116TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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 _____

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Harvesting American Cybersecurity Knowledge through Education Act of 2019'' or the ''HACKED Act of 2019''.

SEC. 2. IMPROVING NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION.

(a) PROGRAM IMPROVEMENTS GENERALLY.—Subsection (a) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451) is amended—

(1) in paragraph (5), by striking ''; and'' and inserting a semicolon;

(2) by redesignating paragraph (6) as paragraph (11); and

(3) by inserting after paragraph (5) the following:

''(6) identifying cybersecurity workforce skill gaps in public and private sectors;

''(7) leading interagency efforts to facilitate coordination of Federal programs to advance cybersecurity education, training, and workforce, such as—

''(A) the Federal Cyber Scholarship for Service program of the National Science Foundation;

''(B) the National Centers of Academic Excellence in Cybersecurity program of the National Security Agency and the Department of Homeland Security;

''(C) the GenCyber Program of the National Science Foundation and the National Security Agency;

"(D) the apprenticeship program of the Department of Labor;

"(E) the Cybersecurity Education and Training Assistance Program of the Department of Homeland Security;

"(F) the Cyber Center of Excellence of the Army;

"(G) the Information Operations Command program of the Navy; and

"(H) such others as the Director considers appropriate;

"(8) promoting higher education and expertise in cybersecurity through designation by the National Security Agency and the Department of Homeland Security of institutions of higher education as National Centers of Academic Excellence in Cybersecurity if such institutions have robust degree programs that align to specific cybersecurity-related knowledge units that are aligned to the knowledge, skills, abilities, and tasks from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework;

"(9) consideration of any specific needs of the cybersecurity workforce of critical infrastructure;

''(10) developing metrics to measure the effectiveness and effect of programs and initiatives to advance the cybersecurity workforce; and''.

(b) STRATEGIC PLAN.—Subsection (c) of such section is amended—

(1) by striking ''The Director'' and inserting the following:

''(1) IN GENERAL.—The Director''; and

(2) by adding at the end the following:

''(2) REQUIREMENT.—The strategic plan developed and implemented under paragraph (1) shall include an indication of how the Director will carry out this section.''.

(c) CYBERSECURITY CAREER PATHWAYS.—

(1) IDENTIFICATION OF MULTIPLE CYBERSECURITY CAREER PATHWAYS.—In carrying out subsection (a) of such section and not later than 540 days after the date of the enactment of this Act, the Director shall use a consultative process with other Federal agencies, academia, and industry to identify multiple career pathways for cybersecurity work roles that can be used in the private and public sectors.

(2) REQUIREMENTS.—The Director shall ensure that the multiple cybersecurity career pathways

identified under paragraph (1) indicate the knowledge, skills, and abilities, including relevant education, training, apprenticeships, certifications, and other experiences, that—

(A) align with employers' cybersecurity skill needs, including proficiency level requirements, for its workforce; and

(B) prepare an individual to be successful in entering or advancing in a cybersecurity career.

(3) FEDERAL CAREERS.—The Director, in coordination with the Director of the Office of Personnel Management, shall ensure the cybersecurity career pathways identified under paragraph (1) identify career opportunities in the Federal Government, including noncompetitive hiring pathways, including for individuals who participate in Federal cybersecurity workforce training programs referred to in section 401(a)(7) of the Cybersecurity Enhancement Act of 2014, as added by subsection (a)(3).

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

(1) in carrying out subsection (a) of such section, assess the scope and sufficiency of efforts to

measure a learner's capability to perform specific tasks found in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181) at all proficiency levels; and

(2) submit to Congress a report—

(A) on the findings of the Director with respect to the assessment carried out under paragraph (1); and

(B) with recommendations for effective methods for measuring the cybersecurity proficiency of learners.

(e) CYBERSECURITY METRICS.—Such section is further amended by adding at the end the following:

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

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

''(f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER PARTNERSHIPS.—

''(1) IN GENERAL.—Pursuant to section 2(b)(4) of the National Institute of Standards and Technology Act (15 U.S.C. 272(b)(4)), the Director shall establish cooperative agreements between the National Initiative for Cybersecurity Education (NICE) of the Institute and regional alliances or partnerships for cybersecurity education and workforce.

