I

116TH CONGRESS
2D SESSION

H. R. 8634

To improve United States cybersecurity through STEM scholarships, prize competitions, and other STEM activities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 20, 2020

Ms. KENDRA S. HORN of Oklahoma introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Education and Labor, 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 improve United States cybersecurity through STEM scholarships, prize competitions, and other STEM activities, 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 ''HACKED Act''.

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(a)) is amended—

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

(2) by redesignating paragraph (6) as paragraph (10); and

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

''(6) supporting efforts to identify cybersecurity workforce skill gaps in public and private sectors;

''(7) facilitating efforts for Federal programs to advance cybersecurity education, training, and workforce development;

''(8) in coordination with the Department of Homeland Security and other appropriate agencies, considering any specific needs of the cybersecurity workforce of critical infrastructure, to include cyber physical systems and control systems;

''(9) advising the Director of the Office of Management and Budget, as needed, in 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 subsection.''.

(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 of the National Institute of Standards and Technology shall, in coordination with the Secretary of Homeland Security, the Director of the Office of Personnel Management, and other appropriate agencies, use a consultative process with other Federal agencies, academia, and industry to make public a report identifying multiple career pathways for cybersecurity work roles that can be used in the private and public sectors.

(2) REQUIREMENTS.—The Director of the National Institute of Standards and Technology shall ensure that the multiple cybersecurity career pathways identified under paragraph (1) indicate the knowledge, skills, and abilities, including relevant education, training, internships, 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) EXCHANGE PROGRAM.—Consistent with requirements under chapter 37 of title 5, United States Code, the Director of the National Institute of Standards and Technology, in coordination with the Director of the Office of Personnel Management, may establish a voluntary program for the exchange of employees engaged in one of the cybersecurity work roles identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework, between the National Institute of Standards and Technology and

private sector institutions, including nonpublic or commercial businesses, research institutions, or institutions of higher education, as the Director of the National Institute of Standards and Technology considers feasible.

(d) PROFICIENCY TO PERFORM CYBERSECURITY TASKS.—In carrying out subsection (a) of such section, the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Homeland Security, and other appropriate agencies—

(1) assess the scope and sufficiency of efforts to measure an individual'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) not later than 540 days after the date of the enactment of this Act, 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 of the Office of Management and Budget may seek input from the Director of the National Institute of Standards and Technology, in coordination with the Department of Homeland Security, the Office of Personnel Management, and such agencies as the Director of the National Institute of Standards and Technology considers relevant, to develop quantifiable metrics for 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, 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, including in-kind 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 therefore

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) An identification of, or a plan to establish, a multistakeholder 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 academic institutions in the Federal Cyber Scholarships for Service, National Centers of Academic Excellence in Cybersecurity program or advanced technological education programs, as well as 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 multi-stakeholder 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, externships, apprenticeships, or cooperative education programs in conjunction with providers of education and training. Inclusion of programs that seek to include veterans and underrepresented groups, including women, minorities, persons from rural and underserved areas, and persons with disabilities, is encouraged.

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

"(C) PRIORITY CONSIDERATION.—In awarding financial assistance under paragraph (3), 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 received 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 participated 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 (5 U.S.C. 301 note) 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''.

(B) Section 2(c)(3) of the NIST Small Business Cybersecurity Act (15 U.S.C. 272 note) 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''.

(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.'';

(3) in subsection (f)—

(A) in paragraph (4), by striking ''; and'' and inserting a semicolon; and

(B) by striking paragraph (5) and inserting the following:

''(5) enter into an agreement accepting and acknowledging the post award employment obligations, pursuant to section (d);

''(6) accept and acknowledge the conditions of support under section (g); and

''(7) accept all terms and conditions of a scholarship under this section.'';

(4) in subsection (g)—

(A) in paragraph (1), by inserting ''the Office of Personnel Management, in coordination with the National Science Foundation, and'' before ''the qualified institution''; and

(B) in paragraph (2)—

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

(ii) by striking subparagraph (E) and inserting the following:

''(E) fails to maintain or fulfill any of the post-graduation or post-award obligations or requirements of the individual; or

''(F) fails to fulfill the requirements of paragraph (1).'';

(5) in subsection (h)(2), by inserting ''and the Director of the Office of Personnel Management'' after ''Foundation'';

(6) in subsection (k)(1)(A), by striking ''and the Director'' and all that follows and inserting '', the Director of the National Science Foundation, and the Director of the Office of Personnel Management of the amounts owed; and''; and

(7) 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 ''once every 3 years'' and all that follows and inserting ''once every 2 years, to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Science, Space, and Technology and the Committee on Oversight and Reform of the House of Representatives a report, including—

''(A) the results of the evaluation under paragraph (1);

''(B) the disparity in any reporting between scholarship recipients and their respective institutions of higher education; and

''(C) any recent statistics regarding the size, composition, and educational requirements of the Federal cybersecurity workforce.''.

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) 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 WORKFORCE DEVELOPMENT AT THE DEPARTMENT OF ENERGY.

