AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 515

116TH CONGRESS *2d Session*	SENATE	REPORT 116–254

HARVESTING AMERICAN CYBERSECURITY KNOWLEDGE THROUGH EDUCATION ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 2775

AUGUST 12, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
99–010 WASHINGTON : 2020

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER F. WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD C. YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD J. MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY C. PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
DAVID STRICKLAND, *Minority Staff Director*

Calendar No. 515

116TH CONGRESS, *2d Session* | SENATE | REPORT 116–254

HARVESTING AMERICAN CYBERSECURITY KNOWLEDGE THROUGH EDUCATION ACT OF 2019

AUGUST 12, 2020.—Ordered to be printed

Mr. WICKER, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 2775]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2775) to improve the cyber workforce of the United States, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The Harvesting American Cybersecurity Knowledge through Education (HACKED) Act of 2019 is intended to improve the cybersecurity workforce of public and private sectors.

BACKGROUND AND NEEDS

Cybersecurity risks impact the United States' economic and national security. The cost of malicious cyber activity to the U.S. economy in 2016 is estimated at $57 billion to $109 billion.[1] In addition, the U.S. Government Accountability Office declared cybersecurity as a "high risk issue" given the threats to Federal networks, the Nation's critical infrastructure, and personal information of in-

[1] The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018 (*https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf*) (accessed Apr. 17, 2020).

dividuals.[2] Despite the growing cybersecurity risks facing the United States, the government and private sector are facing a shortage of cybersecurity workers. According to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), as of 2018, there are more than 300,000 unfilled cybersecurity jobs in the United States. It is projected there will be 500,000 total unfilled positions by 2021.[3] [4] In addition, a recent survey by the International Information Security Certification Consortium (ISC)[2], a cybersecurity professionals organization, found that 63 percent of industry faces a shortage of cybersecurity employees.[5]

In response to the 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[6] the Department of Commerce (DOC) and Department of Homeland Security (DHS) issued a report [7] with recommendations to improve the cybersecurity workforce in the public and private sectors. The report issued a number of findings, including the following:

- The United States needs immediate and sustained improvements in its cybersecurity workforce situation.
- Employers increasingly are concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations.
- Expanding the pool of cybersecurity candidates by retraining those employed in non-cybersecurity fields and by increasing the participation of women, minorities, and veterans as well as students in primary through secondary school is needed and represents significant opportunities.
- There is an apparent shortage of knowledgeable and skilled cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors.
- Hiring considerations—including lengthy security clearance delays and onboarding processes—severely affect the sufficiency of the cybersecurity workforce.
- Comprehensive and reliable data about cybersecurity workforce position needs and education and training programs is lacking—even though the general context and urgency of the situation are obvious.

The report also included a number of recommended actions, many of which are required by the May 2019 Executive Order on America's Cybersecurity Workforce.[8] Several recommendations, including improvements to align education and training with employers' cybersecurity workforce needs by applying the NICE Workforce Framework, developing cybersecurity career model paths, and authorizing Multistakeholder Regional Alliances are included in this legislation.

---

[2] U.S. Government Accountability Office, "Cybersecurity Challenges Facing the Nation—High Risk Issue" (*https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary#t=0*) (accessed Apr. 17, 2020).

[3] CyberSeek, "Cybersecurity Supply/Demand Heat Map" (*https://www.cyberseek.org/heatmap.html*).

[4] U.S. Bureau of Labor Statistics, "Employment by Detailed Occupation" (*https://www.bls.gov/emp/tables/emp-by-detailed-occupation.htm*) (accessed Apr. 17, 2020).

[5] (ISC)[2], "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," 2018 (*www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D 0FB51698D9BA6BF13EEABFA48BD17DB0*) (accessed Apr. 17, 2020).

[6] Executive Order 13800, 82 FR 22391 (2017).

[7] U.S. Department of Commerce and U.S. Department of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," May 10, 2018. p. 2 (*https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/supporting-growth-and-sustainment-of-the-cybersecurity-workforce/final*) (accessed Apr. 17, 2020).

[8] Executive Order 13870, 84 FR 20523 (2019).

