretary shall”.

Statutory Notes and Related Subsidiaries

DEADLINE FOR IMPLEMENTATION

Pub. L. 110–53, title XI, § 1101(c), Aug. 3, 2007, 121 Stat. 378, provided that: “The National Biosurveillance Integration Center under section 316 of the Homeland Security Act [of 2002, 6 U.S.C. 195b], as added by subsection (a), shall be fully operational by not later than September 30, 2008.”

§ 195c. Promoting antiterrorism through international cooperation program

(a) Definitions

In this section:

(1) Director

The term “Director” means the Director selected under subsection (b)(2).

(2) International cooperative activity

The term “international cooperative activity” includes—

(A) coordinated research projects, joint research projects, or joint ventures;

(B) joint studies or technical demonstrations;

(C) coordinated field exercises, scientific seminars, conferences, symposia, and workshops;

(D) training of scientists and engineers;

(E) visits and exchanges of scientists, engineers, or other appropriate personnel;

(F) exchanges or sharing of scientific and technological information; and

(G) joint use of laboratory facilities and equipment.

(b) Science and Technology Homeland Security International Cooperative Programs Office

(1) Establishment

The Under Secretary shall establish the Science and Technology Homeland Security International Cooperative Programs Office.

(2) Director

The Office shall be headed by a Director, who—

(A) shall be selected, in consultation with the Assistant Secretary for International Affairs, by and shall report to the Under Secretary; and

(B) may be an officer of the Department serving in another position.

(3) Responsibilities

(A) Development of mechanisms

The Director shall be responsible for developing, in coordination with the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other Federal agencies, understandings and agreements to allow and to support international cooperative activity in support of homeland security.

(B) Priorities

The Director shall be responsible for developing, in coordination with the Office of International Affairs and other Federal agencies, strategic priorities for international cooperative activity for the Department in support of homeland security.

(C) Activities

The Director shall facilitate the planning, development, and implementation of international cooperative activity to address the strategic priorities developed under subparagraph (B) through mechanisms the Under Secretary considers appropriate, including grants, cooperative agreements, or contracts to or with foreign public or private entities, governmental organizations, businesses (including small businesses and socially and economically disadvantaged small businesses (as those terms are defined in sections 632 and 637 of title 15, respectively)), federally funded research and development centers, and universities.

(D) Identification of partners

The Director shall facilitate the matching of United States entities engaged in homeland security research with non-United

States entities engaged in homeland security research so that they may partner in homeland security research activities.

(4) Coordination

The Director shall ensure that the activities under this subsection are coordinated with the Office of International Affairs and the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other relevant Federal agencies or interagency bodies. The Director may enter into joint activities with other Federal agencies.

(c) Matching funding

(1) In general

(A) Equitability

The Director shall ensure that funding and resources expended in international cooperative activity will be equitably matched by the foreign partner government or other entity through direct funding, funding of complementary activities, or the provision of staff, facilities, material, or equipment.

(B) Grant matching and repayment

(i) In general

The Secretary may require a recipient of a grant under this section—

(I) to make a matching contribution of not more than 50 percent of the total cost of the proposed project for which the grant is awarded; and

(II) to repay to the Secretary the amount of the grant (or a portion thereof), interest on such amount at an appropriate rate, and such charges for administration of the grant as the Secretary determines appropriate.

(ii) Maximum amount

The Secretary may not require that repayment under clause (i)(II) be more than 150 percent of the amount of the grant, adjusted for inflation on the basis of the Consumer Price Index.

(2) Foreign partners

Partners may include Israel, the United Kingdom, Canada, Australia, Singapore, and other allies in the global war on terrorism as determined to be appropriate by the Secretary of Homeland Security and the Secretary of State.

(3) Loans of equipment

The Director may make or accept loans of equipment for research and development and comparative testing purposes.

(d) Foreign reimbursements

If the Science and Technology Homeland Security International Cooperative Programs Office participates in an international cooperative activity with a foreign partner on a cost-sharing basis, any reimbursements or contributions received from that foreign partner to meet its share of the project may be credited to appropriate current appropriations accounts of the Directorate of Science and Technology.

(e) Report to Congress on international cooperative activities

Not later than one year after August 3, 2007, and every 5 years thereafter, the Under Sec-

retary, acting through the Director, shall submit to Congress a report containing—

(1) a brief description of each grant, cooperative agreement, or contract made or entered into under subsection (b)(3)(C), including the participants, goals, and amount and sources of funding;

(2) a list of international cooperative activities underway, including the participants, goals, expected duration, and amount and sources of funding, including resources provided to support the activities in lieu of direct funding; and¹

(3) for international cooperative activities identified in the previous reporting period, a status update on the progress of such activities, including whether goals were realized, explaining any lessons learned, and evaluating overall success; and

(4) a discussion of obstacles encountered in the course of forming, executing, or implementing agreements for international cooperative activities, including administrative, legal, or diplomatic challenges or resource constraints.

(f) Animal and zoonotic diseases

As part of the international cooperative activities authorized in this section, the Under Secretary, in coordination with the Assistant Secretary for the Countering Weapons of Mass Destruction Office, the Department of State, and appropriate officials of the Department of Agriculture, the Department of Defense, and the Department of Health and Human Services, may enter into cooperative activities with foreign countries, including African nations, to strengthen American preparedness against foreign animal and zoonotic diseases overseas that could harm the Nation's agricultural and public health sectors if they were to reach the United States.

(g) Cybersecurity

As part of the international cooperative activities authorized in this section, the Under Secretary, in coordination with the Department of State and appropriate Federal officials, may enter into cooperative research activities with Israel to strengthen preparedness against cyber threats and enhance capabilities in cybersecurity.

(h) Construction; authorities of the Secretary of State

Nothing in this section shall be construed to alter or affect the following provisions of law:

(1) Title V of the Foreign Relations Authorization Act, Fiscal Year 1979 (22 U.S.C. 2656a et seq.).

(2) Section 112b(c) of title 1.

(3) Section 2651a(e)(2) of title 22.

(4) Sections 2752 and 2767 of title 22.

(5) Section 2382(c) of title 22.