''(2) AGREEMENTS.—The cooperative agreements established under paragraph (1) shall advance the goals of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework, by facilitating local and regional partnerships—

''(A) to identify the workforce needs of the local economy and classify such workforce in accordance with such framework;

''(B) to identify the education, training, apprenticeship, and other opportunities available in the local economy; and

''(C) to support opportunities to meet the needs of the local economy.

''(3) FINANCIAL ASSISTANCE.—

"(A) FINANCIAL ASSISTANCE AUTHORIZED.—The Director may award financial assistance to a regional alliance or partnership with whom the Director enters into a cooperative agreement under paragraph (1) in order to assist the regional alliance or partnership in carrying out the term of the cooperative agreement.

"(B) AMOUNT OF ASSISTANCE.—The aggregate amount of financial assistance awarded under subparagraph (A) per cooperative agreement shall not exceed $200,000.

"(C) MATCHING REQUIREMENT.—The Director may not award financial assistance to a regional alliance or partnership under subparagraph (A) unless the regional alliance or partnership agrees that, with respect to the costs to be incurred by the regional alliance or partnership in carrying out the cooperative agreement for which the assistance was awarded, the regional alliance or partnership will make available (directly or through donations from public or private entities) non-Federal contributions in an amount equal to 50 percent of Federal funds provided under the award.

''(4) APPLICATION.—

''(A) IN GENERAL.—A regional alliance or partnership seeking to enter into a cooperative agreement under paragraph (1) and receive financial assistance under paragraph (3) shall submit to the Director an application therefor at such time, in such manner, and containing such information as the Director may require.

''(B) REQUIREMENTS.—Each application submitted under subparagraph (A) shall include the following:

''(i)(I) A plan to establish (or identification of, if it already exists) a multi-stakeholder workforce partnership that includes—

''(aa) at least one institution of higher education or nonprofit training organization; and

''(bb) at least one local employer or owner or operator of critical infrastructure.

''(II) Participation from Federal Cyber Scholarships for Service organizations, National Centers of Academic Excellence in Cybersecurity, advanced techno-

logical education programs, elementary and secondary schools, training and certification providers, State and local governments, economic development organizations, or other community organizations is encouraged.

''(ii) A description of how the workforce partnership would identify the workforce needs of the local economy.

''(iii) A description of how the multistakeholder workforce partnership would leverage the programs and objectives of the National Initiative for Cybersecurity Education, such as the Cybersecurity Workforce Framework and the strategic plan of such initiative.

''(iv) A description of how employers in the community will be recruited to support internships, apprenticeships, or cooperative education programs in conjunction with providers of education and training. Inclusion of programs that seek to include women, minorities, or veterans is encouraged.

"(v) A definition of the metrics that will be used to measure the success of the efforts of the regional alliance or partnership under the agreement.

"(C) PRIORITY CONSIDERATION.—In awarding financial assistance under subparagraph (A), the Director shall give priority consideration to a regional alliance or partnership that includes an institution of higher education that is designated as a National Center of Academic Excellence in Cybersecurity or which receives an award under the Federal Cyber Scholarship for Service program located in the State or region of the regional alliance or partnership.

"(5) AUDITS.—Each cooperative agreement for which financial assistance is awarded under paragraph (3) shall be subject to audit requirements under part 200 of title 2, Code of Federal Regulations (relating to uniform administrative requirements, cost principles, and audit requirements for Federal awards), or successor regulation.

"(6) REPORTS.—

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

pated in the agreement shall submit to the Director a report on the activities of the regional alliance or partnership under the agreement, which may include training and education outcomes.

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

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

''(ii) The metrics used by the regional alliance or partnership to measure the success of the efforts of the regional alliance or partnership under the cooperative agreement.''.

(g) TRANSFER OF SECTION.—

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

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

(3) CLERICAL.—The table of contents in section 1(b) of such Act is amended—

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

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

''Sec. 303. National cybersecurity awareness and education program.''.