NICE, led by the National Institute of Standards and Technology (NIST), serves as the lead for working with the government and public sectors on issues pertaining to cybersecurity education, training, and workforce development. NICE developed the NICE Cybersecurity Workforce Framework (NIST Special Publication 800–181), "a national focused resource that categorizes and describes cybersecurity work".[9] Similar to the well-known Framework for Improving Critical Infrastructure Cybersecurity, the NICE Framework establishes common taxonomy and definitions for cybersecurity work, which is intended to be used by public, private, and academic sectors. NIST also convenes Federal agencies, through the NICE Interagency Coordinating Council, to coordinate Federal programs related to cybersecurity workforce,[10] which would be enhanced under this legislation. The May 2019 Executive Order on America's Cybersecurity Workforce encouraged the adoption of the NICE Framework by both the private and public sectors.

In October, the Office of Science and Technology Policy (OSTP) reported that there are more than 100 Federal programs for STEM education with a budget of over $3.2 billion.[11] These programs focus broadly on STEM education, but only a few focus on cybersecurity. The National Security Agency and the Department of Homeland Security designate 2-year, 4-year, and graduate-level schools as Centers of Academic Excellence (CAE) with three types of cyber designations (cyber defense education, cyber defense research, and cyber operations). There are currently over 270 CAEs across 48 States, 9 of which hold all 3 designations.[12] The National Science Foundation (NSF) CyberCorps Scholarship-for-Service program provides scholarships to students in exchange for service after graduation in a Federal, State, local, or Tribal government organization for a period equal to the length of the scholarship. Over 3,000 students have entered the CyberCorps program since it began in 2011, and have been placed in more than 140 Federal agencies and departments.[13] The program was last amended by the National Defense Authorization Act for Fiscal Year 2018,[14] which directed a pilot program to expand the scholarships to community colleges. Despite the growing need for cybersecurity professionals, there is a shortage of skilled cybersecurity educators. The Computing Research Association estimates that in 2018 only 14 of the approximately 100 Ph.D. graduates secured tenure-track jobs in aca-

---

[9] National Institute of Standards and Technology, "NICE Cybersecurity Workforce Framework" (*https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*) (accessed Apr. 17, 2020).

[10] National Institute of Standards and Technology, "NICE Interagency Coordinating Council" (ICC) (*https://www.nist.gov/itl/applied-cybersecurity/nice/about/interagency-coordinating-council*) (accessed Apr. 17, 2020).

[11] Office of Science and Technology Policy, "Progress Report on the Federal Implementation of the STEM Education Strategic Plan," October 2019 (*https://www.whitehouse.gov/wp-content/uploads/2019/10/Progress-Report-on-the-Federal-Implementation-of-the-STEM-Education-Strategic-Plan.pdf*) (accessed Apr. 17, 2020).

[12] CAE in Cybersecurity Community, "CAE Institution Map" (*https://www.caecommunity.org/content/cae-institution-map*) (accessed Apr. 17, 2020).

[13] CyberCorps Scholarship for Service, "History/Overview" (*https://www.sfs.opm.gov/Overview-History.aspx*) (accessed Apr. 17, 2020).

[14] Pub. L. 115–91.

demia.[15] Further, half of 2-year CAE designated schools have current vacancies for cybersecurity faculty.[16]

SUMMARY OF PROVISIONS

The legislation would amend science education and cybersecurity programs at NIST, NSF, the National Aeronautics and Space Administration (NASA), and the U.S. Department of Transportation (DOT). Specifically, it would do the following:

- Incentivize recruitment of cybersecurity teachers by expanding the NSF CyberCorps Scholarship-for-Service to allow for students to fulfill their service obligation as teachers. Currently the program requires government employment. It would also support cybersecurity camps for K–12 students and teachers.
- Align education and training with cybersecurity workforce needs by authorizing Regional Alliances and Multistakeholder Partnerships to fund partnerships between local employers with educational institutions to fill local cybersecurity workforce needs and directing the improvement of metrics to track and measure cybersecurity workforce needs across the Nation. It would also amend NSF, NASA, and DOT education programs to include cybersecurity as an explicit component.
- Design clear paths in the cybersecurity workforce and educate Federal employees by identifying model career paths for various cybersecurity work roles; identifying tools for assessing skills and capabilities of workers; conducting research on the integration of computer science and cybersecurity; and developing standards on cybersecurity awareness for Federal agencies.
- Increase coordination in Federal cyber workforce programs by directing an existing OSTP interagency working group to coordinate Federal cyber workforce programs and codify NIST as the agency responsible for leading interagency efforts on such coordination.