(i) Authorization of appropriations

There are authorized to be appropriated to carry out this section such sums as are necessary.

(Pub. L. 107-296, title III, §317, as added Pub. L. 110-53, title XIX, §1901(b)(1), Aug. 3, 2007, 121

Stat. 505; amended Pub. L. 114-304, §2(a), Dec. 16, 2016, 130 Stat. 1519; Pub. L. 115-387, §2(f)(3), Dec. 21, 2018, 132 Stat. 5168; Pub. L. 117-263, div. E, title LIX, §5947(a)(3), Dec. 23, 2022, 136 Stat. 3481.)

AMENDMENT OF SUBSECTION (h)(2)

Pub. L. 117-263, div. E, title LIX, §5947(a)(3), (c), Dec. 23, 2022, 136 Stat. 3481, 3482, provided that, effective 270 days after Dec. 23, 2022, subsection (h)(2) of this section is amended by striking “Section 112b(c)” and inserting “Section 112b(g)”. See 2022 Amendment note below.

Editorial Notes

REFERENCES IN TEXT

The Foreign Relations Authorization Act, Fiscal Year 1979, referred to in subsec. (h)(1), is Pub. L. 95-426, Oct. 7, 1978, 92 Stat. 963. Title V of the Act is classified generally to sections 2656a to 2656d of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2022—Subsec. (h)(2). Pub. L. 117-263 substituted “Section 112b(g)” for “Section 112b(c)”.

2018—Subsec. (f). Pub. L. 115-387 substituted “the Assistant Secretary for the Countering Weapons of Mass Destruction Office,” for “the Chief Medical Officer.”

2016—Subsec. (e)(3), (4). Pub. L. 114-304, §2(a)(1), added pars. (3) and (4).

Subsecs. (g) to (i). Pub. L. 114-304, §2(a)(2), (3), added subsec. (g) and redesignated former subsecs. (g) and (h) as (h) and (i), respectively.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2022 AMENDMENT

Amendment by Pub. L. 117-263 effective 270 days after Dec. 23, 2022, see section 5947(c) of Pub. L. 117-263, set out as a note under section 112a of Title 1, General Provisions.

FINDINGS

Pub. L. 110-53, title XIX, §1901(a), Aug. 3, 2007, 121 Stat. 505, provided that: “Congress finds the following:

“(1) The development and implementation of technology is critical to combating terrorism and other high consequence events and implementing a comprehensive homeland security strategy.

“(2) The United States and its allies in the global war on terrorism share a common interest in facilitating research, development, testing, and evaluation of equipment, capabilities, technologies, and services that will aid in detecting, preventing, responding to, recovering from, and mitigating against acts of terrorism.

“(3) Certain United States allies in the global war on terrorism, including Israel, the United Kingdom, Canada, Australia, and Singapore have extensive experience with, and technological expertise in, homeland security.

“(4) The United States and certain of its allies in the global war on terrorism have a history of successful collaboration in developing mutually beneficial equipment, capabilities, technologies, and services in the areas of defense, agriculture, and telecommunications.

“(5) The United States and its allies in the global war on terrorism will mutually benefit from the sharing of technological expertise to combat domestic and international terrorism.

“(6) The establishment of an office to facilitate and support cooperative endeavors between and among government agencies, for-profit business entities, academic institutions, and nonprofit entities of the

¹ So in original. The word “and” probably should not appear.

United States and its allies will safeguard lives and property worldwide against acts of terrorism and other high consequence events.”

TRANSPARENCY OF FUNDS

Pub. L. 110-53, title XIX, §1902, Aug. 3, 2007, 121 Stat. 508, provided that: “For each Federal award (as that term is defined in section 2 of the Federal Funding Accountability and Transparency Act of 2006 [Pub. L. 109-282] (31 U.S.C. 6101 note)) under this title [enacting this section and provisions set out as notes under this section] or an amendment made by this title, the Director of the Office of Management and Budget shall ensure full and timely compliance with the requirements of the Federal Funding Accountability and Transparency Act of 2006 (31 U.S.C. 6101 note).”

§ 195d. Social media working group

(a) Establishment

The Secretary shall establish within the Department a social media working group (in this section referred to as the “Group”).

(b) Purpose

In order to enhance the dissemination of information through social media technologies between the Department and appropriate stakeholders and to improve use of social media technologies in support of preparedness, response, and recovery, the Group shall identify, and provide guidance and best practices to the emergency preparedness and response community on, the use of social media technologies before, during, and after a natural disaster or an act of terrorism or other man-made disaster.

(c) Membership

(1) In general

Membership of the Group shall be composed of a cross section of subject matter experts from Federal, State, local, tribal, territorial, and nongovernmental organization practitioners, including representatives from the following entities:

- (A) The Office of Public Affairs of the Department.
- (B) The Office of the Chief Information Officer of the Department.
- (C) The Privacy Office of the Department.
- (D) The Federal Emergency Management Agency.
- (E) The Office of Disability Integration and Coordination of the Federal Emergency Management Agency.
- (F) The American Red Cross.
- (G) The Forest Service.
- (H) The Centers for Disease Control and Prevention.
- (I) The United States Geological Survey.
- (J) The National Oceanic and Atmospheric Administration.

(2) Chairperson; co-chairperson

(A) Chairperson

The Secretary, or a designee of the Secretary, shall serve as the chairperson of the Group.

(B) Co-chairperson

The chairperson shall designate, on a rotating basis, a representative from a State or local government who is a member of the Group to serve as the co-chairperson of the Group.

(3) Additional members

The chairperson shall appoint, on a rotating basis, qualified individuals to the Group. The total number of such additional members shall—

- (A) be equal to or greater than the total number of regular members under paragraph (1); and
- (B) include—
 - (i) not fewer than 3 representatives from the private sector; and
 - (ii) representatives from—
 - (I) State, local, tribal, and territorial entities, including from—
 - (aa) law enforcement;
 - (bb) fire services;
 - (cc) emergency management; and
 - (dd) public health entities;
 - (II) universities and academia; and
 - (III) nonprofit disaster relief organizations.

