117TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 117–376
Part 1

NATIONAL COMPUTER FORENSICS INSTITUTE REAUTHORIZATION ACT OF 2022

JUNE 17, 2022.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 7174]

The Committee on Homeland Security, to whom was referred the bill (H.R. 7174) 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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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 cybersecurity 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 conducted 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 potential 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).

PURPOSE AND SUMMARY

H.R. 7174, the "National Computer Forensics Institute Reauthorization Act of 2022," would reauthorize the U.S. Secret Service's National Computer Forensics Institute (NCFI) through 2032 and make a number of targeted enhancements to position the NCFI for future success. The legislation would ensure the NCFI is able to continue its important mission of training State, local, Tribal, and Territorial officers, prosecutors, and judges in cybercrime investigations and cyber incident response. Authority to operate the NCFI will sunset in November 2022 if this bill is not enacted. Additionally, this bill would strengthen the NCFI's operations by requiring that the training provided includes privacy, civil rights, and civil liberties protections and by authorizing the NCFI to research and develop training approaches to carry out investigations involving ransomware and the use of digital assets. The bill also requires the Secretary of Homeland Security to report to Congress annually on the NCFI's activities, successes, and projected demands for training.

BACKGROUND AND NEED FOR LEGISLATION

Ransomware attacks—the use of malicious software to compromise computer systems and extort a ransom payment from victims—have surged, both in number and in the size of ransom payments demanded. In 2020, an estimated 2,400 governments, hospitals, and school districts were victims of ransomware attacks in the United States.[1] According to the Congressional Research Service, ransomware attacks are "prevalent."[2] The proliferation of computer systems for business, government, and personal use has resulted in increasing cybercrimes ranging from ransomware attacks to child exploitation. Accordingly, law enforcement, prosecutors, and judicial officials at the State, local, Tribal, Territorial, and Federal levels need advanced cyber training and capabilities.

The NCFI is a federally funded training center operated by the U.S. Secret Service that focuses on training State, local, Tribal, and Territorial officers, prosecutors, and judges in cybercrime investigations and cyber incident response. Since 2008, the NCFI, located in Hoover, Alabama, has trained more than 18,000 law enforcement officers, prosecutors, and judicial officials from all 50 States and five U.S. Territories. NCFI students receive hands-on training in network incident response and digital evidence process, and they

[1] "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Institute for Security and Technology, (2021), available at https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

[2] Peter G. Berris and Jonathan M. Gaffney, "Ransomware and Federal Law: Cybercrime and Cybersecurity," (R46932, Oct. 5, 2021), available at https://crsreports.congress.gov/product/pdf/R/R46932.

are provided equipment for digital forensics examinations. NCFI graduates conducted 122,000 digital forensic examinations in fiscal year 2021, 40 percent of which involved violent crime investigations. In 2017, Congress authorized the NCFI for 5 years.[3]

With ransomware and cyber threats rising, the NCFI's mission is more important than ever. H.R. 7174 will extend the NCFI's authorization for 10 years, through 2032, and strengthen the NCFI's operations by ensuring that its training include privacy, civil rights, and civil liberties protections. The bill also requires the NCFI to engage in research and development to improve its approaches to training and to annual report to Congress on the center's activities, successes, and projected demands for training. Finally, as amended, the bill requires reporting on the nomination process for participation in NCFI education and training to provide Congress with greater insight into how jurisdictions and their personnel are nominated and selected.

HEARING

For the purposes of clause 3(c)(6) of rule XIII of the Rules of the House of Representatives, the following hearing was used to develop H.R. 7174:

- On November 17, 2021, the Subcommittees on Intelligence and Counterterrorism and Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled, "A Whole-of-Government Approach to Combating Ransomware: Examining DHS's Role." The Subcommittees received testimony from Mr. Rob Silvers, Undersecretary of Strategy, Policy, and Plans, Department of Homeland Security; Mr. Brandon Wales, Executive Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security; and Mr. Jeremy Sheridan, Assistant Director of Investigations, U.S. Secret Service, Department of Homeland Security.

COMMITTEE CONSIDERATION

The Committee met on May 19, 2022, a quorum being present, to consider H.R. 7174 and ordered the measure to be favorably reported to the House, as amended, by a voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 7174.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

---

[3] Pub. L. 115–76 (2017) (codified at 6 U.S.C. § 383).

CORRESPONDENCE WITH OTHER COMMITTEES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, June 8, 2022.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR CHAIRMAN THOMPSON: This letter is to advise you that the Committee on the Judiciary has now had an opportunity to review the provisions in H.R. 7174, the "National Computer Forensics Institute Reauthorization Act of 2022," that fall within our Rule X jurisdiction. I appreciate your consulting with us on those provisions. The Judiciary Committe has no objection to your including them in the bill for consideration on the House floor, and to expedite that consideration is willing to forgo action on H.R. 7174, with the understanding that we do not thereby waive any future jurisdicational claim over those provisions or their subject matters.

In the event a House-Senate conference on this or similar legislation is convened, the Judiciary Committee reserves the right to request an appropriate number of conferees to address any concerns with these or similar provisions that may arise in conference.

Please place this letter into the *Congressional Record* during consideration of the measure on the House floor. Thank you for the cooperative spirit in which you have worked regarding this matter and others between our committees.

Sincerely,

JERROLD NADLER,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, June 8, 2022.

Hon. JERROLD NADLER,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR CHAIRMAN NADLER: Thank you for your letter regarding H.R. 7174, the "National Computer Forensics Institute Reauthorization Act of 2022." I recognize that the Committee on the Judiciary has a jurisdictional interest in H.R. 7174, and I appreciate your efforts to allow this bill to be considered on the House floor.