LEGISLATIVE HISTORY

S. 2775 was introduced on November 5, 2019, by Senator Wicker (for himself and Senators Cantwell, Thune, and Rosen) and was referred to the Committee on Commerce, Science, and Transportation of the Senate. On November 13, 2019, the Committee met in open Executive Session and, by voice vote, ordered S. 2775 reported favorably with an amendment. The Committee approved an amendment from Senators Thune, Klobuchar, and Rosen which would require the Director of NIST to establish a voluntary cybersecurity exchange program.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget

---

[15] Stuart Zweben and Betsy Bizot, "2018 Taulbee Survey, Undergrad Enrollment Continues Upward; Doctoral Degree Production Declines but Doctoral Enrollment Rises" (*https://cra.org/wp-content/uploads/2019/05/2018_Taulbee_Survey.pdf*) (accessed Apr. 17, 2020).

[16] Alicia Modestino and Walter McHugh, *Educator Shortage Problem Found in the 2017 CAE Cybersecurity Survey* (*https://aliciasassermodestino.com/wp-content/uploads/2019/04/2018-NAS-Cybersecurity-Survey-Report-1.pdf*) (accessed May 5, 2020).

Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 2775, HACKED Act of 2019

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on November 13, 2019

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	57	not estimated

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

*= between zero and $500,000.

S. 2775 would require the National Institute of Standards and Technology (NIST) to expand its efforts under the National Initiative for Cybersecurity Education. The bill would require the agency to coordinate federal research on the skills cybersecurity workers need in critical infrastructure sectors and to measure the effectiveness of federal programs directed at expanding and advancing the cybersecurity workforce. The bill also would require NIST to identify career pathways for cybersecurity professionals in government and private industry. Under S. 2775, NIST would award grants each year to entities to form public-private partnerships to expand and advance the cybersecurity workforce at the local level.

CBO estimates that implementing S. 2775 would cost $57 million over the 2020–2025 period, assuming appropriation of the estimated amounts. The costs of the bill, detailed in Table 1, fall within budget function 370 (commerce and housing credit).

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2020. Under that assumption, the agency could incur some costs in 2020, but CBO expects that most of the costs would be incurred in 2021 and later.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 2775

	By fiscal year, millions of dollars—						
	2020	2021	2022	2023	2024	2025	2020–2025
Total Changes							
Estimated Authorization	*	15	13	14	14	15	71
Estimated Outlays	*	6	10	13	14	14	57

* = between zero and $500,000.

Using information from NIST, CBO estimates the agency would obligate about $10 million in grants each year beginning in 2021 (the equivalent of a $200,000 grant in each state) and that related administrative costs would be about $2 million a year. CBO expects

that the grants would outlay within a few years of obligation. In total, CBO estimates that providing grants and administering the new program would cost about $50 million over the 2020–2025 period. In addition, CBO estimates that it would cost NIST about $7 million over the 2020–2025 period to hire scientists, engineers, and contractors to fulfill other requirements under the bill related to improving the cybersecurity workforce.

The bill would direct several other federal agencies to advance cybersecurity research, education, and workforce development efforts. CBO estimates that any additional costs incurred by those agencies to fulfill the bill's requirements would be insignificant.

The CBO staff contact for this estimate is David Hughes. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

S. 2775 would amend a number of existing programs at NIST, NSF, NASA, and DOT, which involve grants and cooperative agreements with academia and industry. However, the bill would not authorize any new regulations and therefore would not subject any individuals or organizations to new regulations.

ECONOMIC IMPACT

S. 2775 is not expected to have an adverse impact on the Nation's economy as it is expected to improve cybersecurity workforce-related jobs in the public and private sectors.

PRIVACY

S. 2775 is not expected to have an impact on the personal privacy of individuals.

PAPERWORK

S. 2775 would require NICE to submit a report to Congress on the scope and sufficiency of efforts to measure cybersecurity learners capabilities to perform specific cybersecurity tasks at all proficiency levels. The bill would also require participants in the regional multistakeholder alliance cooperative agreements to submit reports on efforts under the program.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section would provide that the bill may be cited as the "Harvesting American Cybersecurity Knowledge through Education Act of 2019" or "HACKED Act of 2019".