(4) Term limits

The chairperson shall establish term limits for individuals appointed to the Group under paragraph (3).

(d) Consultation with non-members

To the extent practicable, the Group shall work with entities in the public and private sectors to carry out subsection (b).

(e) Meetings

(1) Initial meeting

Not later than 90 days after November 5, 2015, the Group shall hold its initial meeting.

(2) Subsequent meetings

After the initial meeting under paragraph (1), the Group shall meet—

- (A) at the call of the chairperson; and
- (B) not less frequently than twice each year.

(3) Virtual meetings

Each meeting of the Group may be held virtually.

(f) Reports

During each year in which the Group meets, the Group shall submit to the appropriate congressional committees a report that includes the following:

- (1) A review and analysis of current and emerging social media technologies being used to support preparedness and response activities related to natural disasters and acts of terrorism and other man-made disasters.
- (2) A review of best practices and lessons learned on the use of social media technologies during the response to natural disasters and acts of terrorism and other man-made disasters that occurred during the period covered by the report at issue.
- (3) Recommendations to improve the Department’s use of social media technologies for emergency management purposes.
- (4) Recommendations to improve public awareness of the type of information disseminated through social media technologies, and how to access such information, during a natural disaster or an act of terrorism or other man-made disaster.

(5) A review of available training for Federal, State, local, tribal, and territorial officials on the use of social media technologies in response to a natural disaster or an act of terrorism or other man-made disaster.

(6) A review of coordination efforts with the private sector to discuss and resolve legal, operational, technical, privacy, and security concerns.

(g) Duration of group

(1) In general

The Group shall terminate on the date that is 5 years after November 5, 2015, unless the chairperson renews the Group for a successive 5-year period, prior to the date on which the Group would otherwise terminate, by submitting to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a certification that the continued existence of the Group is necessary to fulfill the purpose described in subsection (b).

(2) Continued renewal

The chairperson may continue to renew the Group for successive 5-year periods by submitting a certification in accordance with paragraph (1) prior to the date on which the Group would otherwise terminate.

(Pub. L. 107–296, title III, §318, as added Pub. L. 114–80, §2(a), Nov. 5, 2015, 129 Stat. 646.)

§ 195e. Transparency in research and development

(a) Requirement to list research and development programs

(1) In general

The Secretary shall maintain a detailed list of the following:

(A) Each classified and unclassified research and development project, and all appropriate details for each such project, including the component of the Department responsible for each such project.

(B) Each task order for a Federally Funded Research and Development Center not associated with a research and development project.

(C) Each task order for a University-based center of excellence not associated with a research and development project.

(D) The indicators developed and tracked by the Under Secretary for Science and Technology with respect to transitioned projects pursuant to subsection (c).

(2) Exception for certain completed projects

Paragraph (1) shall not apply to a project completed or otherwise terminated before December 23, 2016.

(3) Updates

The list required under paragraph (1) shall be updated as frequently as possible, but not less frequently than once per quarter.

(4) Research and development defined

For purposes of the list required under paragraph (1), the Secretary shall provide a definition for the term “research and development”.

(b) Requirement to report to Congress on all projects

Not later than January 1, 2017, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified and unclassified report, as applicable, that lists each ongoing classified and unclassified project at the Department, including all appropriate details of each such project.

(c) Indicators of success of transitioned projects

(1) In general

For each project that has been transitioned to practice from research and development, the Under Secretary for Science and Technology shall develop and track indicators to demonstrate the uptake of the technology or project among customers or end-users.

(2) Requirement

To the fullest extent possible, the tracking of a project required under paragraph (1) shall continue for the three-year period beginning on the date on which such project was transitioned to practice from research and development.

(d) Definitions

In this section:

(1) All appropriate details

The term “all appropriate details” means, with respect to a research and development project—

(A) the name of such project, including both classified and unclassified names if applicable;

(B) the name of the component of the Department carrying out such project;

(C) an abstract or summary of such project;

(D) funding levels for such project;

(E) project duration or timeline;

(F) the name of each contractor, grantee, or cooperative agreement partner involved in such project;

(G) expected objectives and milestones for such project; and

(H) to the maximum extent practicable, relevant literature and patents that are associated with such project.

(2) Classified

The term “classified” means anything containing—

(A) classified national security information as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order;

(B) Restricted Data or data that was formerly Restricted Data, as defined in section 2014(y) of title 42;

(C) material classified at the Sensitive Compartmented Information (SCI) level, as defined in section 3345 of title 50; or

(D) information relating to a special access program, as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order.

(3) Controlled unclassified information

The term “controlled unclassified information” means information described as “Con-

trolled Unclassified Information” under Executive Order 13556 (50 U.S.C. 3501 note)¹ or any successor order.

(4) Project

The term “project” means a research or development project, program, or activity administered by the Department, whether ongoing, completed, or otherwise terminated.

(e) Limitation

Nothing in this section overrides or otherwise affects the requirements specified in section 468 of this title.

(Pub. L. 107–296, title III, §319, as added Pub. L. 114–328, div. A, title XIX, §1906(a), Dec. 23, 2016, 130 Stat. 2676.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13556, referred to in subsec. (d)(3), is set out as a note under section 3501 of Title 44, Public Printing and Documents.

PRIOR PROVISIONS

A prior section 319 of Pub. L. 107–296 was renumbered section 320 and is classified to section 195f of this title.

§ 195f. EMP and GMD mitigation research and development and threat assessment, response, and recovery

(a) In general

In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of threats of EMP and GMD.

(b) Scope

The scope of the research and development under subsection (a) shall include the following:

(1) An objective scientific analysis—

(A) evaluating the risks to critical infrastructure from a range of threats of EMP and GMD; and

(B) which shall—

(i) be conducted in conjunction with the Office of Intelligence and Analysis; and

(ii) include a review and comparison of the range of threats and hazards facing critical infrastructure of the electrical grid.

(2) Determination of the critical utilities and national security assets and infrastructure that are at risk from threats of EMP and GMD.

(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, which shall include a review of the feasibility of rapidly isolating

one or more portions of the electrical grid from the main electrical grid.