(4) CONFORMING AMENDMENTS.—

(A) Section 302(3) of the Federal Cybersecurity Workforce Assessment Act of 2015 (Public Law 114–113) is amended by striking ''under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)'' and inserting ''under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)''.

(B) Section 2(c)(3) of the NIST Small Business Cybersecurity Act (Public Law 115–236) is amended by striking ''under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)'' and inserting ''under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)''.

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

SEC. 3. DEVELOPMENT OF STANDARDS AND GUIDELINES FOR IMPROVING CYBERSECURITY WORKFORCE OF FEDERAL AGENCIES.

(a) IN GENERAL.—Section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) is amended—

(1) in paragraph (3), by striking ''; and'' and inserting a semicolon;

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

(3) by adding at the end the following:

''(5) identify and develop standards and guidelines for improving the cybersecurity workforce for an agency as part of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework.''.

(b) PUBLICATION OF STANDARDS AND GUIDELINES ON CYBERSECURITY AWARENESS.—Not later than 3 years after the date of the enactment of this Act and pursuant to section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), the Director of the National Institute of Standards and Technology shall publish standards and guidelines for improving cybersecurity awareness of employees and contractors of Federal agencies.

SEC. 4. MODIFICATIONS TO FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

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

(1) in subsection (b)—

(A) in paragraph (2), by striking ''information technology'' and inserting ''information technology and cybersecurity'';

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

''(3) prioritize the placement of scholarship recipients fulfilling the post-award employment obligation under this section to ensure that—

''(A) not less than 70 percent of such recipients are placed in an executive agency (as defined in section 105 of title 5, United States Code);

''(B) not more than 10 percent of such recipients are placed as educators in the field of cybersecurity at qualified institutions of higher education that provide scholarships under this section; and

''(C) not more than 20 percent of such recipients are placed in positions described in paragraphs (2) through (5) of subsection (d); and''; and

(C) in paragraph (4), in the matter preceding subparagraph (A), by inserting ", including by seeking to provide awards in coordination with other relevant agencies for summer cybersecurity camp or other experiences, including teacher training, in each of the 50 States," after "cybersecurity education";

(2) in subsection (d)—

(A) in paragraph (4), by striking "or" at the end;

(B) in paragraph (5), by striking the period at the end and inserting "; or"; and

(C) by adding at the end the following:

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

(3) in subsection (m)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking "cyber" and inserting "cybersecurity"; and

(B) in paragraph (2), by striking "cyber" and inserting "cybersecurity".

SEC. 5. CYBERSECURITY IN PROGRAMS OF THE NATIONAL SCIENCE FOUNDATION.

(a) COMPUTER SCIENCE AND CYBERSECURITY EDUCATION RESEARCH.—Section 310 of the American Inno-

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

(1) in subsection (b)—

(A) in paragraph (1), by inserting ''and cybersecurity'' after ''computer science''; and

(B) in paragraph (2)—

(i) in subparagraph (C), by striking ''; and'' and inserting a semicolon;

(ii) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(E) tools and models for the integration of cybersecurity and other interdisciplinary efforts into computer science education and computational thinking at secondary and postsecondary levels of education.''; and

(2) in subsection (c), by inserting '', cybersecurity,'' after ''computing''.

(b) SCIENTIFIC AND TECHNICAL EDUCATION.—Section 3(j)(9) of the Scientific and Advanced-Technology Act of 1992 (42 U.S.C. 1862i(j)(9)) is amended by inserting ''and cybersecurity'' after ''computer science''.

(c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section 414(d) of the American Competitiveness and Workforce Improvement Act of 1998 (42 U.S.C. 1869c) is amended—

(1) in paragraph (1), by striking ''or computer science'' and inserting ''computer science, or cybersecurity''; and

(2) in paragraph (2)(A)(iii), by inserting ''cybersecurity,'' after ''computer science,''.