Section 2. Improving national initiative for cybersecurity education

This section would make a series of amendments to NICE within NIST. The section would direct NIST to coordinate interagency efforts to identify cybersecurity workforce skill gaps in public and private sectors, coordinate existing Federal cybersecurity workforce programs, promote the National Security Agency and DHS designated National Centers of Academic Excellence in Cybersecurity, consider needs for cybersecurity workforce in critical infrastructure, and develop metrics for measuring the effectiveness of current cybersecurity workforce programs and initiatives. This section would also establish a voluntary talent exchange of cybersecurity employees between NIST and private sector or research institutions, as the Director considers feasible. In carrying out the NICE effort, this section would direct a report identifying multiple cybersecurity career pathways in private and public sectors, including noncompetitive hiring pathways in the Federal Government and evaluation of efforts to measure proficiency to perform cybersecurity tasks.

The section would further authorize Regional Alliances and Multistakeholder Partnerships to address the workforce needs of local communities in order to support job driven education and training programs. The section would define the requirements for the cooperative agreements including outlining eligible regional alliances, which must include at least one institution of higher education or nonprofit training organization and at least one local employer or owner or operator of critical infrastructure. It would also cap each regional alliance award at $200,000 and require awardees to provide a non-Federal contribution. The section would require that the regional alliances leverage the objectives of the NICE program and encourage programs that seek to include women, minorities, or veterans.

Section 3. Development of standards and guidelines for improving cybersecurity workforce of Federal agencies

This section would direct NIST to identify, develop, and publish standards for improving the cybersecurity workforce for Federal agencies as part of the NICE Cybersecurity Workforce Framework. It would also direct NIST to issue cybersecurity awareness standards and guidelines for use by Federal agencies.

Section 4. Modifications to Federal Cyber Scholarship-for-Service program

This section would amend the NSF Scholarship-for-Service program (also called "CyberCorps scholarships") to grow the number of cybersecurity educators. It would allow up to 10 percent of the scholarship recipients to fulfill their service obligation as an educator in a Cybercorps school. Currently, the program requires that scholarship recipients agree to work after graduation for a govern-

ment agency for a period equal to the length of their scholarship. The section would direct that cybersecurity summer camps, including teacher training, be carried out as part of the scholarship program.

Section 5. Cybersecurity in programs of the National Science Foundation

This section would ensure cybersecurity is addressed in existing NSF STEM programs, including computer science education research, the Advanced Technological Education program, Low-income Scholarship Program, and the Graduate Research Fellowship Program. It would also direct research on the integration of cybersecurity into computer science education and ensure that educators and mentors in fields relating to cybersecurity be considered for Presidential Awards for Excellence in Mathematics and Science Teaching and for Excellence in STEM.

Section 6. Cybersecurity in STEM programs of the National Aeronautics and Space Administration

This section would encourage cybersecurity education opportunities in existing STEM programs at NASA.

Section 7. Cybersecurity in Department of Transportation programs

This section would amend the DOT University Transportation Centers program to conduct research on transportation cybersecurity, including research on cybersecurity implications associated with autonomous vehicles, connected vehicles, and critical infrastructure. It would also require the Secretary of Transportation to include reducing transportation cybersecurity risks as part of the 5-year strategic research and development plan.

Section 8. Coordination of Federal cybersecurity workforce

This section would improve coordination of Federal cybersecurity workforce programs by establishing or designating a subcommittee on cybersecurity workforce within the existing Committee on Science, Technology, Engineering, and Math Education (otherwise referred to as the CoSTEM Committee). The section would designate the directors of OSTP and NIST as the co-chairs of the subcommittee.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 49—TRANSPORTATION

Subtitle III—General and Intermodal Programs

CHAPTER 55—INTERMODAL TRANSPORTATION

Subchapter I—General

* * * * * * *

§ 5505. University transportation centers program

(a) UNIVERSITY TRANSPORTATION CENTERS PROGRAM.—

(1) ESTABLISHMENT AND OPERATION.—The Secretary shall make grants under this section to eligible nonprofit institutions of higher education to establish and operate university transportation centers.