(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to threats of EMP and GMD, including an analysis of neutral current blocking devices that may protect high-voltage transmission lines.

(5) The restoration and recovery capabilities of critical infrastructure under differing levels of damage and disruption from various threats of EMP and GMD, as informed by the objective scientific analysis conducted under paragraph (1).

(6) An analysis of the feasibility of a real-time alert system to inform electrical grid operators and other stakeholders within milliseconds of a high-altitude nuclear explosion.

(c) Exemption from disclosure

(1) Information shared with the Federal Government

Section 673 of this title, and any regulations issued pursuant to such section, shall apply to any information shared with the Federal Government under this section.

(2) Information shared by the Federal Government

Information shared by the Federal Government with a State, local, or tribal government under this section shall be exempt from disclosure under any provision of State, local, or tribal freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

(d) Threat assessment, response, and recovery

(1) Roles and responsibilities

(A) Distribution of information

(i) In general

Beginning not later than June 19, 2020, the Secretary shall provide timely distribution of information on EMPs and GMDs to Federal, State, and local governments, owners and operators of critical infrastructure, and other persons determined appropriate by the Secretary.

(ii) Briefing

The Secretary shall brief the appropriate congressional committees on the effectiveness of the distribution of information under clause (i).

(B) Response and recovery

(i) In general

The Administrator of the Federal Emergency Management Agency shall—

(I) coordinate the response to and recovery from the effects of EMPs and GMDs on critical infrastructure, in coordination with the heads of appropriate Sector-Specific Agencies, and on matters related to the bulk power system, in consultation with the Secretary of Energy and the Federal Energy Regulatory Commission; and

(II) to the extent practicable, incorporate events that include EMPs and ex-

¹ See References in Text note below.

treme GMDs as a factor in preparedness scenarios and exercises.

(ii) Implementation

The Administrator of the Federal Emergency Management Agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, and on matters related to the bulk power system, the Secretary of Energy and the Federal Energy Regulatory Commission, shall—

(I) not later than June 19, 2020, develop plans and procedures to coordinate the response to and recovery from EMP and GMD events; and

(II) not later than December 21, 2020, conduct a national exercise to test the preparedness and response of the Nation to the effect of an EMP or extreme GMD event.

(C) Research and development

(i) In general

The Secretary, in coordination with the heads of relevant Sector-Specific Agencies, shall—

(I) without duplication of existing or ongoing efforts, conduct research and development to better understand and more effectively model the effects of EMPs and GMDs on critical infrastructure (which shall not include any system or infrastructure of the Department of Defense or any system or infrastructure of the Department of Energy associated with nuclear weapons activities); and

(II) develop technologies to enhance the resilience of and better protect critical infrastructure.

(ii) Plan

Not later than March 26, 2020, and in coordination with the heads of relevant Sector-Specific Agencies, the Secretary shall submit to the appropriate congressional committees a research and development action plan to rapidly address modeling shortfall and technology development.

(D) Emergency information system

(i) In general

The Administrator of the Federal Emergency Management Agency, in coordination with relevant stakeholders, shall maintain a network of systems, such as the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title, that are capable of providing appropriate emergency information to the public before (if possible), during, and in the aftermath of an EMP or GMD.

(ii) Briefing

Not later than December 21, 2020, the Administrator of the Federal Emergency Management Agency, shall brief the appropriate congressional committees regarding the maintenance of systems, including the alerting capabilities of the integrated public alert and warning system authorized under section 321o of this title.

(E) Quadrennial risk assessments

(i) In general

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce, and informed by intelligence-based threat assessments, shall conduct a quadrennial EMP and GMD risk assessment.

(ii) Briefings

Not later than March 26, 2020, and every four years thereafter until 2032, the Secretary, the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce shall provide a briefing to the appropriate congressional committees regarding the quadrennial EMP and GMD risk assessment.

(iii) Enhancing resilience

The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other relevant Sector-Specific Agencies, shall use the results of the quadrennial EMP and GMD risk assessments to better understand and to improve resilience to the effects of EMPs and GMDs across all critical infrastructure sectors, including coordinating the prioritization of critical infrastructure at greatest risk to the effects of EMPs and GMDs.

(2) Coordination

(A) Report on technological options

Not later than December 21, 2020, and every four years thereafter until 2032, the Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the heads of other appropriate agencies, and, as appropriate, private-sector partners, shall submit to the appropriate congressional committees, a report that—

(i) assesses the technological options available to improve the resilience of critical infrastructure to the effects of EMPs and GMDs; and

(ii) identifies gaps in available technologies and opportunities for technological developments to inform research and development activities.

(B) Test data

(i) In general

Not later than December 20, 2020, the Secretary, in coordination with the heads of Sector-Specific Agencies, the Secretary of Defense, and the Secretary of Energy, shall—

(I) review test data regarding the effects of EMPs and GMDs on critical infrastructure systems, networks, and assets representative of those throughout the Nation; and

(II) identify any gaps in the test data.

(ii) Plan

Not later than 180 days after identifying gaps in test data under clause (i), the Secretary, in coordination with the heads of Sector-Specific Agencies and in consulta-

tion with the Secretary of Defense and the Secretary of Energy, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps.

(iii) Implementation

The heads of each agency identified in the plan developed under clause (ii) shall implement the plan in collaboration with the voluntary efforts of the private sector, as appropriate.

(3) Definitions

In this subsection:

(A) The term “appropriate congressional committees” means—

(i) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Energy and Natural Resources, and the Committee on Commerce, Science, and Transportation of the Senate; and

(ii) the Committee on Transportation and Infrastructure, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Science, Space and Technology of the House of Representatives.

(B) The terms “prepare” and “preparedness” mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the homeland, including the prediction and notification of impending EMPs and GMDs.

(C) The term “Sector Risk Management Agency” has the meaning given that term in section 650 of this title.

(e) Rule of construction

Nothing in this section may be construed—¹

(1) to affect in any manner the authority of the executive branch to implement Executive Order 13865, dated March 26, 2019, and entitled “Coordinating National Resilience to Electromagnetic Pulses”, or any other authority existing on the day before December 20, 2019, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America’s Surface Transportation Act (6 U.S.C. 121 note), including the authority under section 824o of title 16, and including the authority of independent agencies to be independent; or

(2) as diminishing or transferring any authorities vested in the Administrator of the Federal Emergency Management Agency or in the Agency prior to December 20, 2019.

