

Calendar No. 515

116TH CONGRESS
2D SESSION**S. 2775****[Report No. 116–254]**

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

AUGUST 12, 2020

Reported by Mr. WICKER, with amendments

[Omit the part struck through and insert the part printed in *italic*]**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 *of the National Institute of Standards and*
20 *Technology* shall use a consultative process with
21 other Federal agencies, academia, and industry to
22 identify multiple career pathways for cybersecurity
23 work roles that can be used in the private and public
24 sectors.

1 (2) REQUIREMENTS.—The Director shall en-
2 sure that the multiple cybersecurity career pathways
3 identified under paragraph (1) indicate the knowl-
4 edge, skills, and abilities, including relevant edu-
5 cation, training, apprenticeships, certifications, and
6 other experiences, that—

7 (A) align with employers’ cybersecurity
8 skill needs, including proficiency level require-
9 ments, for its workforce; and

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

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

23 (4) EXCHANGE PROGRAM.—*The Director of the*
24 *National Institute of Standards and Technology, in*
25 *coordination with the Director of the Office of Per-*

1 *sonnel Management, shall establish a voluntary pro-*
2 *gram for the exchange of employees engaged in one of*
3 *the cybersecurity work roles identified in the National*
4 *Initiative for Cybersecurity Education (NICE) Cyber-*
5 *security Workforce Framework (NIST Special Publi-*
6 *cation 800–181), or successor framework, between the*
7 *National Institute of Standards and Technology and*
8 *private sector institutions, including a nonpublic or*
9 *commercial business, a research institution, or an in-*
10 *stitution of higher education, as the Director of the*
11 *National Institute of Standards and Technology con-*
12 *siders feasible.*

13 (d) PROFICIENCY TO PERFORM CYBERSECURITY
14 TASKS.—Not later than 540 days after the date of the
15 enactment of this Act, the Director of *the National Insti-*
16 *tute of Standards and Technology* shall—

17 (1) in carrying out subsection (a) of such sec-
18 tion, assess the scope and sufficiency of efforts to
19 measure a learner’s capability to perform specific
20 tasks found in the National Initiative for Cybersecu-
21 rity Education (NICE) Cybersecurity Workforce
22 Framework (NIST Special Publication 800–181) at
23 all proficiency levels; and

24 (2) submit to Congress a report—

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

4 (B) with recommendations for effective
5 methods for measuring the cybersecurity pro-
6 ficiency of learners.

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

9 “(e) CYBERSECURITY METRICS.—In carrying out
10 subsection (a), the Director, in coordination with such
11 agencies as the Director considers relevant, shall develop
12 repeatable measures and reliable metrics for measuring
13 and evaluating Federally funded cybersecurity workforce
14 programs and initiatives based on the outcomes of such
15 programs and initiatives.”.

16 (f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER
17 PARTNERSHIPS.—Such section is further amended by
18 adding at the end the following:

19 “(f) REGIONAL ALLIANCES AND MULTISTAKE-
20 HOLDER PARTNERSHIPS.—

21 “(1) IN GENERAL.—Pursuant to section 2(b)(4)
22 of the National Institute of Standards and Tech-
23 nology Act (15 U.S.C. 272(b)(4)), the Director shall
24 establish cooperative agreements between the Na-
25 tional Initiative for Cybersecurity Education (NICE)

1 of the Institute and regional alliances or partner-
2 ships for cybersecurity education and workforce.

3 “(2) AGREEMENTS.—The cooperative agree-
4 ments established under paragraph (1) shall advance
5 the goals of the National Initiative for Cybersecurity
6 Education Cybersecurity Workforce Framework
7 (NIST Special Publication 800–181), or successor
8 framework, by facilitating local and regional partner-
9 ships—

10 “(A) to identify the workforce needs of the
11 local economy and classify such workforce in ac-
12 cordance with such framework;

13 “(B) to identify the education, training,
14 apprenticeship, and other opportunities avail-
15 able in the local economy; and

16 “(C) to support opportunities to meet the
17 needs of the local economy.

18 “(3) FINANCIAL ASSISTANCE.—

19 “(A) FINANCIAL ASSISTANCE AUTHOR-
20 IZED.—The Director may award financial as-
21 sistance to a regional alliance or partnership
22 with whom the Director enters into a coopera-
23 tive agreement under paragraph (1) in order to
24 assist the regional alliance or partnership in

1 carrying out the term of the cooperative agree-
2 ment.

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

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

20 “(4) APPLICATION.—

21 “(A) IN GENERAL.—A regional alliance or
22 partnership seeking to enter into a cooperative
23 agreement under paragraph (1) and receive fi-
24 nancial assistance under paragraph (3) shall
25 submit to the Director an application therefor

1 at such time, in such manner, and containing
2 such information as the Director may require.

3 “(B) REQUIREMENTS.—Each application
4 submitted under subparagraph (A) shall include
5 the following:

6 “(i)(I) A plan to establish (or identi-
7 fication of, if it already exists) a multi-
8 stakeholder workforce partnership that in-
9 cludes—

10 “(aa) at least one institution of
11 higher education or nonprofit training
12 organization; and

13 “(bb) at least one local employer
14 or owner or operator of critical infra-
15 structure.