(2) ROLE OF CENTERS.—The role of each university transportation center referred to in paragraph (1) shall be—

(A) to advance transportation expertise and technology in the varied disciplines that comprise the field of transportation through education, research, and technology transfer activities;

(B) to provide for a critical transportation knowledge base outside of the Department of Transportation; and

(C) to address critical workforce needs and educate the next generation of transportation leaders *in the matters described in subparagraphs (A) through (G) of section 6503(c)(1)*.

(b) * * *

(c) GRANTS.—

(1) * * *

(2) * * *

(3) REGIONAL UNIVERSITY TRANSPORTATION CENTERS.—

(A) * * *

(B) * * *

(C) * * *

(D) * * *

(E) FOCUSED RESEARCH.—**[**The Secretary**]**

(i) 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).

(ii) FOCUSED OBJECTIVES.—The Secretary shall make a grant to 1 of the 10 regional university transportation centers established under this paragraph for the purpose of furthering the objectives described in subsection (a)(2) in the field of comprehensive transportation safety, congestion, connected vehicles, connected infrastructure, and autonomous vehicles*, including the cybersecurity implications of technologies*

relating to connected vehicles, connected infrastructure, and autonomous vehicles.

* * * * * * *

CHAPTER 65—RESEARCH PLANNING

* * * * * * *

§ 6503. Transportation research and development 5-year strategic plan

(a) * * *
(b) * * *
(c) CONTENTS.—The strategic plan developed under subsection (a) shall—

(1) describe how the plan furthers the primary purposes of the transportation research and development program, which shall include—

(A) improving mobility of people and goods;
(B) reducing congestion;
(C) promoting safety;
(D) improving the durability and extending the life of transportation infrastructure;
(E) preserving the environment; [and]
(F) preserving the existing transportation system; *and*
(G) reducing transportation cybersecurity risks;

* * * * * * *

AMERICA COMPETES REAUTHORIZATION ACT OF 2010

[42 U.S.C. 6621; as amended through Pub. L. 114–329]

SEC. 101. COORDINATION OF FEDERAL STEM EDUCATION.

(a) ESTABLISHMENT.—The Director shall establish a committee under the National Science and Technology Council, including the Office of Management and Budget, with the responsibility to coordinate Federal programs and activities in support of STEM education, including at the National Science Foundation, the Department of Energy, the National Aeronautics and Space Administration, *the National Institute of Standards and Technology,* the National Oceanic and Atmospheric Administration, the Department of Education, and all other Federal agencies that have programs and activities in support of STEM education.

(b) RESPONSIBILITIES.—The committee established under subsection (a) shall—

(1) coordinate the STEM education activities and programs of the Federal agencies;

(2) coordinate STEM education activities and programs with the Office of Management and Budget;

(3) encourage the teaching of innovation and entrepreneurship as part of STEM education activities;

(4) review STEM education activities and programs to ensure they are not duplicative of similar efforts within the Federal government;

(5) develop, implement through the participating agencies, and update once every 5 years a 5-year STEM education strategic plan, which shall—

(A) specify and prioritize annual and long-term objectives;

(B) specify the common metrics that will be used to assess progress toward achieving the objectives;

(C) describe the approaches that will be taken by each participating agency to assess the effectiveness of its STEM education programs and activities; and

(D) with respect to subparagraph (A), describe the role of each agency in supporting programs and activities designed to achieve the objectives;

(6) establish, periodically update, and maintain an inventory of federally sponsored STEM education programs and activities, including documentation of assessments of the effectiveness of such programs and activities and rates of participation by women, underrepresented minorities, and persons in rural areas in such programs and activities;

(7) collaborate with the STEM Education Advisory Panel established under section 303 of the American Innovation and Competitiveness Act and other outside stakeholders to ensure the engagement of the STEM education community;

(8) review the measures used by a Federal agency to evaluate its STEM education activities and programs;

(9) request and review feedback from States on how the States are utilizing Federal STEM education programs and activities; and

(10) recommend the reform, termination, or consolidation of Federal STEM education activities and programs, taking into consideration the recommendations of the STEM Education Advisory Panel.

(c) RESPONSIBILITIES OF OSTP.—The Director shall encourage and monitor the efforts of the participating agencies to ensure that the strategic plan under subsection (b)(5) is developed and executed effectively and that the objectives of the strategic plan are met.

(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.

