

117TH CONGRESS
2D SESSION

H. R. 7174

AN ACT

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “National Computer
3 Forensics Institute Reauthorization Act of 2022”.

4 **SEC. 2. REAUTHORIZATION OF THE NATIONAL COMPUTER**
5 **FORENSICS INSTITUTE OF THE DEPARTMENT**
6 **OF HOMELAND SECURITY.**

7 (a) IN GENERAL.—Section 822 of the Homeland Se-
8 curity Act of 2002 (6 U.S.C. 383) is amended—

9 (1) in subsection (a)—

10 (A) in the subsection heading, by striking
11 “IN GENERAL” and inserting “IN GENERAL;
12 MISSION”;

13 (B) by striking “2022” and inserting
14 “2032”; and

15 (C) by striking the second sentence and in-
16 serting “The Institute’s mission shall be to edu-
17 cate, train, and equip State, local, territorial,
18 and Tribal law enforcement officers, prosecu-
19 tors, judges, participants in the United States
20 Secret Service’s network of cyber fraud task
21 forces, and other appropriate individuals re-
22 garding the investigation and prevention of cy-
23 bersecurity incidents, electronic crimes, and re-
24 lated cybersecurity threats, including through
25 the dissemination of homeland security informa-
26 tion, in accordance with relevant Department

1 guidance regarding privacy, civil rights, and
2 civil liberties protections.”;

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

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

7 “(b) CURRICULUM.—In furtherance of subsection
8 (a), all education and training of the Institute shall be
9 conducted in accordance with relevant Federal law and
10 policy regarding privacy, civil rights, and civil liberties pro-
11 tections, including best practices for safeguarding data
12 privacy and fair information practice principles. Education
13 and training provided pursuant to subsection (a) shall re-
14 late to the following:

15 “(1) Investigating and preventing cybersecurity
16 incidents, electronic crimes, and related cybersecu-
17 rity threats, including relating to instances involving
18 illicit use of digital assets and emerging trends in cy-
19 bersecurity and electronic crime.

20 “(2) Conducting forensic examinations of com-
21 puters, mobile devices, and other information sys-
22 tems.

23 “(3) Prosecutorial and judicial considerations
24 related to cybersecurity incidents, electronic crimes,
25 related cybersecurity threats, and forensic examina-

1 tions of computers, mobile devices, and other infor-
2 mation systems.

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

5 “(c) RESEARCH AND DEVELOPMENT.—In further-
6 ance of subsection (a), the Institute shall research, de-
7 velop, and share information relating to investigating cy-
8 bersecurity incidents, electronic crimes, and related cyber-
9 security threats that prioritize best practices for forensic
10 examinations of computers, mobile devices, and other in-
11 formation systems. Such information may include training
12 on methods to investigate ransomware and other threats
13 involving the use of digital assets.”;

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

15 (A) by striking “cyber and electronic crime
16 and related threats is shared with State, local,
17 tribal, and territorial law enforcement officers
18 and prosecutors” and inserting “cybersecurity
19 incidents, electronic crimes, and related cyberse-
20 curity threats is shared with recipients of edu-
21 cation and training provided pursuant to sub-
22 section (a)”;

23 (B) by adding at the end the following new
24 sentence: “The Institute shall prioritize pro-
25 viding education and training to individuals

1 from geographically-diverse jurisdictions
2 throughout the United States.”;

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

4 (A) by striking “State, local, tribal, and
5 territorial law enforcement officers” and insert-
6 ing “recipients of education and training pro-
7 vided pursuant to subsection (a)”;

8 (B) by striking “necessary to conduct
9 cyber and electronic crime and related threat
10 investigations and computer and mobile device
11 forensic examinations” and inserting “for inves-
12 tigating and preventing cybersecurity incidents,
13 electronic crimes, related cybersecurity threats,
14 and for forensic examinations of computers,
15 mobile devices, and other information systems”;

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

17 (A) by amending the heading to read as
18 follows: “CYBER FRAUD TASK FORCES”;

19 (B) by striking “Electronic Crime” and in-
20 serting “Cyber Fraud”;

21 (C) by striking “State, local, tribal, and
22 territorial law enforcement officers” and insert-
23 ing “recipients of education and training pro-
24 vided pursuant to subsection (a)”;

25 (D) by striking “at” and inserting “by”;

1 (7) by redesignating subsection (g), as redesign-
2 nated pursuant to paragraph (2), as subsection (j);
3 and

4 (8) by inserting after subsection (f), as so re-
5 designated, the following new subsections:

6 “(g) EXPENSES.—The Director of the United States
7 Secret Service may pay for all or a part of the education,
8 training, or equipment provided by the Institute, including
9 relating to the travel, transportation, and subsistence ex-
10 penses of recipients of education and training provided
11 pursuant to subsection (a).

