

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 7174
OFFERED BY MS. SLOTKIN OF MICHIGAN**

Strike all after the enacting clause and insert the following:

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-

1 tors, judges, participants in the United States
2 Secret Service’s network of cyber fraud task
3 forces, and other appropriate individuals re-
4 garding the investigation and prevention of cy-
5 bersecurity incidents, electronic crimes, and re-
6 lated cybersecurity threats, including through
7 the dissemination of homeland security informa-
8 tion, in accordance with relevant Department
9 guidance regarding privacy, civil rights, and
10 civil liberties protections.”;

11 (2) by redesignating subsections (e) through (f)
12 as subsections (d) through (g), respectively;

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

15 “(b) CURRICULUM.—In furtherance of subsection
16 (a), all education and training of the Institute shall be
17 conducted in accordance with relevant Federal law and
18 policy regarding privacy, civil rights, and civil liberties pro-
19 tections, including best practices for safeguarding data
20 privacy and fair information practice principles. Education
21 and training provided pursuant to subsection (a) shall re-
22 late to the following:

23 “(1) Investigating and preventing cybersecurity
24 incidents, electronic crimes, and related cybersecu-
25 rity threats, including relating to instances involving

1 illicit use of digital assets and emerging trends in cy-
2 bersecurity and electronic crime.

3 “(2) Conducting forensic examinations of com-
4 puters, mobile devices, and other information sys-
5 tems.

6 “(3) Prosecutorial and judicial considerations
7 related to cybersecurity incidents, electronic crimes,
8 related cybersecurity threats, and forensic examina-
9 tions of computers, mobile devices, and other infor-
10 mation systems.

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

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

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

23 (A) by striking “cyber and electronic crime
24 and related threats is shared with State, local,
25 tribal, and territorial law enforcement officers

1 and prosecutors” and inserting “cybersecurity
2 incidents, electronic crimes, and related cyberse-
3 curity threats is shared with recipients of edu-
4 cation and training provided pursuant to sub-
5 section (a)”;

6 (B) by adding at the end the following new
7 sentence: “The Institute shall prioritize pro-
8 viding education and training to individuals
9 from geographically-diverse jurisdictions
10 throughout the United States.”;

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

12 (A) by striking “State, local, tribal, and
13 territorial law enforcement officers” and insert-
14 ing “recipients of education and training pro-
15 vided pursuant to subsection (a)”;

16 (B) by striking “necessary to conduct
17 cyber and electronic crime and related threat
18 investigations and computer and mobile device
19 forensic examinations” and inserting “for inves-
20 tigating and preventing cybersecurity incidents,
21 electronic crimes, related cybersecurity threats,
22 and for forensic examinations of computers,
23 mobile devices, and other information systems”;

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

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

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

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

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

10 (7) by redesignating subsection (g), as redesign-
11 ated pursuant to paragraph (2), as subsection (j);
12 and

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

15 “(g) EXPENSES.—The Director of the United States
16 Secret Service may pay for all or a part of the education,
17 training, or equipment provided by the Institute, including
18 relating to the travel, transportation, and subsistence ex-
19 penses of recipients of education and training provided
20 pursuant to subsection (a).

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

1 “(1) Activities of the Institute, including, where
2 possible, an identification of jurisdictions with recipi-
3 ents of education and training provided pursuant to
4 subsection (a) of this section during such year and
5 information relating to the costs associated with
6 such education and training.

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

9 “(3) Impacts of the Institute’s activities on ju-
10 risdications’ capability to investigate and prevent cy-
11 bersecurity incidents, electronic crimes, and related
12 cybersecurity threats.

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

15 “(i) DEFINITIONS.—In this section—

16 “(1) CYBERSECURITY THREAT.—The term ‘cy-
17 bersecurity threat’ has the meaning given such term
18 in section 102 of the Cybersecurity Act of 2015 (en-
19 acted as division N of the Consolidated Appropria-
20 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
21 1501))

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

24 “(3) INFORMATION SYSTEM.—The term ‘infor-
25 mation system’ has the meaning given such term in

1 section 102 of the Cybersecurity Act of 2015 (en-
2 acted as division N of the Consolidated Appropria-
3 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
4 1501(9))).”.

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

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

1 forensics exams conducted annually. The Director shall,
2 as appropriate, revise such template and disseminate to
3 jurisdictions described in this subsection any such revised
4 templates.

5 (d) REQUIREMENTS ANALYSIS.—

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

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

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

1 (B) Expanding the availability of virtual
2 education and training to all or a subset of po-
3 tential recipients of education and training from
4 the Institute.

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

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



**AMENDMENT TO THE AMENDMENT IN THE
NATURE OF A SUBSTITUTE TO H.R. 7174
OFFERED BY Mr . Thompson**

Page 6, beginning line 13, insert the following:

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



**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 7778
OFFERED BY MR. THOMPSON OF MISSISSIPPI**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Department of Home-
3 land Security Seal Protection Act of 2022”.