(Pub. L. 107–296, title III, § 320, formerly § 319, as added Pub. L. 114–328, div. A, title XIX, § 1913(a)(3), Dec. 23, 2016, 130 Stat. 2685; renu-

bered § 320 and amended Pub. L. 115–278, § 2(g)(3)(B), (C), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 116–92, div. A, title XVII, § 1740(a)(1), Dec. 20, 2019, 133 Stat. 1821; Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(A), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(A), Dec. 23, 2022, 136 Stat. 3659.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13865, referred to in subsec. (e)(1), is Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, which is set out as a note under this section.

Section 61003(c) of division F of the Fixing America’s Surface Transportation Act, referred to in subsec. (e)(1), is section 61003(c) of Pub. L. 114–94, div. F, Dec. 4, 2015, 129 Stat. 1778, which is set out as a note under section 121 of this title.

AMENDMENTS

2022—Subsec. (d)(3)(C). Pub. L. 117–263 substituted “section 650 of this title” for “section 651 of this title”.

2021—Subsec. (d)(3)(C). Pub. L. 116–283, § 9002(c)(2)(A)(i), substituted “Sector Risk Management Agency” for “Sector-Specific Agency”.

Subsec. (e)(1). Pub. L. 116–283, § 9002(c)(2)(A)(ii), substituted “Sector Risk Management Agency” for “Sector-Specific Agency”.

2019—Pub. L. 116–92, § 1740(a)(1)(A), inserted “and threat assessment, response, and recovery” after “development” in section catchline.

Subsecs. (d), (e). Pub. L. 116–92, § 1740(a)(1)(B), added subsecs. (d) and (e).

2018—Subsec. (c)(1). Pub. L. 115–278, § 2(g)(3)(C), substituted “Section 673 of this title” for “Section 133 of this title”.

Statutory Notes and Related Subsidiaries

BENCHMARKS; DEFINITIONS

Pub. L. 116–92, div. A, title XVII, § 1740(d), (h), Dec. 20, 2019, 133 Stat. 1824, 1825, provided that:

“(d) BENCHMARKS.—Not later than March 26, 2020, and as appropriate thereafter, the Secretary of Energy, in consultation with the Secretary of Defense, the Secretary of Homeland Security, and, as appropriate, the private sector, may develop or update, as necessary, quantitative and voluntary benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure. Nothing in this subsection shall affect the authority of the Electric Reliability Organization to develop and enforce, or the authority of the Federal Energy Regulatory Commission to approve, reliability standards.

“(h) DEFINITIONS.—In this section [amending this section and section 347 of this title and enacting this note and provisions not set out in the Code]:

“(1) The term ‘appropriate congressional committees’ has the meaning given that term in subsection (d) of section 320 of the Homeland Security Act of 2002 [6 U.S.C. 195f(d)], as added by subsection (a) of this section; and

“(2) The terms ‘critical infrastructure’, ‘EMP’, and ‘GMD’ have the meanings given such terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).”

Executive Documents

EX. ORD. NO. 13865. COORDINATING NATIONAL RESILIENCE TO ELECTROMAGNETIC PULSES

Ex. Ord. No. 13865, Mar. 26, 2019, 84 F.R. 12041, 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:

¹ So in original. Probably should be “construed—”.

SECTION 1. *Purpose.* An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs.

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

(a) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) "Electromagnetic pulse" is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth. A geomagnetic disturbance (GMD) is a type of natural EMP driven by a temporary disturbance of Earth's magnetic field resulting from interactions with solar eruptions. Both HEMPs and GMDs can affect large geographic areas.

(c) "National Critical Functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(d) "National Essential Functions" means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as an EMP that adversely affects the performance of Government.

(e) "Prepare" and "preparedness" mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. These terms include the prediction and notification of impending EMPs.

(f) A "Sector-Specific Agency" (SSA) is the Federal department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

SEC. 3. *Policy.* (a) It is the policy of the United States to prepare for the effects of EMPs through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement. The Federal Government must provide warning of an impending EMP; protect against, respond to, and recover from the effects of an EMP through public and private engagement, planning, and investment; and prevent adversarial events through deterrence, defense, and nuclear nonproliferation efforts. To achieve these goals, the Federal Government shall engage in risk-informed planning, prioritize research and development (R&D) to address the needs of critical infrastructure stakeholders, and, for adversarial threats, consult Intelligence Community assessments.

(b) To implement the actions directed in this order, the Federal Government shall promote collaboration and facilitate information sharing, including the sharing of threat and vulnerability assessments, among executive departments and agencies (agencies), the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate. The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innova-

tion that strengthens critical infrastructure against the effects of EMPs through the development and implementation of best practices, regulations, and appropriate guidance.

SEC. 4. *Coordination.* (a) The Assistant to the President for National Security Affairs (APNSA), through National Security Council staff and in consultation with the Director of the Office of Science and Technology Policy (OSTP), shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of EMPs. The APNSA shall, on an annual basis, submit a report to the President summarizing progress on the implementation of this order, identifying gaps in capability, and recommending how to address those gaps.

(b) To further the Federal R&D necessary to prepare the Nation for the effects of EMPs, the Director of OSTP shall coordinate efforts of agencies through the National Science and Technology Council (NSTC). The Director of OSTP, through the NSTC, shall annually review and assess the R&D needs of agencies conducting preparedness activities for EMPs, consistent with this order.

SEC. 5. *Roles and Responsibilities.* (a) The Secretary of State shall:

(i) lead the coordination of diplomatic efforts with United States allies and international partners regarding enhancing resilience to the effects of EMPs; and

(ii) in coordination with the Secretary of Defense and the heads of other relevant agencies, strengthen nuclear nonproliferation and deterrence efforts, which would reduce the likelihood of an EMP attack on the United States or its allies and partners by limiting the availability of nuclear devices.

