

117TH CONGRESS  
2D SESSION

# 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.

---

## 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

---

## 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.

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

3 **SECTION 1. SHORT TITLE.**

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

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

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

6 (1) in subsection (a)—

7 (A) in the subsection heading, by striking  
8 “IN GENERAL” and inserting “IN GENERAL;  
9 MISSION”;

10 (B) by striking “2022” and inserting  
11 “2032”; and

12 (C) by striking the second sentence and in-  
13 serting “The Institute’s mission shall be to edu-  
14 cate, train, and equip State, local, territorial,  
15 and Tribal law enforcement officers, prosecu-  
16 tors, judges, participants in the United States  
17 Secret Service’s network of cyber fraud task  
18 forces, and other appropriate individuals re-  
19 garding investigating and preventing cybersecu-  
20 rity incidents, electronic crimes, and related cy-  
21 bersecurity threats, including through the dis-  
22 semination of homeland security information, in  
23 accordance with relevant Department guidance  
24 regarding privacy, civil rights, and civil liberties  
25 protections.”;

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

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

5           “(b) CURRICULUM.—In furtherance of subsection  
6 (a), all activities of the Institute shall be conducted in ac-  
7 cordance with relevant Federal law and policy regarding  
8 privacy, civil rights, and civil liberties protections, includ-  
9 ing best practices for safeguarding data privacy and fair  
10 information practice principles. Activities undertaken pur-  
11 suant to subsection (a) shall relate to the following:

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

17           “(2) Conducting forensic examinations of com-  
18 puters, mobile devices, and other information sys-  
19 tems.

20           “(3) Prosecutorial and judicial considerations  
21 related to cybersecurity incidents, electronic crimes,  
22 related cybersecurity threats, and forensic examina-  
23 tions of computers, mobile devices, and other infor-  
24 mation systems.

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

3           “(c) RESEARCH, DEVELOPMENT, AND INNOVA-  
4 TION.—In furtherance of subsection (a), the Institute  
5 shall research, develop, and share innovative approaches  
6 to investigating cybersecurity incidents, electronic crimes,  
7 and related cybersecurity threats that prioritize best prac-  
8 tices for forensic examinations of computers, mobile de-  
9 vices, and other information systems. Such innovative ap-  
10 proaches may include training on methods to investigate  
11 ransomware and other threats involving the use of digital  
12 assets.”;

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

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

22           (B) by adding at the end the following new  
23           sentence: “The Institute shall prioritize pro-  
24           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 identi-  
18               fying the jurisdictions with recipients of education  
19               and training provided pursuant to subsection (a) of  
20               this section during such year, the Institute’s oper-  
21               ating budget for such year, and projected demands  
22               for education and training over the next five years.

23               “(2) Impacts of the Institute’s activities on ju-  
24               risdictions’ capability to investigate and prevent cy-

1       bersecurity incidents, electronic crimes, and related  
2       cybersecurity threats.

3               “(3) Any other issues determined relevant by  
4       the Secretary.

5       “(i) DEFINITIONS.—In this section—

6               “(1) CYBERSECURITY THREAT.—The term ‘cy-  
7       bersecurity threat’ has the meaning given such term  
8       in section 102 of the Cybersecurity Act of 2015 (en-  
9       acted as division N of the Consolidated Appropria-  
10      tions Act, 2016 (Public Law 114–113; 6 U.S.C.  
11      1501)).

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

14              “(3) INFORMATION SYSTEM.—The term ‘infor-  
15      mation system’ has the meaning given such term in  
16      section 102 of the Cybersecurity Act of 2015 (en-  
17      acted as division N of the Consolidated Appropria-  
18      tions Act, 2016 (Public Law 114–113; 6 U.S.C.  
19      1501(9))).”.

20       (b) GUIDANCE FROM THE PRIVACY OFFICER AND  
21      CIVIL RIGHTS AND CIVIL LIBERTIES OFFICER.—The Pri-  
22      vacy Officer and the Officer for Civil Rights and Civil Lib-  
23      erties of the Department of Homeland Security shall pro-  
24      vide guidance, upon the request of the Director of the  
25      United States Secret Service, regarding the functions

1 specified in subsection (b) of section 822 of the Homeland  
2 Security Act of 2002 (6 U.S.C. 383), as amended by sub-  
3 section (a).

4 (c) TEMPLATE FOR INFORMATION COLLECTION  
5 FROM PARTICIPATING JURISDICTIONS.—Not later than  
6 180 days after the date of the enactment of this Act, the  
7 Director of the United States Secret Service shall develop  
8 and disseminate to jurisdictions that are recipients of edu-  
9 cation and training provided by the National Computer  
10 Forensics Institute pursuant to subsection (a) of section  
11 822 of the Homeland Security Act of 2002 (6 U.S.C.  
12 383), as amended by subsection (a), a template to permit  
13 each such jurisdiction to submit to the Director reports  
14 on the impacts on such jurisdiction of such education and  
15 training, including information on the number of digital  
16 forensics exams conducted annually. The Director shall,  
17 as appropriate, revise such template and disseminate to  
18 jurisdictions described in this subsection any such revised  
19 templates.

20 (d) REQUIREMENTS ANALYSIS.—

21 (1) IN GENERAL.—Not later than one year  
22 after the date of the enactment of this Act, the Di-  
23 rector of the United States Secret Service shall carry  
24 out a requirements analysis of approaches to expand  
25 capacity of the National Computer Forensics Insti-



1       tute to carry out the Institute’s mission as set forth  
2       in subsection (a) of section 822 of the Homeland Se-  
3       curity Act of 2002 (6 U.S.C. 383), as amended by  
4       subsection (a).

5               (2) SUBMISSION.—Not later than 90 days after  
6       completing the requirements analysis under para-  
7       graph (1), the Director of the United States Secret  
8       Service shall submit to Congress such analysis, to-  
9       gether with a plan to expand the capacity of the Na-  
10      tional Computer Forensics Institute to provide edu-  
11      cation and training described in such subsection.  
12      Such analysis and plan shall consider the following:

13               (A) Expanding the physical operations of  
14      the Institute.

15               (B) Expanding the availability of virtual  
16      education and training to all or a subset of po-  
17      tential recipients of education and training from  
18      the Institute.

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

21      (e) RESEARCH AND DEVELOPMENT.—The Director  
22      of the United States Secret Service, in coordination with  
23      the Under Secretary for Science and Technology of the  
24      Department of Homeland Security, shall carry out re-  
25      search and development of systems and procedures to en-

1 hance the National Computer Forensics Institute's capa-  
2 bilities and capacity to educate, train, equip, and dissemi-  
3 nate information consistent with the Institute's mission as  
4 set forth in subsection (a) of section 822 of the Homeland  
5 Security Act of 2002 (6 U.S.C. 383), as amended by sub-  
6 section (a).

○