16 “(II) Participation from Federal
17 Cyber Scholarships for Service organiza-
18 tions, National Centers of Academic Excel-
19 lence in Cybersecurity, advanced techno-
20 logical education programs, elementary and
21 secondary schools, training and certifi-
22 cation providers, State and local govern-
23 ments, economic development organiza-
24 tions, or other community organizations is
25 encouraged.

1 “(ii) A description of how the work-
2 force partnership would identify the work-
3 force needs of the local economy.

4 “(iii) A description of how the multi-
5 stakeholder workforce partnership would
6 leverage the programs and objectives of the
7 National Initiative for Cybersecurity Edu-
8 cation, such as the Cybersecurity Work-
9 force Framework and the strategic plan of
10 such initiative.

11 “(iv) A description of how employers
12 in the community will be recruited to sup-
13 port internships, apprenticeships, or coop-
14 erative education programs in conjunction
15 with providers of education and training.
16 Inclusion of programs that seek to include
17 women, minorities, or veterans is encour-
18 aged.

19 “(v) A definition of the metrics that
20 will be used to measure the success of the
21 efforts of the regional alliance or partner-
22 ship under the agreement.

23 “(C) PRIORITY CONSIDERATION.—In
24 awarding financial assistance under ~~subpara-~~
25 ~~graph (A)~~ *paragraph (3)(A)*, the Director shall

1 give priority consideration to a regional alliance
2 or partnership that includes an institution of
3 higher education that is designated as a Na-
4 tional Center of Academic Excellence in Cyber-
5 security or which receives an award under the
6 Federal Cyber Scholarship for Service program
7 located in the State or region of the regional al-
8 liance or partnership.

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

16 “(6) REPORTS.—

17 “(A) IN GENERAL.—Upon completion of a
18 cooperative agreement under paragraph (1), the
19 regional alliance or partnership that partici-
20 pated in the agreement shall submit to the Di-
21 rector a report on the activities of the regional
22 alliance or partnership under the agreement,
23 which may include training and education out-
24 comes.

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

4 “(i) An assessment of efforts made by
5 the regional alliance or partnership to
6 carry out paragraph (2).

7 “(ii) The metrics used by the regional
8 alliance or partnership to measure the suc-
9 cess of the efforts of the regional alliance
10 or partnership under the cooperative agree-
11 ment.”.

12 (g) TRANSFER OF SECTION.—

13 (1) TRANSFER.—Such section is transferred to
14 the end of title III of such Act and redesignated as
15 section 303.

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

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

19 (A) by striking the items relating to title
20 IV and section 401; and

21 (B) by inserting after the item relating to
22 section 302 the following:

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

23 (4) CONFORMING AMENDMENTS.—

24 (A) Section 302(3) of the Federal Cyberse-
25 curity Workforce Assessment Act of 2015 (Pub-

1 lic Law 114–113) is amended by striking
2 “under section 401 of the Cybersecurity En-
3 hancement Act of 2014 (15 U.S.C. 7451)” and
4 inserting “under section 303 of the Cybersecu-
5 rity Enhancement Act of 2014 (Public Law
6 113–274)”.

7 (B) Section 2(e)(3) of the NIST Small
8 Business Cybersecurity Act (Public Law 115–
9 236) is amended by striking “under section 401
10 of the Cybersecurity Enhancement Act of 2014
11 (15 U.S.C. 7451)” and inserting “under section
12 303 of the Cybersecurity Enhancement Act of
13 2014 (Public Law 113–274)”.

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

18 **SEC. 3. DEVELOPMENT OF STANDARDS AND GUIDELINES**
19 **FOR IMPROVING CYBERSECURITY WORK-**
20 **FORCE OF FEDERAL AGENCIES.**

21 (a) IN GENERAL.—Section 20(a) of the National In-
22 stitute of Standards and Technology Act (15 U.S.C.
23 278g–3(a)) is amended—

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

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

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

4 “(5) identify and develop standards and guide-
5 lines for improving the cybersecurity workforce for
6 an agency as part of the National Initiative for Cy-
7 bersecurity Education (NICE) Cybersecurity Work-
8 force Framework (NIST Special Publication 800–
9 181), or successor framework.”.

10 (b) **PUBLICATION OF STANDARDS AND GUIDELINES**
11 **ON CYBERSECURITY AWARENESS.**—Not later than 3 years
12 after the date of the enactment of this Act and pursuant
13 to section 20 of the National Institute of Standards and
14 Technology Act (15 U.S.C. 278g–3), the Director of the
15 National Institute of Standards and Technology shall pub-
16 lish standards and guidelines for improving cybersecurity
17 awareness of employees and contractors of Federal agen-
18 cies.