**4 SEC. 2. PROHIBITION ON MISUSE OF THE DEPARTMENT OF
5 HOMELAND SECURITY SEAL.**

6 Subsection (a) of section 875 of the Homeland Secu-
7 rity Act of 2002 (6 U.S.C. 455) is amended to read as
8 follows:

9 “(a) SEAL.—

10 “(1) IN GENERAL.—The Department shall have
11 a seal, the design of which shall be subject to the
12 approval of the President.

13 “(2) PROTECTION OF SEAL.—Except with the
14 written permission of the Secretary, no person may
15 knowingly use the seal, or any colorable imitation
16 thereof, of the Department in a manner reasonably
17 calculated to convey the impression that the Depart-
18 ment or any organizational component or element of

1 the Department has approved, endorsed, or author-
2 ized such use.

3 “(3) CONSTRUCTION.—Nothing in this sub-
4 section may be construed to restrict the use of the
5 seal of the Department by officers and employees of
6 the Department in their course of their official du-
7 ties.

8 “(4) EXISTING DESIGN.—Notwithstanding
9 paragraph (1), nothing in this subsection renders
10 unlawful the use of any seal of the Department the
11 design of which was lawful as of the date of the en-
12 actment of this subsection.”.



AMENDMENT TO H.R. 7779
OFFERED BY MR. THOMPSON OF
MISSISSIPPI

Page 3, beginning line 15, strike “or Chinese entity of concern”.

Page 3, beginning line 20, strike “or Chinese entity of concern, as the case may be”.

Add at the end the following:

1 (c) CHINESE ENTITIES OF CONCERN RELATIONSHIP
2 DISCLOSURES.—Beginning on the date that is 12 months
3 after the date of the enactment of this Act, the Secretary
4 of Homeland Security shall require each institution of
5 higher education which has a relationship with a Chinese
6 entity of concern that is seeking or receives Science and
7 Technology or Research and Development funds from the
8 Department of Homeland Security to notify the Secretary
9 of such relationship. Such notification shall include the fol-
10 lowing with respect to such relationship:

11 (1) An identification of the Chinese entity of
12 concern.

13 (2) Information relating to the length of such
14 relationship.

1 (3) A description of the nature of such institu-
2 tion's relationship with such Chinese entity of con-
3 cern, including the monetary value of any contract
4 awarded, or agreement entered into, as well as any
5 in-kind donation or gift, from such Chinese entity of
6 concern.

7 (d) ASSISTANCE.—The Secretary of Homeland Secu-
8 rity shall provide outreach and, upon request, technical as-
9 sistance to institutions of higher education relating to
10 compliance with this Act. In carrying out this subsection,
11 the Secretary shall provide particular attention to institu-
12 tions assisting historically Black colleges and universities
13 (as such term is defined in part B of section 322(2) of
14 the Higher Education Act of 1965 (22 U.S.C. 1061(2)),
15 Hispanic serving institutions (as such term is defined in
16 section 502 of the Higher Education Act of 1965 (20
17 U.S.C. 1101a)), Tribal colleges and universities (as such
18 term is defined in section 316(b) of the Higher Education
19 Act of 1965 (20 U.S.C. 1059c(b)), and other minority
20 serving institutions (as such defined in section 371(a) of
21 the Higher Education Act of 1965 (20 U.S.C. 1067q(a))).

22 (e) WAIVER.—

23 (1) IN GENERAL.—The Secretary of Homeland
24 Security may waive, on a case-by-case basis, and for
25 a period of not more than one year, the application

1 of subsection (b) to an institution of higher edu-
2 cation if the Secretary determines such is in the na-
3 tional security interests of the United States.

4 (2) RENEWAL.—The Secretary of Homeland
5 Security may annually renew a waiver issued pursu-
6 ant to paragraph (1) if the Secretary determines
7 such is in the national security interests of the
8 United States.

9 (3) NOTIFICATION.—If the Secretary of Home-
10 land Security issues or renews a waiver pursuant to
11 paragraph (1) or (2), respectively, not later than 30
12 days after such issuance or renewal, as the case may
13 be, the Secretary shall provide written notification to
14 the Committee on Homeland Security of the House
15 of Representatives and the Committee on Homeland
16 Security and Governmental Affairs of the Senate re-
17 garding such issuance or renewal, including a jus-
18 tification relating thereto.

19 (f) REPORTS.—Not later than 18 months after the
20 date of the enactment of this Act and annually thereafter,
21 the Secretary of Homeland Security shall report to the
22 Committee on Homeland Security of the House of Rep-
23 resentatives and the Committee on Homeland Security
24 and Governmental Affairs of the Senate regarding imple-
25 mentation of this Act during the immediately preceding

1 12 month period. Each such report shall include informa-
2 tion relating to—

3 (1) the implementation of subsections (b) and
4 (c), including the information disclosed pursuant to
5 such subsection (c); and

6 (2) outreach and the provision of technical as-
7 sistance pursuant to subsection (d).

