117TH CONGRESS
2D SESSION

H. R. 7174

[Report No. 117–]

To amend the Homeland Security Act of 2002 to reauthorize the National Computer Forensics Institute of the United States Secret Service, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 18, 2022

Ms. SLOTKIN (for herself, Mr. PALMER, and Ms. SEWELL) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

JUNE --, 2022

Reported from the Committee on Homeland Security with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on March 18, 2022]

A BILL

To amend the Homeland Security Act of 2002 to reauthorize the National Computer Forensics Institute of the United States Secret Service, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Computer Forensics Institute Reauthorization Act of 2022".

SEC. 2. REAUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383) is amended—

(1) in subsection (a)—

(A) in the subsection heading, by striking "IN GENERAL" and inserting "IN GENERAL; MISSION";

(B) by striking "2022" and inserting "2032"; and

(C) by striking the second sentence and inserting "The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service's network of cyber fraud task forces, and other appropriate individuals regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecu-

rity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections.";

(2) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively;

(3) by striking subsection (b) and inserting the following new subsections:

"(b) CURRICULUM.—In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law and policy regarding privacy, civil rights, and civil liberties protections, including best practices for safeguarding data privacy and fair information practice principles. 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) RESEARCH AND DEVELOPMENT.—In furtherance of subsection (a), the Institute shall research, develop, and share information relating to investigating cybersecurity incidents, electronic crimes, and related cybersecurity threats that prioritize best practices for forensic examinations of computers, mobile devices, and other information systems. Such information may include training on methods to investigate ransomware and other threats involving the use of digital assets.";

(4) in subsection (d), as so redesignated—

(A) by striking "cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors" and inserting "cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)"; and

(B) by adding at the end the following new sentence: "The Institute shall prioritize providing education and training to individuals from geographically-diverse jurisdictions throughout the United States.";

(5) in subsection (e), as so redesignated—

(A) by striking "State, local, tribal, and territorial law enforcement officers" and inserting "recipients of education and training provided pursuant to subsection (a)"; and

(B) by striking "necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations" and inserting "for investigating and preventing cybersecurity incidents, electronic crimes, related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems";

(6) in subsection (f), as so redesignated—

(A) by amending the heading to read as follows: "CYBER FRAUD TASK FORCES";

(B) by striking "Electronic Crime" and inserting "Cyber Fraud";

(C) by striking "State, local, tribal, and territorial law enforcement officers" and inserting

"recipients of education and training provided pursuant to subsection (a)"; and

(D) by striking "at" and inserting "by";

(7) by redesignating subsection (g), as redesignated pursuant to paragraph (2), as subsection (j); and

(8) by inserting after subsection (f), as so redesignated, the following new subsections:

"(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.—The Secretary shall include in the annual report required pursuant to section 1116 of title 31, United States Code, information regarding the activities of the Institute, including relating to the following:

"(1) Activities of the Institute, including, where possible, an identification of jurisdictions with recipients of education and training provided pursuant to subsection (a) of this section during such year and information relating to the costs associated with such education and training.

"(2) Any information regarding projected future demand for such education and training.

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

"(4) A description of the nomination process for State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service's network of cyber fraud task forces, and other appropriate individuals to receive the education and training provided pursuant to subsection (a).

"(5) Any other issues determined relevant by the Secretary.

"(i) DEFINITIONS.—In this section—

"(1) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501))

"(2) INCIDENT.—The term 'incident' has the meaning given such term in section 2209(a).

"(3) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))).".

(b) GUIDANCE FROM THE PRIVACY OFFICER AND CIVIL RIGHTS AND CIVIL LIBERTIES OFFICER.—The Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall provide guidance, upon the request of the Director of the United States Secret Service, regarding the functions specified in subsection (b) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(c) TEMPLATE FOR INFORMATION COLLECTION FROM PARTICIPATING JURISDICTIONS.—Not later than 180 days after the date of the enactment of this Act, the Director of the United States Secret Service shall develop and disseminate to jurisdictions that are recipients of education and training provided by the National Computer Forensics Institute pursuant to subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a), a template to permit each such jurisdiction to submit to the Director reports on the impacts on such jurisdiction of such education and training, including information on the number of digital forensics exams con-

ducted annually. The Director shall, as appropriate, revise such template and disseminate to jurisdictions described in this subsection any such revised templates.

(d) REQUIREMENTS ANALYSIS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director of the United States Secret Service shall carry out a requirements analysis of approaches to expand capacity of the National Computer Forensics Institute to carry out the Institute's mission as set forth in subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(2) SUBMISSION.—Not later than 90 days after completing the requirements analysis under paragraph (1), the Director of the United States Secret Service shall submit to Congress such analysis, together with a plan to expand the capacity of the National Computer Forensics Institute to provide education and training described in such subsection. Such analysis and plan shall consider the following:

(A) Expanding the physical operations of the Institute.

(B) Expanding the availability of virtual education and training to all or a subset of po-

tential recipients of education and training from the Institute.

(C) Some combination of the considerations set forth in subparagraphs (A) and (B).

(e) RESEARCH AND DEVELOPMENT.—The Director of the United States Secret Service may coordinate with the Under Secretary for Science and Technology of the Department of Homeland Security to carry out research and development of systems and procedures to enhance the National Computer Forensics Institute's capabilities and capacity to carry out the Institute's mission as set forth in subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).