AMENDMENTS

2014—Subsec. (a). Pub. L. 113–76 substituted ''2014 and thereafter'' for ''2013'' in introductory provisions.

2013—Subsec. (a). Pub. L. 113–6 substituted ''2013'' for ''2012'' in introductory provisions.

2011—Subsec. (a). Pub. L. 112–74 substituted ''2012'' for ''2011'' in introductory provisions.

Pub. L. 112–10 substituted ''2011'' for ''2010'' in introductory provisions.

2009—Subsec. (a). Pub. L. 111–83 substituted ''2010'' for ''2009'' in introductory provisions.

2008—Subsec. (a). Pub. L. 110–329 substituted ''2009'' for ''2008'' in introductory provisions.

2007—Subsec. (a). Pub. L. 110–161 substituted ''2008'' for ''2007'' in introductory provisions.

§ 383. National Computer Forensics Institute

(a) In general; mission

There is authorized for fiscal years 2023 through 2028 within the United States Secret Service a National Computer Forensics Institute (in this section referred to as the ''Institute''). The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, and judges, as well as participants in the United States Secret Service's network of cyber fraud task forces who are Federal employees, members of the uniformed services, or State, local, Tribal, or territorial employees, regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections.

(b) Curriculum

In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections. Education and training provided pursuant to subsection (a) shall relate to the following:

(1) Investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, including relating to instances involving illicit use of digital assets and emerging trends in cybersecurity and electronic crime.

(2) Conducting forensic examinations of computers, mobile devices, and other information systems.

(3) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

(4) Methods to obtain, process, store, and admit digital evidence in court.

(c) Principles

In carrying out the functions specified in subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and information related to cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a). When selecting participants for such training, the Institute shall prioritize, to the extent reasonable and practicable, providing education and training to individuals from geographically-diverse jurisdictions throughout the United States, and the Institute shall prioritize, to the extent reasonable and practicable, State, local, tribal, and territorial law enforcement officers, prosecutors, judges, and other employees.

(d) Equipment

The Institute may provide recipients of education and training provided pursuant to subsection (a) with computer equipment, hardware, software, manuals, and tools for investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems.

(e) Cyber Fraud Task Forces

The Institute shall facilitate the expansion of the network of Cyber Fraud Task Forces of the United States Secret Service through the addition of recipients of education and training provided pursuant to subsection (a) educated and trained by the Institute.

(f) Savings provision

All authorized activities and functions carried out by the Institute at any location as of the day before November 2, 2017, are authorized to continue to be carried out at any such location on and after such date.

(g) Expenses

The Director of the United States Secret Service may pay for all or a part of the education, training, or equipment provided by the Institute, including relating to the travel, transportation, and subsistence expenses of recipients of education and training provided pursuant to subsection (a).

(h) Annual reports to Congress

(1) In general

The Secretary shall include in the annual report required under section 1116 of title 31 information regarding the activities of the Institute, including, where possible, the following:

(A) An identification of jurisdictions with recipients of the education and training provided pursuant to subsection (a) during such year.

(B) Information relating to the costs associated with that education and training.

(C) Any information regarding projected future demand for the education and training provided pursuant to subsection (a).

(D) Impacts of the activities of the Institute on the capability of jurisdictions to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats.

(E) A description of the nomination process for potential recipients of the information and training provided pursuant to subsection (a).

(F) Any other issues determined relevant by the Secretary.

(2) Exception

Any information required under paragraph (1) that is submitted as part of the annual

budget submitted by the President to Congress under section 1105 of title 31 is not required to be included in the report required under paragraph (1).

(i) Definitions

In this section:

(1) Cybersecurity threat

The term ''cybersecurity threat'' has the meaning given such term in section 1501 of this title.

(2) Incident

The term ''incident'' has the meaning given such term in section 659(a)[1] of this title.

(3) Information system

The term ''information system'' has the meaning given such term in section 1501(9) of this title.

(Pub. L. 107–296, title VIII, § 822, as added Pub. L. 115–76, § 2(a), Nov. 2, 2017, 131 Stat. 1246; amended Pub. L. 117–263, div. G, title LXXI, § 7123, Dec. 23, 2022, 136 Stat. 3641.)

Editorial Notes

REFERENCES IN TEXT

Section 659(a) of this title, referred to in subsec. (i)(2), was amended by Pub. L. 117–263, § 7143(b)(2)(D)(i), and no longer defines the term ''incident''. Reference to term ''incident'' as defined in this chapter deemed to be a reference to that term as defined in section 650(12) of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, § 7123(1), substituted, in heading, ''In general; mission'' for ''In general'', in first sentence, ''2023 through 2028'' for ''2017 through 2022'', and, in second sentence, ''The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, and judges, as well as participants in the United States Secret Service's network of cyber fraud task forces who are Federal employees, members of the uniformed services, or State, local, Tribal, or territorial employees, regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections.'' for ''The Institute shall disseminate information related to the investigation and prevention of cyber and electronic crime and related threats, and educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.''

Subsec. (b). Pub. L. 117–263, § 7123(2), amended subsec. (b) generally. Prior to amendment, subsec. (b) related to the functions of the Institute.

Subsec. (c). Pub. L. 117–263, § 7123(3), substituted ''cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)'' for ''cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors'' and inserted at end ''When selecting participants for such training, the Institute shall prioritize, to the extent reasonable and practicable, providing education and training to individuals from geographically-diverse jurisdictions throughout the United States, and the Institute shall prioritize, to the extent reasonable and practicable, State, local, tribal, and territorial law enforcement officers, prosecutors, judges, and other employees.''

Subsec. (d). Pub. L. 117–263, § 7123(4), substituted ''recipients of education and training provided pursuant to subsection (a)'' for ''State, local, tribal, and territorial law enforcement officers'' and ''for investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems'' for ''necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations''.

Subsec. (e). Pub. L. 117–263, § 7123(5), in heading, substituted ''Cyber Fraud Task Forces'' for ''Electronic Crime Task Forces'' and, in text, substituted ''Cyber Fraud'' for ''Electronic Crime'', ''recipients of education and training provided pursuant to subsection (a)'' for ''State, local, tribal, and territorial law enforcement officers'', and ''by'' for ''at''.

Subsecs. (g) to (i). Pub. L. 117–263, § 7123(6), added subsecs. (g) to (i).

PART D—ACQUISITIONS

§ 391. Research and development projects

(a) Authority

Until September 30, 2024, and subject to subsection (d),[1] the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) In general

When the Secretary carries out basic, applied, and advanced research and development projects, including the expenditure of funds for such projects, the Secretary may exercise the same authority (subject to the same limitations and conditions) with respect to such research and projects as the Secretary of Defense may exercise under section 4021 of title 10 (except for subsections (b) and (f)), after making a determination that the use of a contract, grant, or cooperative agreement for such project is not feasible or appropriate. The annual report required under subsection (b)[1] of this section, as applied to the Secretary by this paragraph, shall be submitted to the President of the Senate and the Speaker of the House of Representatives.

(2) Prototype projects

The Secretary—

(A) may, under the authority of paragraph (1), carry out prototype projects under section 4022 of title 10; and

(B) in applying the authorities of such section 4022, the Secretary shall perform the functions of the Secretary of Defense as prescribed in such section.

(b) Procurement of temporary and intermittent services

The Secretary may—

(1) procure the temporary or intermittent services of experts or consultants (or organizations thereof) in accordance with section 3109(b) of title 5; and

(2) whenever necessary due to an urgent homeland security need, procure temporary (not to exceed 1 year) or intermittent personal

[1] See References in Text note below.

[1] See References in Text note below.