I concur with you that forgoing action on the bill does not in any way prejudice the Committee on the Judiciary with respect to its jurisdicational prerogatives on this bill or similar legislation in the future, and I would support your effort to seek appointment of an appropriate number of conferees to any House-Senate conference involving this legislation.

I will include our letters on H.R. 7174 in the Committee report on this measure and in the *Congressional Record* during floor consideration of this bill. I look forward to working with you on this legislation and other matters of great importance to this Nation.

Sincerely,

BENNIE G. THOMPSON,
Chairman.

CONGRESSIONAL BUDGET OFFICE ESTIMATE NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 7174 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 7174 is to reauthorize the NCFI for a period of 10 years (to end in 2032) and to make improvements to its operations.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 7174 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that the 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

Subsection (a) amends 6 U.S.C. § 383 to reauthorize the NCFI through 2032. It additionally makes targeted improvements by amending 6 U.S.C. § 383 as follows:

(1) providing that the NCFI's mission shall be to educate, train, and equip State, local, Tribal, and Territorial law enforcement officers, prosecutors, judges, participants in the U.S. 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 cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections;

(2) establishing curriculum requirements in furtherance of subsection (a) and requiring that training be conducted in accordance with relevant Federal law and policy regarding privacy, civil rights, and civil liberties protections;

(3) requiring the NCFI to research, develop, and share information relating to investigating cybersecurity incidents, electronic crimes, and related cybersecurity threats, which prioritizes best practices and may include training on methods to investigate ransomware and other threats involving the use of digital assets;

(4) requiring the NCFI to prioritize providing education and training to individuals from geographically diverse jurisdictions throughout the United States;

(5) permitting the Director of the Secret Service to pay for all or a part of the education, training, or equipment provided by the Institute, including relating to travel, transportation, and subsistence expenses;

(6) requiring the Secretary of Homeland Security to report on NCFI activities, including identifying jurisdictions that receive education and training, a description of the process by which individuals are nominated and selected for training and education at the NCFI, projected future demand for NCFI education and training, and impacts of NCFI education and training on jurisdictions' capability to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats; and

(7) establishing definitions for "cybersecurity threat," "incident," and "information system."

The report by the Secretary of Homeland Security required by section 2(a)(8) of the bill, as amended, includes a description of the process by which individuals are nominated for training and education at the NCFI, which necessarily includes a description of the selection process by the NCFI. The Committee notes that in discussions with NCFI leadership, resource limitations have resulted in the Center not being able to take students from all the jurisdictions that seek the training and, as such, believes that it is worthwhile for the Center to look at a range of options to expand capacity to address current and future demand. The Committee has an interest in a wide range of personnel with varying levels of experience

from geographically diverse jurisdictions accessing this valuable training and support.

Subsection (b) requires the Privacy Officer and Officer for Civil Rights and Civil Liberties of the Department of Homeland Security to, upon request of the Director of the Secret Service, provide guidance on NCFI training and education activities.

Subsection (c) directs the Director of the Secret Service to develop and disseminate, to jurisdictions that receive education and training provided by the NCFI, a template to permit each jurisdiction to submit to the Director reports on the impacts of NCFI education and training, including information on the number of forensics exams conducted annually.

Subsection (d) requires, within 1 year after the date of enactment, the Director of the Secret Service to carry out a requirements analysis of approaches to expand the NCFI's capacity and to submit such analysis to Congress, together with a plan to expand the capacity of the NCFI. Additionally, it requires such analysis and plan to consider expanding the physical operations of the Institute, expanding the availability of virtual education and training, and some combination of the two.

Subsection (e) permits the Director of the Secret Service to 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 NCFI's capabilities and capacity.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle C—United States Secret Service

* * * * * * *

SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.

(a) [IN GENERAL] *IN GENERAL; MISSION*.—There is authorized for fiscal years 2017 through [2022] *2032* within the United States

Secret Service a National Computer Forensics Institute (in this section referred to as the "Institute"). [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.] *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 cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections.*

[(b) FUNCTIONS.—The functions of the Institute shall include the following:

[(1) Educating State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on current—

[(A) cyber and electronic crimes and related threats;

[(B) methods for investigating cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations; and

[(C) prosecutorial and judicial challenges related to cyber and electronic crime and related threats, and computer and mobile device forensic examinations.

[(2) Training State, local, tribal, and territorial law enforcement officers to—

[(A) conduct cyber and electronic crime and related threat investigations;

[(B) conduct computer and mobile device forensic examinations; and

[(C) respond to network intrusion incidents.

[(3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.]

(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.

[(c)**]** *(d)* 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 **[**cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors**]** *cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a). The Institute shall prioritize providing education and training to individuals from geographically-diverse jurisdictions throughout the United States.*

[(d)**]** *(e)* EQUIPMENT.—The Institute may provide **[**State, local, tribal, and territorial law enforcement officers**]** *recipients of education and training provided pursuant to subsection (a)* with computer equipment, hardware, software, manuals, and tools **[**necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations**]** *for investigating and preventing cybersecurity incidents, electronic crimes, related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems*.

[(e) ELECTRONIC CRIME TASK FORCES.—**]**

(f) CYBER FRAUD TASK FORCES.—The Institute shall facilitate the expansion of the network of **[**Electronic Crime**]** *Cyber Fraud* Task Forces of the United States Secret Service through the addition of **[**State, local, tribal, and territorial law enforcement officers**]** *recipients of education and training provided pursuant to subsection (a)* educated and trained **[**at**]** *by* the Institute.

(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))).

[(f)**]** *(j)* SAVINGS PROVISION.—All authorized activities and functions carried out by the Institute at any location as of the day before the date of the enactment of this section are authorized to continue to be carried out at any such location on and after such date.

* * * * * * *

○