

116TH CONGRESS  
1ST SESSION

# S. 2775

To improve the cyber workforce of the United States, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

NOVEMBER 5, 2019

Mr. WICKER (for himself, Ms. CANTWELL, Mr. THUNE, and Ms. ROSEN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## A BILL

To improve the cyber workforce of the United States, 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 “Harvesting American  
5 Cybersecurity Knowledge through Education Act of 2019”  
6 or the “HACKED Act of 2019”.

1 **SEC. 2. IMPROVING NATIONAL INITIATIVE FOR CYBERSE-**  
2 **CURITY EDUCATION.**

3 (a) PROGRAM IMPROVEMENTS GENERALLY.—Sub-  
4 section (a) of section 401 of the Cybersecurity Enhance-  
5 ment Act of 2014 (15 U.S.C. 7451) is amended—

6 (1) in paragraph (5), by striking “; and” and  
7 inserting a semicolon;

8 (2) by redesignating paragraph (6) as para-  
9 graph (11); and

10 (3) by inserting after paragraph (5) the fol-  
11 lowing:

12 “(6) identifying cybersecurity workforce skill  
13 gaps in public and private sectors;

14 “(7) leading interagency efforts to facilitate co-  
15 ordination of Federal programs to advance cyberse-  
16 curity education, training, and workforce, such as—

17 “(A) the Federal Cyber Scholarship for  
18 Service program of the National Science Foun-  
19 dation;

20 “(B) the National Centers of Academic  
21 Excellence in Cybersecurity program of the Na-  
22 tional Security Agency and the Department of  
23 Homeland Security;

24 “(C) the GenCyber Program of the Na-  
25 tional Science Foundation and the National Se-  
26 curity Agency;

1           “(D) the apprenticeship program of the  
2           Department of Labor;

3           “(E) the Cybersecurity Education and  
4           Training Assistance Program of the Depart-  
5           ment of Homeland Security;

6           “(F) the Cyber Center of Excellence of the  
7           Army;

8           “(G) the Information Operations Com-  
9           mand program of the Navy; and

10          “(H) such others as the Director considers  
11          appropriate;

12          “(8) promoting higher education and expertise  
13          in cybersecurity through designation by the National  
14          Security Agency and the Department of Homeland  
15          Security of institutions of higher education as Na-  
16          tional Centers of Academic Excellence in Cybersecu-  
17          rity if such institutions have robust degree programs  
18          that align to specific cybersecurity-related knowledge  
19          units that are aligned to the knowledge, skills, abili-  
20          ties, and tasks from the National Initiative for Cy-  
21          bersecurity Education (NICE) Cybersecurity Work-  
22          force Framework (NIST Special Publication 800-  
23          181), or successor framework;

24          “(9) consideration of any specific needs of the  
25          cybersecurity workforce of critical infrastructure;

1           “(10) developing metrics to measure the effec-  
2           tiveness and effect of programs and initiatives to ad-  
3           vance the cybersecurity workforce; and”.

4           (b) STRATEGIC PLAN.—Subsection (c) of such sec-  
5           tion is amended—

6           (1) by striking “The Director” and inserting  
7           the following:

8           “(1) IN GENERAL.—The Director”; and

9           (2) by adding at the end the following:

10           “(2) REQUIREMENT.—The strategic plan devel-  
11           oped and implemented under paragraph (1) shall in-  
12           clude an indication of how the Director will carry  
13           out this section.”.

14           (c) CYBERSECURITY CAREER PATHWAYS.—

15           (1) IDENTIFICATION OF MULTIPLE CYBERSECU-  
16           RITY CAREER PATHWAYS.—In carrying out sub-  
17           section (a) of such section and not later than 540  
18           days after the date of the enactment of this Act, the  
19           Director shall use a consultative process with other  
20           Federal agencies, academia, and industry to identify  
21           multiple career pathways for cybersecurity work  
22           roles that can be used in the private and public sec-  
23           tors.

24           (2) REQUIREMENTS.—The Director shall en-  
25           sure that the multiple cybersecurity career pathways

1 identified under paragraph (1) indicate the knowl-  
2 edge, skills, and abilities, including relevant edu-  
3 cation, training, apprenticeships, certifications, and  
4 other experiences, that—

5 (A) align with employers' cybersecurity  
6 skill needs, including proficiency level require-  
7 ments, for its workforce; and

8 (B) prepare an individual to be successful  
9 in entering or advancing in a cybersecurity ca-  
10 reer.