[(d)] *(e)* REPORTS.—The Director shall transmit a report annually to Congress at the time of the President's budget request describing the plan required under subsection (b)(5). The annual report shall include—

(1) a description of the STEM education programs and activities for the previous and current fiscal years, and the proposed programs and activities under the President's budget request, of each participating Federal agency;

(2) the levels of funding for each participating Federal agency for the programs and activities described under paragraph (1) for the previous fiscal year and under the President's budget request;

(3) an evaluation of the levels of duplication and fragmentation of the programs and activities described under paragraph (1);

(4) except for the initial annual report, a description of the progress made in carrying out the implementation plan, including a description of the outcome of any program assessments completed in the previous year, and any changes made to that plan since the previous annual report;

(5) a description of how the participating Federal agencies will disseminate information about federally supported resources for STEM education practitioners, including teacher professional development programs, to States and to STEM education practitioners, including to teachers and administrators in schools that meet the criteria described in subsection (c)(1)(A) and (B) of section 7381j of this title;

(6) a description of all consolidations and terminations of Federal STEM education programs and activities implemented in the previous fiscal year, including an explanation for the consolidations and terminations;

(7) recommendations for reforms, consolidations, and terminations of STEM education programs or activities in the upcoming fiscal year; and

(8) a description of any significant new STEM education public-private partnerships.

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

* * * * * * *

AMERICAN COMPETITIVENESS AND WORKFORCE IMPROVEMENT ACT OF 1998

[42 U.S.C. 1869c]

SEC. 414. * * *

(a) * * *

(b) * * *

(c) * * *

(d) LOW-INCOME SCHOLARSHIP PROGRAM.—

(1) ESTABLISHMENT.—The Director of the National Science Foundation (referred to in this section as the "Director") shall award scholarships to low-income individuals to enable such individuals to pursue associate, undergraduate, or graduate level degrees in mathematics, engineering, [or computer science] *computer science, or cybersecurity*.

(2) ELIGIBILITY.—

(A) IN GENERAL.—To be eligible to receive a scholarship under this section, an individual—

(i) * * *

(ii) * * *

(iii) shall certify to the Director that the individual intends to use amounts received under the scholarship to enroll or continue enrollment at an institution of higher education (as defined in section 101(a) of the Higher Education Act of 1965) in order to pursue an associate, undergraduate, or graduate level degree in mathematics, engineering, computer science, *cybersecurity,* or other technology and science programs designated by the Director.

* * * * * * *

AMERICAN INNOVATION AND COMPETITIVENESS ACT

[42 U.S.C. 1862s–7; Pub. L. 114–329]

SEC. 310. COMPUTER SCIENCE EDUCATION RESEARCH.

(a) FINDINGS.—Congress finds that as the lead Federal agency for building the research knowledge base for computer science education, the Foundation is well positioned to make investments that will accelerate ongoing efforts to enable rigorous and engaging computer science throughout the Nation as an integral part of STEM education.

(b) GRANT PROGRAM.—

(1) IN GENERAL.—The Director of the Foundation shall award grants to eligible entities to research computer science *and cybersecurity* education and computational thinking.

(2) RESEARCH.—The research described in paragraph (1) may include the development or adaptation, piloting or full implementation, and testing of—

(A) models of preservice preparation for teachers who will teach computer science and computational thinking;

(B) scalable and sustainable models of professional development and ongoing support for the teachers described in subparagraph (A);

(C) tools and models for teaching and learning aimed at supporting student success and inclusion in computing within and across diverse populations, particularly poor, rural, and tribal populations and other populations that have been historically underrepresented in computer science and STEM fields**[**; and**]***;*

(D) high-quality learning opportunities for teaching computer science and, especially in poor, rural, or tribal schools at the elementary school and middle school levels, for integrating computational thinking into STEM teaching and learning**[**.**]***; and*

(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.

(c) COLLABORATIONS.—In carrying out the grants established in subsection (b), eligible entities may collaborate and partner with local or remote schools to support the integration of computing *, cybersecurity,* and computational thinking within pre-kindergarten through grade 12 STEM curricula and instruction.