(a) IN GENERAL.—The Secretary of Energy shall support the development of a cybersecurity workforce through a program that—

(1) facilitates collaboration between under-graduate and graduate students, researchers at the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005), and the private sector;

(2) prioritizes science and technology in areas relevant to the mission of the Department of Energy through the design and application of cybersecurity technologies;

(3) develops, or facilitates private sector development of, voluntary cybersecurity training and retraining standards, lessons, and recommendations

for the energy sector that minimize duplication of cybersecurity compliance training programs; and

(4) maintains a public database of cybersecurity education, training, and certification programs.

(b) COLLABORATION.—In carrying out the program authorized in subsection (a), the Secretary of Energy shall leverage programs and activities carried out across the Department of Energy, other relevant Federal agencies, institutions of higher education, and other appropriate entities best suited to provide national leadership on cybersecurity related issues.

SEC. 8. NATIONAL CYBERSECURITY CHALLENGES.

(a) IN GENERAL.—Title II of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7431 et seq.) is amended by adding at the end the following:

"SEC. 205. NATIONAL CYBERSECURITY CHALLENGES.

"(a) ESTABLISHMENT OF NATIONAL CYBERSECURITY CHALLENGES.—

"(1) IN GENERAL.—To achieve high-priority breakthroughs in cybersecurity by 2028, the Director of the National Institutes of Standards and Technology shall establish the following national cybersecurity challenges:

"(A) ECONOMICS OF A CYBER ATTACK.—Building more resilient systems that measur-

ably and exponentially raise adversary costs of carrying out common cyber attacks.

"(B) CYBER TRAINING.—

"(i) Empowering the people of the United States with an appropriate and measurably sufficient level of digital literacy to make safe and secure decisions online.

"(ii) Developing a cybersecurity workforce with measurable skills to protect and maintain information systems.

"(C) EMERGING TECHNOLOGY.—Advancing cybersecurity efforts in response to emerging technology, such as artificial intelligence, quantum science, and next generation communications technologies.

"(D) REIMAGINING DIGITAL IDENTITY.—Maintaining a high sense of usability while improving the privacy, security and safety of online activity of individuals in the United States.

"(E) FEDERAL AGENCY RESILIENCE.—Reducing cybersecurity risks to Federal networks and systems, and improving the response of Federal agencies to cybersecurity incidents on such networks and systems.

''(2) COORDINATION.—In establishing the challenges under paragraph (1), the Director of the National Institutes of Standards and Technology shall coordinate with the Secretary of Homeland Security on the challenges under subparagraphs (B) and (E) of such paragraph.

''(b) PURSUIT OF NATIONAL CYBERSECURITY CHALLENGES.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Director of the National Institutes of Standards and Technology, shall commence efforts to pursue the national cybersecurity challenges established under subsection (a).

''(2) COMPETITIONS.—The efforts required by paragraph (1) shall include carrying out programs to award prizes, including cash and noncash prizes, competitively pursuant to the authorities and processes established under section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) or any other applicable provision of law.

''(3) ADDITIONAL AUTHORITIES.—In carrying out paragraph (1), the Director of the National Institutes of Standards and Technology may enter into

and perform such other transactions as the Director considers necessary and on such terms as the Director considers appropriate.

''(4) COORDINATION.—In pursuing national cybersecurity challenges under paragraph (1), the Director of the National Institutes of Standards and Technology shall coordinate with the following:

''(A) The Director of the National Science Foundation.

''(B) The Secretary of Homeland Security.

''(C) The Director of the Defense Advanced Research Projects Agency.

''(D) The Director of the Office of Science and Technology Policy.

''(E) The Director of the Office of Management and Budget.

''(F) The heads of such other Federal agencies as the Secretary of Commerce considers appropriate for purposes of this section.

''(5) SOLICITATION OF ACCEPTANCE OF FUNDS.—

''(A) IN GENERAL.—Pursuant to section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719), the Director of the National Institutes of Standards and

Technology shall request and accept funds from other Federal agencies, State, United States territory, local, or tribal government agencies, private sector for-profit entities, and nonprofit entities to support efforts to pursue a national cybersecurity challenge under this section.

''(B) RULE OF CONSTRUCTION.—Nothing in subparagraph (A) shall be construed to require any person or entity to provide funds or otherwise participate in an effort or competition under this section.

''(c) RECOMMENDATIONS.—

''(1) IN GENERAL.—In carrying out this section, the Director of the National Institutes of Standards and Technology shall designate an advisory council to seek recommendations.

''(2) ELEMENTS.—The recommendations required by paragraph (1) shall include the following:

''(A) A scope for efforts carried out under subsection (b).

''(B) Metrics to assess submissions for prizes under competitions carried out under subsection (b) as the submissions pertain to the national cybersecurity challenges established under subsection (a).

''(3) NO ADDITIONAL COMPENSATION.—The Director of the National Institutes of Standards and Technology may not provide any additional compensation, except for travel expenses, to a member of the advisory council designated under paragraph (1) for participation in the advisory council.''.

(b) CONFORMING AMENDMENTS.—Section 201(a)(1) of such Act is amended—

(1) in subparagraph (J), by striking ''; and'' and inserting a semicolon;

(2) by redesignating subparagraph (K) as subparagraph (L); and

(3) by inserting after subparagraph (J) the following:

''(K) implementation of section 205 through research and development on the topics identified under subsection (a) of such section; and''.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 204 the following:

''Sec. 205. National cybersecurity challenges.''.

○