11 (3) FEDERAL CAREERS.—The Director, in co-  
12 ordination with the Director of the Office of Per-  
13 sonnel Management, shall ensure the cybersecurity  
14 career pathways identified under paragraph (1)  
15 identify career opportunities in the Federal Govern-  
16 ment, including noncompetitive hiring pathways, in-  
17 cluding for individuals who participate in Federal cy-  
18 bersecurity workforce training programs referred to  
19 in section 401(a)(7) of the Cybersecurity Enhance-  
20 ment Act of 2014, as added by subsection (a)(3).

21 (d) PROFICIENCY TO PERFORM CYBERSECURITY  
22 TASKS.—Not later than 540 days after the date of the  
23 enactment of this Act, the Director shall—

24 (1) in carrying out subsection (a) of such sec-  
25 tion, assess the scope and sufficiency of efforts to

1 measure a learner’s capability to perform specific  
2 tasks found in the National Initiative for Cybersecu-  
3 rity Education (NICE) Cybersecurity Workforce  
4 Framework (NIST Special Publication 800–181) at  
5 all proficiency levels; and

6 (2) submit to Congress a report—

7 (A) on the findings of the Director with re-  
8 spect to the assessment carried out under para-  
9 graph (1); and

10 (B) with recommendations for effective  
11 methods for measuring the cybersecurity pro-  
12 ficiency of learners.

13 (e) CYBERSECURITY METRICS.—Such section is fur-  
14 ther amended by adding at the end the following:

15 “(e) CYBERSECURITY METRICS.—In carrying out  
16 subsection (a), the Director, in coordination with such  
17 agencies as the Director considers relevant, shall develop  
18 repeatable measures and reliable metrics for measuring  
19 and evaluating Federally funded cybersecurity workforce  
20 programs and initiatives based on the outcomes of such  
21 programs and initiatives.”.

22 (f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER  
23 PARTNERSHIPS.—Such section is further amended by  
24 adding at the end the following:

1       “(f) REGIONAL ALLIANCES AND MULTISTAKE-  
2 HOLDER PARTNERSHIPS.—

3               “(1) IN GENERAL.—Pursuant to section 2(b)(4)  
4 of the National Institute of Standards and Tech-  
5 nology Act (15 U.S.C. 272(b)(4)), the Director shall  
6 establish cooperative agreements between the Na-  
7 tional Initiative for Cybersecurity Education (NICE)  
8 of the Institute and regional alliances or partner-  
9 ships for cybersecurity education and workforce.

10              “(2) AGREEMENTS.—The cooperative agree-  
11 ments established under paragraph (1) shall advance  
12 the goals of the National Initiative for Cybersecurity  
13 Education Cybersecurity Workforce Framework  
14 (NIST Special Publication 800–181), or successor  
15 framework, by facilitating local and regional partner-  
16 ships—

17                      “(A) to identify the workforce needs of the  
18 local economy and classify such workforce in ac-  
19 cordance with such framework;

20                      “(B) to identify the education, training,  
21 apprenticeship, and other opportunities avail-  
22 able in the local economy; and

23                      “(C) to support opportunities to meet the  
24 needs of the local economy.

25              “(3) FINANCIAL ASSISTANCE.—

1           “(A) FINANCIAL ASSISTANCE AUTHOR-  
2           IZED.—The Director may award financial as-  
3           sistance to a regional alliance or partnership  
4           with whom the Director enters into a coopera-  
5           tive agreement under paragraph (1) in order to  
6           assist the regional alliance or partnership in  
7           carrying out the term of the cooperative agree-  
8           ment.

9           “(B) AMOUNT OF ASSISTANCE.—The ag-  
10          gregate amount of financial assistance awarded  
11          under subparagraph (A) per cooperative agree-  
12          ment shall not exceed \$200,000.