(b) The Secretary of Defense shall:

(i) in cooperation with the heads of relevant agencies and with United States allies, international partners, and private-sector entities as appropriate, improve and develop the ability to rapidly characterize, attribute, and provide warning of EMPs, including effects on space systems of interest to the United States;

(ii) provide timely operational observations, analyses, forecasts, and other products for naturally occurring EMPs to support the mission of the Department of Defense along with United States allies and international partners, including the provision of alerts and warnings for natural EMPs that may affect weapons systems, military operations, or the defense of the United States;

(iii) conduct R&D and testing to understand the effects of EMPs on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of EMPs, and develop technologies to protect Department of Defense systems and infrastructure from the effects of EMPs to ensure the successful execution of Department of Defense missions;

(iv) review and update existing EMP-related standards for Department of Defense systems and infrastructure, as appropriate;

(v) share technical expertise and data regarding EMPs and their potential effects with other agencies and with the private sector, as appropriate;

(vi) incorporate attacks that include EMPs as a factor in defense planning scenarios; and

(vii) defend the Nation from adversarial EMPs originating outside of the United States through defense and deterrence, consistent with the mission and national security policy of the Department of Defense.

(c) The Secretary of the Interior shall support the research, development, deployment, and operation of capabilities that enhance understanding of variations of Earth's magnetic field associated with EMPs.

(d) The Secretary of Commerce shall:

(i) provide timely and accurate operational observations, analyses, forecasts, and other products for natural EMPs, exclusive of the responsibilities of the Secretary of Defense set forth in subsection (b)(ii) of this section; and

(ii) use the capabilities of the Department of Commerce, the private sector, academia, and nongovern-

mental organizations to continuously improve operational forecasting services and the development of standards for commercial EMP technology.

(e) The Secretary of Energy shall conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize sources of EMPs and their couplings to the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.

(f) The Secretary of Homeland Security shall:

(i) provide timely distribution of information on EMPs and credible associated threats to Federal, State, and local governments, critical infrastructure owners and operators, and other stakeholders;

(ii) in coordination with the heads of any relevant SSAs, use the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs;

(iii) coordinate response to and recovery from the effects of EMPs on critical infrastructure, in coordination with the heads of appropriate SSAs;

(iv) incorporate events that include EMPs as a factor in preparedness scenarios and exercises;

(v) in coordination with the heads of relevant SSAs, conduct R&D to better understand and more effectively model the effects of EMPs on national critical functions and associated critical infrastructure—excluding Department of Defense systems and infrastructure—and develop technologies and guidelines to enhance these functions and better protect this infrastructure;

(vi) maintain survivable means to provide necessary emergency information to the public during and after EMPs; and

(vii) in coordination with the Secretaries of Defense and Energy, and informed by intelligence-based threat assessments, develop quadrennial risk assessments on EMPs, with the first risk assessment delivered within 1 year of the date of this order [Mar. 26, 2019].

(g) The Director of National Intelligence shall:

(i) coordinate the collection, analysis, and promulgation, as appropriate, of intelligence-based assessments on adversaries' capabilities to conduct an attack utilizing an EMP and the likelihood of such an attack; and

(ii) provide intelligence-based threat assessments to support the heads of relevant SSAs in the development of quadrennial risk assessments on EMPs.

(h) The heads of all SSAs, in coordination with the Secretary of Homeland Security, shall enhance and facilitate information sharing with private-sector counterparts, as appropriate, to enhance preparedness for the effects of EMPs, to identify and share vulnerabilities, and to work collaboratively to reduce vulnerabilities.

(i) The heads of all agencies that support National Essential Functions shall ensure that their all-hazards preparedness planning sufficiently addresses EMPs, including through mitigation, response, and recovery, as directed by national preparedness policy.

SEC. 6. *Implementation.* (a) Identifying national critical functions and associated priority critical infrastructure at greatest risk.

(i) Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security. The Secretary of Homeland Security shall update this list as necessary.

(ii) Within 1 year of the identification described in subsection (a)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other

agencies as appropriate, shall, using appropriate government and private-sector standards for EMPs, assess which identified critical infrastructure systems, networks, and assets are most vulnerable to the effects of EMPs. The Secretary of Homeland Security shall provide this list to the President, through the APNSA. The Secretary of Homeland Security shall update this list using the results produced pursuant to subsection (b) of this section, and as necessary thereafter.

(b) Improving understanding of the effects of EMPs.

(i) Within 180 days of the identification described in subsection (a)(ii) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall review test data—identifying any gaps in such data—regarding the effects of EMPs on critical infrastructure systems, networks, and assets representative of those throughout the Nation.

(ii) Within 180 days of identifying the gaps in existing test data, as directed by subsection (b)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps. The heads of agencies identified in the plan shall implement the plan in collaboration with the private sector, as appropriate.

(iii) Within 1 year of the date of this order, and as appropriate thereafter, the Secretary of Energy, in consultation with the heads of other agencies and the private sector, as appropriate, shall review existing standards for EMPs and develop or update, as necessary, quantitative benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure.

(iv) Within 4 years of the date of this order, the Secretary of the Interior shall complete a magnetotelluric survey of the contiguous United States to help critical infrastructure owners and operators conduct EMP vulnerability assessments.

(c) Evaluating approaches to mitigate the effects of EMPs.

(i) Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, and in consultation with the Director of OSTP, the heads of other appropriate agencies, and private-sector partners as appropriate, shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of EMPs. The Secretaries of Defense, Energy, and Homeland Security shall also identify gaps in available technologies and opportunities for future technological developments to inform R&D activities.

(ii) Within 180 days of the completion of the activities directed by subsections (b)(iii) and (c)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies and in consultation with the private sector as appropriate, shall develop and implement a pilot test to evaluate available engineering approaches for mitigating the effects of EMPs on the most vulnerable critical infrastructure systems, networks, and assets, as identified in subsection (a)(ii) of this section.

(iii) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of relevant SSAs, and in consultation with appropriate regulatory and utility commissions and other stakeholders, shall identify regulatory and non-regulatory mechanisms, including cost recovery measures, that can enhance private-sector engagement to address the effects of EMPs.