19 **SEC. 4. MODIFICATIONS TO FEDERAL CYBER SCHOLAR-**
20 **SHIP-FOR-SERVICE PROGRAM.**

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

23 (1) in subsection (b)—

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

4 (B) by amending paragraph (3) to read as
5 follows:

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

9 “(A) not less than 70 percent of such re-
10 cipients are placed in an executive agency (as
11 defined in section 105 of title 5, United States
12 Code);

13 “(B) not more than 10 percent of such re-
14 cipients are placed as educators in the field of
15 cybersecurity at qualified institutions of higher
16 education that provide scholarships under this
17 section; and

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

22 (C) in paragraph (4), in the matter pre-
23 ceding subparagraph (A), by inserting “, includ-
24 ing by seeking to provide awards in coordina-
25 tion with other relevant agencies for summer

1 cybersecurity camp or other experiences, includ-
 2 ing teacher training, in each of the 50 States,”
 3 after “cybersecurity education”;

4 (2) in subsection (d)—

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

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

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

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

12 (3) in subsection (m)—

13 (A) in paragraph (1), in the matter pre-
 14 ceding subparagraph (A), by striking “cyber”
 15 and inserting “cybersecurity”; and

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

18 **SEC. 5. CYBERSECURITY IN PROGRAMS OF THE NATIONAL**
 19 **SCIENCE FOUNDATION.**

20 (a) **COMPUTER SCIENCE AND CYBERSECURITY EDU-**
 21 **CATION RESEARCH.**—Section 310 of the American Inno-
 22 vation and Competitiveness Act (42 U.S.C. 1862s-7) is
 23 amended—

24 (1) in subsection (b)—

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

3 (B) in paragraph (2)—

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

6 (ii) in subparagraph (D), by striking
7 the period at the end and inserting “;
8 and”; and

9 (iii) by adding at the end the fol-
10 lowing:

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

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

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

22 (c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section
23 414(d) of the American Competitiveness and Workforce
24 Improvement Act of 1998 (42 U.S.C. 1869e) is amend-
25 ed—

1 (1) in paragraph (1), by striking “or computer
2 science” and inserting “computer science, or cyber-
3 security”; and

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

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

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

18 (1) Presidential Awards for Excellence in Math-
19 ematics and Science Teaching made under section
20 117 of the National Science Foundation Authoriza-
21 tion Act of 1988 (42 U.S.C. 1881b); and

22 (2) Presidential Awards for Excellence in
23 STEM ~~mentoring~~ *Mentoring* administered under sec-
24 tion 307 of the American Innovation and Competi-
25 tiveness Act (42 U.S.C. 1862s–6).

1 **SEC. 6. CYBERSECURITY IN STEM PROGRAMS OF THE NA-**
2 **TIONAL AERONAUTICS AND SPACE ADMINIS-**
3 **TRATION.**

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

11 **SEC. 7. CYBERSECURITY IN DEPARTMENT OF TRANSPOR-**
12 **TATION PROGRAMS.**

13 (a) UNIVERSITY TRANSPORTATION CENTERS PRO-
14 GRAM.—Section 5505 of title 49, United States Code, is
15 amended—

16 (1) in subsection (a)(2)(C), by inserting “in the
17 matters described in subparagraphs (A) through (G)
18 of section 6503(c)(1)” after “transportation lead-
19 ers”; and

20 (2) in subsection (c)(3)(E)—

21 (A) by inserting “, including the cybersecu-
22 rity implications of technologies relating to con-
23 nected vehicles, connected infrastructure, and
24 autonomous vehicles” after “autonomous vehi-
25 cles”; and

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

3 ~~“(1) IN GENERAL.—A regional university trans-~~
 4 ~~portation center receiving a grant under this para-~~
 5 ~~graph shall carry out research focusing on 1 or more~~
 6 ~~of the matters described in subparagraphs (A)~~
 7 ~~through (G) of section 6503(c)(1).~~

8 ~~“(2) FOCUSED OBJECTIVES.—The Secretary”.~~

9 *“(i) IN GENERAL.—A regional univer-*
 10 *sity transportation center receiving a grant*
 11 *under this paragraph shall carry out re-*
 12 *search focusing on 1 or more of the matters*
 13 *described in subparagraphs (A) through (G)*
 14 *of section 6503(c)(1).*

15 *“(ii) FOCUSED OBJECTIVES.—The Sec-*
 16 *retary”.*

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

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

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

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

1 “(G) reducing transportation cybersecurity
2 risks;”.

3 **SEC. 8. COORDINATION OF FEDERAL CYBERSECURITY**
4 **WORKFORCE.**

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

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

14 (1) by redesignating subsection (d) as sub-
15 section (e);

16 (2) by inserting after subsection (c) the fol-
17 lowing:

18 “(d) SUBCOMMITTEES AND WORKING GROUPS.—

19 “(1) SUBCOMMITTEES AND WORKING GROUPS
20 AUTHORIZED.—

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

1 “(B) COMPOSITION.—A member of the
2 committee established under subsection (a) may
3 serve on a subcommittee or working group es-
4 tablished under subparagraph (A).

5 “(2) SUBCOMMITTEE ON CYBERSECURITY
6 WORKFORCE REQUIRED.—

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

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

15 “(i) the Director;

16 “(ii) the Director of the National In-
17 stitute of Standards and Technology; and

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

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

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

Calendar No. 515

116TH CONGRESS
2^D SESSION

S. 2775

[Report No. 116-254]

A BILL

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

AUGUST 12, 2020

Reported with amendments