13          “(C) MATCHING REQUIREMENT.—The Di-  
14          rector may not award financial assistance to a  
15          regional alliance or partnership under subpara-  
16          graph (A) unless the regional alliance or part-  
17          nership agrees that, with respect to the costs to  
18          be incurred by the regional alliance or partner-  
19          ship in carrying out the cooperative agreement  
20          for which the assistance was awarded, the re-  
21          gional alliance or partnership will make avail-  
22          able (directly or through donations from public  
23          or private entities) non-Federal contributions in  
24          an amount equal to 50 percent of Federal funds  
25          provided under the award.



1 “(4) APPLICATION.—

2 “(A) IN GENERAL.—A regional alliance or  
3 partnership seeking to enter into a cooperative  
4 agreement under paragraph (1) and receive fi-  
5 nancial assistance under paragraph (3) shall  
6 submit to the Director an application therefor  
7 at such time, in such manner, and containing  
8 such information as the Director may require.

9 “(B) REQUIREMENTS.—Each application  
10 submitted under subparagraph (A) shall include  
11 the following:

12 “(i)(I) A plan to establish (or identi-  
13 fication of, if it already exists) a multi-  
14 stakeholder workforce partnership that in-  
15 cludes—

16 “(aa) at least one institution of  
17 higher education or nonprofit training  
18 organization; and

19 “(bb) at least one local employer  
20 or owner or operator of critical infra-  
21 structure.

22 “(II) Participation from Federal  
23 Cyber Scholarships for Service organiza-  
24 tions, National Centers of Academic Excel-  
25 lence in Cybersecurity, advanced techno-

1 logical education programs, elementary and  
2 secondary schools, training and certifi-  
3 cation providers, State and local govern-  
4 ments, economic development organiza-  
5 tions, or other community organizations is  
6 encouraged.

7 “(ii) A description of how the work-  
8 force partnership would identify the work-  
9 force needs of the local economy.

10 “(iii) A description of how the multi-  
11 stakeholder workforce partnership would  
12 leverage the programs and objectives of the  
13 National Initiative for Cybersecurity Edu-  
14 cation, such as the Cybersecurity Work-  
15 force Framework and the strategic plan of  
16 such initiative.

17 “(iv) A description of how employers  
18 in the community will be recruited to sup-  
19 port internships, apprenticeships, or coop-  
20 erative education programs in conjunction  
21 with providers of education and training.  
22 Inclusion of programs that seek to include  
23 women, minorities, or veterans is encour-  
24 aged.

1                   “(v) A definition of the metrics that  
2                   will be used to measure the success of the  
3                   efforts of the regional alliance or partner-  
4                   ship under the agreement.

5                   “(C) PRIORITY CONSIDERATION.—In  
6                   awarding financial assistance under subpara-  
7                   graph (A), the Director shall give priority con-  
8                   sideration to a regional alliance or partnership  
9                   that includes an institution of higher education  
10                  that is designated as a National Center of Aca-  
11                  demic Excellence in Cybersecurity or which re-  
12                  ceives an award under the Federal Cyber Schol-  
13                  arship for Service program located in the State  
14                  or region of the regional alliance or partnership.

15                  “(5) AUDITS.—Each cooperative agreement for  
16                  which financial assistance is awarded under para-  
17                  graph (3) shall be subject to audit requirements  
18                  under part 200 of title 2, Code of Federal Regula-  
19                  tions (relating to uniform administrative require-  
20                  ments, cost principles, and audit requirements for  
21                  Federal awards), or successor regulation.

22                  “(6) REPORTS.—

23                  “(A) IN GENERAL.—Upon completion of a  
24                  cooperative agreement under paragraph (1), the  
25                  regional alliance or partnership that partici-

1           pated in the agreement shall submit to the Di-  
2           rector a report on the activities of the regional  
3           alliance or partnership under the agreement,  
4           which may include training and education out-  
5           comes.

6           “(B) CONTENTS.—Each report submitted  
7           under subparagraph (A) by a regional alliance  
8           or partnership shall include the following:

9                   “(i) An assessment of efforts made by  
10                  the regional alliance or partnership to  
11                  carry out paragraph (2).

12                  “(ii) The metrics used by the regional  
13                  alliance or partnership to measure the suc-  
14                  cess of the efforts of the regional alliance  
15                  or partnership under the cooperative agree-  
16                  ment.”.

17       (g) TRANSFER OF SECTION.—

18           (1) TRANSFER.—Such section is transferred to  
19           the end of title III of such Act and redesignated as  
20           section 303.