12 “(h) ANNUAL REPORTS TO CONGRESS.—The Sec-
13 retary shall include in the annual report required pursuant
14 to section 1116 of title 31, United States Code, informa-
15 tion regarding the activities of the Institute, including re-
16 lating to the following:

17 “(1) Activities of the Institute, including, where
18 possible, an identification of jurisdictions with recipi-
19 ents of education and training provided pursuant to
20 subsection (a) of this section during such year and
21 information relating to the costs associated with
22 such education and training.

23 “(2) Any information regarding projected fu-
24 ture demand for such education and training.

1 “(3) Impacts of the Institute’s activities on ju-
2 risdictions’ capability to investigate and prevent cy-
3 bersecurity incidents, electronic crimes, and related
4 cybersecurity threats.

5 “(4) A description of the nomination process
6 for State, local, territorial, and Tribal law enforce-
7 ment officers, prosecutors, judges, participants in
8 the United States Secret Service’s network of cyber
9 fraud task forces, and other appropriate individuals
10 to receive the education and training provided pursu-
11 ant to subsection (a).

12 “(5) Any other issues determined relevant by
13 the Secretary.

14 “(i) DEFINITIONS.—In this section—

15 “(1) CYBERSECURITY THREAT.—The term ‘cy-
16 bersecurity threat’ has the meaning given such term
17 in section 102 of the Cybersecurity Act of 2015 (en-
18 acted as division N of the Consolidated Appropria-
19 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
20 1501))

21 “(2) INCIDENT.—The term ‘incident’ has the
22 meaning given such term in section 2209(a).

23 “(3) INFORMATION SYSTEM.—The term ‘infor-
24 mation system’ has the meaning given such term in
25 section 102 of the Cybersecurity Act of 2015 (en-

1 acted as division N of the Consolidated Appropria-
2 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
3 1501(9))).”.

4 (b) GUIDANCE FROM THE PRIVACY OFFICER AND
5 CIVIL RIGHTS AND CIVIL LIBERTIES OFFICER.—The Pri-
6 vacy Officer and the Officer for Civil Rights and Civil Lib-
7 erties of the Department of Homeland Security shall pro-
8 vide guidance, upon the request of the Director of the
9 United States Secret Service, regarding the functions
10 specified in subsection (b) of section 822 of the Homeland
11 Security Act of 2002 (6 U.S.C. 383), as amended by sub-
12 section (a).

13 (c) TEMPLATE FOR INFORMATION COLLECTION
14 FROM PARTICIPATING JURISDICTIONS.—Not later than
15 180 days after the date of the enactment of this Act, the
16 Director of the United States Secret Service shall develop
17 and disseminate to jurisdictions that are recipients of edu-
18 cation and training provided by the National Computer
19 Forensics Institute pursuant to subsection (a) of section
20 822 of the Homeland Security Act of 2002 (6 U.S.C.
21 383), as amended by subsection (a), a template to permit
22 each such jurisdiction to submit to the Director reports
23 on the impacts on such jurisdiction of such education and
24 training, including information on the number of digital
25 forensics exams conducted annually. The Director shall,

1 as appropriate, revise such template and disseminate to
2 jurisdictions described in this subsection any such revised
3 templates.

4 (d) REQUIREMENTS ANALYSIS.—

5 (1) IN GENERAL.—Not later than one year
6 after the date of the enactment of this Act, the Di-
7 rector of the United States Secret Service shall carry
8 out a requirements analysis of approaches to expand
9 capacity of the National Computer Forensics Insti-
10 tute to carry out the Institute’s mission as set forth
11 in subsection (a) of section 822 of the Homeland Se-
12 curity Act of 2002 (6 U.S.C. 383), as amended by
13 subsection (a).

14 (2) SUBMISSION.—Not later than 90 days after
15 completing the requirements analysis under para-
16 graph (1), the Director of the United States Secret
17 Service shall submit to Congress such analysis, to-
18 gether with a plan to expand the capacity of the Na-
19 tional Computer Forensics Institute to provide edu-
20 cation and training described in such subsection.
21 Such analysis and plan shall consider the following:

22 (A) Expanding the physical operations of
23 the Institute.

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

1 tential recipients of education and training from
2 the Institute.

3 (C) Some combination of the consider-
4 ations set forth in subparagraphs (A) and (B).

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

Passed the House of Representatives July 13, 2022.

Attest:

Clerk.

117TH CONGRESS
2^D SESSION

H. R. 7174

AN ACT

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.