(d) Strengthening critical infrastructure to withstand the effects of EMPs.

(i) Within 90 days of completing the actions directed in subsection (c)(ii) of this section, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy and in consultation with the heads of other appropriate agencies and with the private sector as appropriate, shall develop a plan to mitigate the effects of EMPs on the vulnerable priority critical infrastructure systems, networks, and assets identified under subsection (a)(ii) of this section. The plan shall align with and build on actions identified in reports required by Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) [6 U.S.C. 1500 note prec.]. The Secretary of Homeland Security shall implement those elements of the plan that are consistent with Department of Homeland Security authorities and resources, and report to the APNSA regarding any additional authorities and resources needed to complete its implementation. The Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, shall update the plan as necessary based on results from the actions directed in subsections (b) and (c) of this section.

(ii) Within 180 days of the completion of the actions identified in subsection (c)(i) of this section, the Secretary of Defense, in consultation with the Secretaries of Homeland Security and Energy, shall conduct a pilot test to evaluate engineering approaches used to harden a strategic military installation, including infrastructure that is critical to supporting that installation, against the effects of EMPs.

(iii) Within 180 days of completing the pilot test described in subsection (d)(ii) of this section, the Secretary of Defense shall report to the President, through the APNSA, regarding the cost and effectiveness of the evaluated approaches.

(e) Improving response to EMPs.

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, in coordination with the heads of appropriate SSAs, shall review and update Federal response plans, programs, and procedures to account for the effects of EMPs.

(ii) Within 180 days of the completion of actions directed by subsection (e)(i) of this section, agencies that support National Essential Functions shall update operational plans documenting their procedures and responsibilities to prepare for, protect against, and mitigate the effects of EMPs.

(iii) Within 180 days of identifying vulnerable priority critical infrastructure systems, networks, and assets as directed by subsection (a)(ii) of this section, the Secretary of Homeland Security, in consultation with the Secretaries of Defense and Commerce, and the Chairman of the Federal Communications Commission, shall provide the Deputy Assistant to the President for Homeland Security and Counterterrorism and the Director of OSTP with an assessment of the effects of EMPs on critical communications infrastructure, and recommend changes to operational plans to enhance national response and recovery efforts after an EMP.

SEC. 7. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

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

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

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

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

DONALD J. TRUMP.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a

reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

§ 195g. Countering Unmanned Aircraft Systems Coordinator

(a) Coordinator

(1) In general

The Secretary shall designate an individual in a Senior Executive Service position (as defined in section 3132 of title 5) of the Department within the Office of Strategy, Policy, and Plans as the Countering Unmanned Aircraft Systems Coordinator (in this section referred to as the “Coordinator”) and provide appropriate staff to carry out the responsibilities of the Coordinator.

(2) Responsibilities

The Coordinator shall—

(A) oversee and coordinate with relevant Department offices and components, including the Office of Civil Rights and Civil Liberties and the Privacy Office, on the development of guidance and regulations to counter threats associated with unmanned aircraft systems (in this section referred to as “UAS”) as described in section 124n of this title;

(B) promote research and development of counter UAS technologies in coordination within the Science and Technology Directorate;

(C) coordinate with the relevant components and offices of the Department, including the Office of Intelligence and Analysis, to ensure the sharing of information, guidance, and intelligence relating to countering UAS threats, counter UAS threat assessments, and counter UAS technology, including the retention of UAS and counter UAS incidents within the Department;

(D) serve as the Department liaison, in coordination with relevant components and offices of the Department, to the Department of Defense, Federal, State, local, and Tribal law enforcement entities, and the private sector regarding the activities of the Department relating to countering UAS;

(E) maintain the information required under section 124n(g)(3) of this title; and

(F) carry out other related counter UAS authorities and activities under section 124n of this title, as directed by the Secretary.

(b) Coordination with applicable Federal laws

The Coordinator shall, in addition to other assigned duties, coordinate with relevant Department components and offices to ensure testing, evaluation, or deployment of a system used to identify, assess, or defeat a UAS is carried out in accordance with applicable Federal laws.

(c) Coordination with private sector

The Coordinator shall, among other assigned duties, working with the Office of Partnership and Engagement and other relevant Department offices and components, or other Federal agencies, as appropriate, serve as the principal Department official responsible for sharing to the

private sector information regarding counter UAS technology, particularly information regarding instances in which counter UAS technology may impact lawful private sector services or systems.

(Pub. L. 107-296, title III, §321, as added Pub. L. 116-260, div. U, title VII, §701(b)(1), Dec. 27, 2020, 134 Stat. 2295.)

§ 195h. National Urban Security Technology Laboratory

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 188(c)(2) of this title. Such laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

(b) Laboratory described

The laboratory described in this subsection is the laboratory—

- (1) known, as of December 27, 2021, as the National Urban Security Technology Laboratory; and
- (2) transferred to the Department pursuant to section 183(1)(E) of this title.

(c) Laboratory activities

The National Urban Security Technology Laboratory shall—

- (1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of such technologies that can connect to the internet, for emergency response providers;
- (2) act as a technical advisor to emergency response providers; and
- (3) carry out other such activities as the Secretary determines appropriate.

(d) Rule of construction

Nothing in this section may be construed as affecting in any manner the authorities or responsibilities of the Countering Weapons of Mass Destruction Office of the Department.

(Pub. L. 107-296, title III, §322, as added Pub. L. 117-81, div. F, title LXIV, §6406(a), Dec. 27, 2021, 135 Stat. 2402.)

§ 195i. Chemical Security Analysis Center

(a) In general

The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 188(c)(2) of this title, which shall be used to conduct studies, analyses, and research to assess and address domestic chemical security events.

(b) Laboratory described

The laboratory described in this subsection is the laboratory known, as of December 23, 2022, as the Chemical Security Analysis Center.