21           (2) REPEAL.—Title IV of such Act is repealed.

22           (3) CLERICAL.—The table of contents in sec-  
23           tion 1(b) of such Act is amended—

24                   (A) by striking the items relating to title  
25                   IV and section 401; and

1 (B) by inserting after the item relating to  
2 section 302 the following:

“Sec. 303. National cybersecurity awareness and education program.”.

3 (4) CONFORMING AMENDMENTS.—

4 (A) Section 302(3) of the Federal Cyberse-  
5 curity Workforce Assessment Act of 2015 (Pub-  
6 lic Law 114–113) is amended by striking  
7 “under section 401 of the Cybersecurity En-  
8 hancement Act of 2014 (15 U.S.C. 7451)” and  
9 inserting “under section 303 of the Cybersecu-  
10 rity Enhancement Act of 2014 (Public Law  
11 113–274)”.

12 (B) Section 2(e)(3) of the NIST Small  
13 Business Cybersecurity Act (Public Law 115–  
14 236) is amended by striking “under section 401  
15 of the Cybersecurity Enhancement Act of 2014  
16 (15 U.S.C. 7451)” and inserting “under section  
17 303 of the Cybersecurity Enhancement Act of  
18 2014 (Public Law 113–274)”.

19 (C) Section 302(f) of the Cybersecurity  
20 Enhancement Act of 2014 (15 U.S.C. 7442(f))  
21 is amended by striking “under section 401”  
22 and inserting “under section 303”.

1 **SEC. 3. DEVELOPMENT OF STANDARDS AND GUIDELINES**  
2 **FOR IMPROVING CYBERSECURITY WORK-**  
3 **FORCE OF FEDERAL AGENCIES.**

4 (a) IN GENERAL.—Section 20(a) of the National In-  
5 stitute of Standards and Technology Act (15 U.S.C.  
6 278g–3(a)) is amended—

7 (1) in paragraph (3), by striking “; and” and  
8 inserting a semicolon;

9 (2) in paragraph (4), by striking the period at  
10 the end and inserting “; and”; and

11 (3) by adding at the end the following:

12 “(5) identify and develop standards and guide-  
13 lines for improving the cybersecurity workforce for  
14 an agency as part of the National Initiative for Cy-  
15 bersecurity Education (NICE) Cybersecurity Work-  
16 force Framework (NIST Special Publication 800–  
17 181), or successor framework.”.

18 (b) PUBLICATION OF STANDARDS AND GUIDELINES  
19 ON CYBERSECURITY AWARENESS.—Not later than 3 years  
20 after the date of the enactment of this Act and pursuant  
21 to section 20 of the National Institute of Standards and  
22 Technology Act (15 U.S.C. 278g–3), the Director of the  
23 National Institute of Standards and Technology shall pub-  
24 lish standards and guidelines for improving cybersecurity  
25 awareness of employees and contractors of Federal agen-  
26 cies.

1 **SEC. 4. MODIFICATIONS TO FEDERAL CYBER SCHOLAR-**  
2 **SHIP-FOR-SERVICE PROGRAM.**

3 Section 302 of the Cybersecurity Enhancement Act  
4 of 2014 (15 U.S.C. 7442) is amended—

5 (1) in subsection (b)—

6 (A) in paragraph (2), by striking “infor-  
7 mation technology” and inserting “information  
8 technology and cybersecurity”;

9 (B) by amending paragraph (3) to read as  
10 follows:

11 “(3) prioritize the placement of scholarship re-  
12 cipients fulfilling the post-award employment obliga-  
13 tion under this section to ensure that—

14 “(A) not less than 70 percent of such re-  
15 cipients are placed in an executive agency (as  
16 defined in section 105 of title 5, United States  
17 Code);

18 “(B) not more than 10 percent of such re-  
19 cipients are placed as educators in the field of  
20 cybersecurity at qualified institutions of higher  
21 education that provide scholarships under this  
22 section; and

23 “(C) not more than 20 percent of such re-  
24 cipients are placed in positions described in  
25 paragraphs (2) through (5) of subsection (d);  
26 and”;