(d) SCHOLARSHIPS AND GRADUATE FELLOWSHIPS.—The Director of the National Science Foundation shall ensure that students pursuing master's degrees and doctoral degrees in fields relating to cybersecurity are considered as applicants for scholarships and graduate fellowships under the Graduate Research Fellowship Program under section 10 of the National Science Foundation Act of 1950 (42 U.S.C. 1869).

(e) PRESIDENTIAL AWARDS FOR TEACHING EXCELLENCE.—The Director of the National Science Foundation shall ensure that educators and mentors in fields relating to cybersecurity can be considered for—

(1) Presidential Awards for Excellence in Mathematics and Science Teaching made under section 117 of the National Science Foundation Authorization Act of 1988 (42 U.S.C. 1881b); and

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

SEC. 6. CYBERSECURITY IN STEM PROGRAMS OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION.

In carrying out any STEM education program of the National Aeronautics and Space Administration (referred to in this section as ''NASA''), including a program of the Office of STEM Engagement, the Administrator of NASA shall, to the maximum extent practicable, encourage the inclusion of cybersecurity education opportunities in such program.

SEC. 7. CYBERSECURITY IN DEPARTMENT OF TRANSPORTATION PROGRAMS.

(a) UNIVERSITY TRANSPORTATION CENTERS PROGRAM.—Section 5505 of title 49, United States Code, is amended—

(1) in subsection (a)(2)(C), by inserting ''in the matters described in subparagraphs (A) through (G) of section 6503(c)(1)'' after ''transportation leaders''; and

(2) in subsection (c)(3)(E)—

(A) by inserting ", including the cybersecurity implications of technologies relating to connected vehicles, connected infrastructure, and autonomous vehicles" after "autonomous vehicles"; and

(B) by striking "The Secretary" and inserting the following:

"(1) IN GENERAL.—A regional university transportation center receiving a grant under this paragraph shall carry out research focusing on 1 or more of the matters described in subparagraphs (A) through (G) of section 6503(c)(1).

"(2) FOCUSED OBJECTIVES.—The Secretary".

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

(1) in subparagraph (E), by striking "and" at the end;

(2) in subparagraph (F), by inserting "and" after the semicolon at the end; and

(3) by adding at the end the following:

"(G) reducing transportation cybersecurity risks;".

SEC. 8. COORDINATION OF FEDERAL CYBERSECURITY WORKFORCE.

(a) COORDINATION OF FEDERAL STEM PROGRAMS AND ACTIVITIES.—Section 101(a) of the America COMPETES Reauthorization Act of 2010 (42 U.S.C. 6621(a)) is amended by inserting ''the National Institute of Standards and Technology,'' after ''the National Aeronautics and Space Administration,''.

(b) SUBCOMMITTEES AND WORKING GROUPS.—Section 101 of the America COMPETES Reauthorization Act of 2010 (42 U.S.C. 6621) is amended—

(1) by redesignating subsection (d) as subsection (e);

(2) by inserting after subsection (c) the following:

''(d) SUBCOMMITTEES AND WORKING GROUPS.—

''(1) SUBCOMMITTEES AND WORKING GROUPS AUTHORIZED.—

''(A) IN GENERAL.—The committee established under subsection (a) may establish 1 or more subcommittees or working groups to address specific issues in STEM education, as the committee considers appropriate.

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

serve on a subcommittee or working group established under subparagraph (A).

''(2) SUBCOMMITTEE ON CYBERSECURITY WORKFORCE REQUIRED.—

''(A) IN GENERAL.—The committee established under subsection (a) shall establish or designate a subcommittee to coordinate cybersecurity education and workforce activities and programs of the Federal agencies.

''(B) CHAIRPERSONS.—The chairpersons of the subcommittee established or designated under subsection (a) shall be—

''(i) the Director;

''(ii) the Director of the National Institute of Standards and Technology; and

''(iii) the head of any Federal agency, as the Director and the Director of the National Institute of Standards and Technology consider appropriate.''; and

(3) by adding at the end the following:

''(f) STEM EDUCATION DEFINED.—For purposes of this section, the term 'STEM education' includes cybersecurity education.''.