(c) Laboratory activities

Pursuant to the authority under section 182(4) of this title, the Chemical Security Analysis Center shall—

(1) identify and develop approaches and mitigation strategies to domestic chemical security threats, including the development of comprehensive, research-based definable goals relating to such approaches and mitigation strategies;

(2) provide an enduring science-based chemical threat and hazard analysis capability;

(3) provide expertise regarding risk and consequence modeling, chemical sensing and detection, analytical chemistry, acute chemical toxicology, synthetic chemistry and reaction characterization, and nontraditional chemical agents and emerging chemical threats;

(4) staff and operate a technical assistance program that provides operational support and subject matter expertise, design and execute laboratory and field tests, and provide a comprehensive knowledge repository of chemical threat information that is continuously updated with data from scientific, intelligence, operational, and private sector sources;

(5) consult, as appropriate, with the Countering Weapons of Mass Destruction Office of the Department to mitigate, prepare, and respond to threats, hazards, and risks associated with domestic chemical security events; and

(6) carry out such other activities authorized under this section as the Secretary determines appropriate.

(d) Special rule

Nothing in this section amends, alters, or affects—

(1) the responsibilities of the Countering Weapons of Mass Destruction Office of the Department; or

(2) the activities or requirements authorized to other entities within the Federal Government, including the activities and requirements of the Environmental Protection Agency under section 7412(r) of title 42, the Toxic Substances Control Act (15 U.S.C. 2601 et seq.), and the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (commonly referred to as “Superfund”; 42 U.S.C. 9601 et seq.).

(Pub. L. 107-296, title III, §323, as added Pub. L. 117-263, div. G, title LXXI, §7106(a), Dec. 23, 2022, 136 Stat. 3624.)

Editorial Notes

REFERENCES IN TEXT

The Toxic Substances Control Act, referred to in subsec. (d)(2), is Pub. L. 94-469, Oct. 11, 1976, 90 Stat. 2003, which is classified generally to chapter 53 (§2601 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 2601 of Title 15 and Tables.

The Comprehensive Environmental Response, Compensation, and Liability Act of 1980, referred to in subsec. (d)(2), is Pub. L. 96-510, Dec. 11, 1980, 94 Stat. 2767, which is classified principally to chapter 103 (§9601 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 9601 of Title 42 and Tables.

SUBCHAPTER IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

Editorial Notes

CODIFICATION

Pub. L. 114–125, title VIII, §802(g)(1)(B)(i), Feb. 24, 2016, 130 Stat. 211, substituted “BORDER, MARITIME, AND TRANSPORTATION SECURITY” for “DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY” in subchapter heading.

PART A—BORDER, MARITIME, AND TRANSPORTATION SECURITY RESPONSIBILITIES AND FUNCTIONS

Editorial Notes

CODIFICATION

Pub. L. 114–125, title VIII, §802(g)(1)(B)(ii)(I), Feb. 24, 2016, 130 Stat. 211, substituted “Border, Maritime, and Transportation Security Responsibilities and Functions” for “Under Secretary for Border and Transportation Security” in part heading.

§ 201. Repealed. Pub. L. 114–125, title VIII, § 802(g)(2), Feb. 24, 2016, 130 Stat. 212

Section, Pub. L. 107–296, title IV, §401, Nov. 25, 2002, 116 Stat. 2177, established the Directorate of Border and Transportation Security headed by an Under Secretary for Border and Transportation Security.

§ 202. Border, maritime, and transportation responsibilities

The Secretary shall be responsible for the following:

- (1) Preventing the entry of terrorists and the instruments of terrorism into the United States.
- (2) Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.
- (3) Carrying out the immigration enforcement functions vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or any officer, employee, or component of the Immigration and Naturalization Service) immediately before the date on which the transfer of functions specified under section 251 of this title takes effect.
- (4) Establishing and administering rules, in accordance with section 236 of this title, governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States.
- (5) Establishing national immigration enforcement policies and priorities.
- (6) Except as provided in part C of this subchapter, administering the customs laws of the United States.
- (7) Conducting the inspection and related administrative functions of the Department of Agriculture transferred to the Secretary of Homeland Security under section 231 of this title.
- (8) In carrying out the foregoing responsibilities, ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce.

(Pub. L. 107–296, title IV, §402, Nov. 25, 2002, 116 Stat. 2177; Pub. L. 114–125, title VIII, §802(g)(1)(B)(ii)(II), Feb. 24, 2016, 130 Stat. 211.)

Editorial Notes

REFERENCES IN TEXT

Part C of this subchapter, referred to in par. (6), was in the original “subtitle C”, meaning subtitle C (§421 et seq.) of title IV of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2182, which enacted part C (§231 et seq.) of this subchapter and amended sections 2279e and 2279f of Title 7, Agriculture, and sections 115, 44901, and 47106 of Title 49, Transportation. For complete classification of subtitle C to the Code, see Tables.

The customs laws of the United States, referred to in par. (6), are classified generally to Title 19, Customs Duties.

AMENDMENTS

2016—Pub. L. 114–125 substituted “Border, maritime, and transportation responsibilities” for “Responsibilities” in section catchline and struck out “, acting through the Under Secretary for Border and Transportation Security,” after “The Secretary” in introductory provisions.

§ 203. Functions transferred

In accordance with subchapter XII (relating to transition provisions), there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of—

- (1) the United States Customs Service of the Department of the Treasury, including the functions of the Secretary of the Treasury relating thereto;
- (2) the Transportation Security Administration of the Department of Transportation, including the functions of the Secretary of Transportation, and of the Under Secretary of Transportation for Security, relating thereto;
- (3) the Federal Protective Service of the General Services Administration, including the functions of the Administrator of General Services relating thereto;
- (4) the Federal Law Enforcement Training Center of the Department of the Treasury; and
- (5) the Office for Domestic Preparedness of the Office of Justice Programs, including the functions of the Attorney General relating thereto.

(Pub. L. 107–296, title IV, §403, Nov. 25, 2002, 116 Stat. 2178.)

§ 204. Surface Transportation Security Advisory Committee

(a) Establishment

The Administrator of the Transportation Security Administration (referred to in this section as “Administrator”) shall establish within the Transportation Security Administration the Surface Transportation Security Advisory Committee (referred to in this section as the “Advisory Committee”).

(b) Duties

(1) In general

The Advisory Committee may advise, consult with, report to, and make recommendations to the Administrator on surface transportation security matters, including the de-