1 (C) in paragraph (4), in the matter pre-  
 2 ceding subparagraph (A), by inserting “, includ-  
 3 ing by seeking to provide awards in coordina-  
 4 tion with other relevant agencies for summer  
 5 cybersecurity camp or other experiences, includ-  
 6 ing teacher training, in each of the 50 States,”  
 7 after “cybersecurity education”;

8 (2) in subsection (d)—

9 (A) in paragraph (4), by striking “or” at  
 10 the end;

11 (B) in paragraph (5), by striking the pe-  
 12 riod at the end and inserting “; or”; and

13 (C) by adding at the end the following:

14 “(6) as provided by subsection (b)(3)(B), a  
 15 qualified institution of higher education.”; and

16 (3) in subsection (m)—

17 (A) in paragraph (1), in the matter pre-  
 18 ceding subparagraph (A), by striking “cyber”  
 19 and inserting “cybersecurity”; and

20 (B) in paragraph (2), by striking “cyber”  
 21 and inserting “cybersecurity”.

22 **SEC. 5. CYBERSECURITY IN PROGRAMS OF THE NATIONAL**  
 23 **SCIENCE FOUNDATION.**

24 (a) **COMPUTER SCIENCE AND CYBERSECURITY EDU-**  
 25 **CATION RESEARCH.**—Section 310 of the American Inno-



1 vation and Competitiveness Act (42 U.S.C. 1862s–7) is  
2 amended—

3 (1) in subsection (b)—

4 (A) in paragraph (1), by inserting “and cy-  
5 bersecurity” after “computer science”; and

6 (B) in paragraph (2)—

7 (i) in subparagraph (C), by striking “;  
8 and” and inserting a semicolon;

9 (ii) in subparagraph (D), by striking  
10 the period at the end and inserting “;  
11 and”; and

12 (iii) by adding at the end the fol-  
13 lowing:

14 “(E) tools and models for the integration  
15 of cybersecurity and other interdisciplinary ef-  
16 forts into computer science education and com-  
17 putational thinking at secondary and postsec-  
18 ondary levels of education.”; and

19 (2) in subsection (c), by inserting “, cybersecu-  
20 rity,” after “computing”.

21 (b) SCIENTIFIC AND TECHNICAL EDUCATION.—Sec-  
22 tion 3(j)(9) of the Scientific and Advanced-Technology Act  
23 of 1992 (42 U.S.C. 1862i(j)(9)) is amended by inserting  
24 “and cybersecurity” after “computer science”.

1 (c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section  
2 414(d) of the American Competitiveness and Workforce  
3 Improvement Act of 1998 (42 U.S.C. 1869e) is amend-  
4 ed—

5 (1) in paragraph (1), by striking “or computer  
6 science” and inserting “computer science, or cyber-  
7 security”; and

8 (2) in paragraph (2)(A)(iii), by inserting “cy-  
9 bersecurity,” after “computer science,”.

10 (d) SCHOLARSHIPS AND GRADUATE FELLOW-  
11 SHIPS.—The Director of the National Science Foundation  
12 shall ensure that students pursuing master’s degrees and  
13 doctoral degrees in fields relating to cybersecurity are con-  
14 sidered as applicants for scholarships and graduate fellow-  
15 ships under the Graduate Research Fellowship Program  
16 under section 10 of the National Science Foundation Act  
17 of 1950 (42 U.S.C. 1869).

18 (e) PRESIDENTIAL AWARDS FOR TEACHING EXCEL-  
19 LENCE.—The Director of the National Science Founda-  
20 tion shall ensure that educators and mentors in fields re-  
21 lating to cybersecurity can be considered for—

22 (1) Presidential Awards for Excellence in Math-  
23 ematics and Science Teaching made under section  
24 117 of the National Science Foundation Authoriza-  
25 tion Act of 1988 (42 U.S.C. 1881b); and

1           (2) Presidential Awards for Excellence in  
2           STEM mentoring administered under section 307 of  
3           the American Innovation and Competitiveness Act  
4           (42 U.S.C. 1862s–6).

5 **SEC. 6. CYBERSECURITY IN STEM PROGRAMS OF THE NA-**  
6                           **TIONAL AERONAUTICS AND SPACE ADMINIS-**  
7                           **TRATION.**

8           In carrying out any STEM education program of the  
9           National Aeronautics and Space Administration (referred  
10          to in this section as “NASA”), including a program of  
11          the Office of STEM Engagement, the Administrator of  
12          NASA shall, to the maximum extent practicable, encour-  
13          age the inclusion of cybersecurity education opportunities  
14          in such program.

15 **SEC. 7. CYBERSECURITY IN DEPARTMENT OF TRANSPOR-**  
16                           **TATION PROGRAMS.**

17          (a) UNIVERSITY TRANSPORTATION CENTERS PRO-  
18          GRAM.—Section 5505 of title 49, United States Code, is  
19          amended—

20                 (1) in subsection (a)(2)(C), by inserting “in the  
21                 matters described in subparagraphs (A) through (G)  
22                 of section 6503(c)(1)” after “transportation lead-  
23                 ers”; and

24                 (2) in subsection (c)(3)(E)—

1 (A) by inserting “, including the cybersecu-  
2 rity implications of technologies relating to con-  
3 nected vehicles, connected infrastructure, and  
4 autonomous vehicles” after “autonomous vehi-  
5 cles”; and

6 (B) by striking “The Secretary” and in-  
7 serting the following:

8 “(1) IN GENERAL.—A regional university trans-  
9 portation center receiving a grant under this para-  
10 graph shall carry out research focusing on 1 or more  
11 of the matters described in subparagraphs (A)  
12 through (G) of section 6503(c)(1).

13 “(2) FOCUSED OBJECTIVES.—The Secretary”.

14 (b) TRANSPORTATION RESEARCH AND DEVELOP-  
15 MENT 5-YEAR STRATEGIC PLAN.—Section 6503(c)(1) of  
16 title 49, United States Code, is amended—

17 (1) in subparagraph (E), by striking “and” at  
18 the end;

19 (2) in subparagraph (F), by inserting “and”  
20 after the semicolon at the end; and

21 (3) by adding at the end the following:

22 “(G) reducing transportation cybersecurity  
23 risks;”.

1 **SEC. 8. COORDINATION OF FEDERAL CYBERSECURITY**  
2 **WORKFORCE.**

3 (a) COORDINATION OF FEDERAL STEM PROGRAMS  
4 AND ACTIVITIES.—Section 101(a) of the America COM-  
5 PETES Reauthorization Act of 2010 (42 U.S.C. 6621(a))  
6 is amended by inserting “the National Institute of Stand-  
7 ards and Technology,” after “the National Aeronautics  
8 and Space Administration,”.

9 (b) SUBCOMMITTEES AND WORKING GROUPS.—Sec-  
10 tion 101 of the America COMPETES Reauthorization Act  
11 of 2010 (42 U.S.C. 6621) is amended—

12 (1) by redesignating subsection (d) as sub-  
13 section (e);

14 (2) by inserting after subsection (c) the fol-  
15 lowing:

16 “(d) SUBCOMMITTEES AND WORKING GROUPS.—

17 “(1) SUBCOMMITTEES AND WORKING GROUPS  
18 AUTHORIZED.—

19 “(A) IN GENERAL.—The committee estab-  
20 lished under subsection (a) may establish 1 or  
21 more subcommittees or working groups to ad-  
22 dress specific issues in STEM education, as the  
23 committee considers appropriate.

24 “(B) COMPOSITION.—A member of the  
25 committee established under subsection (a) may

1           serve on a subcommittee or working group es-  
2           tablished under subparagraph (A).

3           “(2) SUBCOMMITTEE ON CYBERSECURITY  
4           WORKFORCE REQUIRED.—

5                   “(A) IN GENERAL.—The committee estab-  
6           lished under subsection (a) shall establish or  
7           designate a subcommittee to coordinate cyberse-  
8           curity education and workforce activities and  
9           programs of the Federal agencies.

10                   “(B) CHAIRPERSONS.—The chairpersons  
11           of the subcommittee established or designated  
12           under subsection (a) shall be—

13                           “(i) the Director;

14                           “(ii) the Director of the National In-  
15           stitute of Standards and Technology; and

16                           “(iii) the head of any Federal agency,  
17           as the Director and the Director of the  
18           National Institute of Standards and Tech-  
19           nology consider appropriate.”; and

20           (3) by adding at the end the following:

21                   “(f) STEM EDUCATION DEFINED.—For purposes of  
22           this section, the term ‘STEM education’ includes cyberse-  
23           curity education.”.

○