* * * * * * *

CYBERSECURITY ENHANCEMENT ACT OF 2014

[15 U.S.C. 7451; Pub. L. 113–274]

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cybersecurity Enhancement Act of 2014".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

* * * * * * *

* * * * * * *

[15 U.S.C. 7442; as amended through Pub. L. 115–91]

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

SEC. 301. * * *

SEC. 302. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) * * *

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The Federal Cyber Scholarship-for-Service Program shall—

(1) provide scholarships through qualified institutions of higher education, including community colleges, to students who are enrolled in programs of study at institutions of higher education leading to degrees or specialized program certifications in the cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal [information technology] *information technology and cybersecurity* workforce;

[(3) prioritize the employment placement of at least 80 percent of scholarship recipients in an executive agency (as defined in section 105 of title 5, United States Code); and]

(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

(4) provide awards to improve cybersecurity education *, 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,* at the kindergarten through grade 12 level—

(A) to increase interest in cybersecurity careers;

(B) to help students practice correct and safe online behavior and understand the foundational principles of cybersecurity;

(C) to improve teaching methods for delivering cybersecurity content for kindergarten through grade 12 computer science curricula; and

(D) to promote teacher recruitment in the field of cybersecurity.

(d) POST-AWARD EMPLOYMENT OBLIGATIONS.—Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work for a period equal to the length of the scholarship, following receipt of the student's degree, in the cybersecurity mission of—

(1) an executive agency (as defined in section 105 of title 5, United States Code);

(2) Congress, including any agency, entity, office, or commission established in the legislative branch;

(3) an interstate agency;

(4) a State, local, or Tribal government; **[**or**]**

(5) a State, local, or Tribal government-affiliated nonprofit that is considered to be critical infrastructure (as defined in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e))**[**.**]***; or*

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

(e) * * *

(f) ELIGIBILITY.—To be eligible to receive a scholarship underthis section, an individual shall—

(1) be a citizen or lawful permanent resident of the United States;

(2) demonstrate a commitment to a career in improving the security of information technology;

(3) have demonstrated a high level of competency in relevant knowledge, skills, and abilities, as defined by the national cybersecurity awareness and education program **[**under section 401**]** *under section 303*;

(4) be a full-time student in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation, except that in the case of a student who is enrolled in a community college, be a student pursuing a degree on a less than full-time basis, but not less than half-time basis; and

(5) accept the terms of a scholarship under this section.

(g) * * *

(h) * * *

(i) * * *

(j) * * *

(k) * * *

(l) * * *

(m) PUBLIC INFORMATION.—

(1) EVALUATION.—The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall periodically evaluate and make public, in a manner that protects the personally identifiable information of scholarship recipients, information on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector **[**cyber**]** *cybersecurity* workforce, including information on—

(A) * * *

(1) * * *

(2) REPORTS.—The Director of the National Science Foundation, in coordination with the Office of Personnel Management, shall submit, not less frequently than once every 3 years, to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report, including the results of the evaluation under paragraph (1) and any recent

statistics regarding the size, composition, and educational requirements of the Federal [cyber] *cybersecurity* workforce.

* * * * * * *

[NOTE: Title IV—Cybersecurity Awareness and Preparedness is repealed. Section 401 is transferred to the end of title III of such Act and redesignated as section 303.]

SEC. [401.] *303.* **NATIONAL CYBERSECURITY AWARENESS AND EDUCATION PROGRAM.**

(a) NATIONAL CYBERSECURITY AWARENESS AND EDUCATION PROGRAM.—The Director of the National Institute of Standards and Technology (referred to in this section as the "Director"), in consultation with appropriate Federal agencies, industry, educational institutions, National Laboratories, the Networking and Information Technology Research and Development program, and other organizations shall continue to coordinate a national cybersecurity awareness and education program, that includes activities such as—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Director;

(2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, educational institutions, and State, local, and tribal governments;

(3) increasing public awareness of cybersecurity, cyber safety, and cyber ethics;

(4) increasing the understanding of State, local, and tribal governments, institutions of higher education, and private sector entities of—

(A) the benefits of ensuring effective risk management of information technology versus the costs of failure to do so; and

(B) the methods to mitigate and remediate vulnerabilities;

(5) supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government[; and]*;*

(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

[(6)] *(11)* promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.

(b) * * *

(c) STRATEGIC PLAN.—[The Director]

(1) IN GENERAL.—The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of the date of enactment of this Act to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and education program under subsection (a).

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

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, and every 5 years thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(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.—

(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 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 Federal Cyber Scholarships for Service organizations, National Centers of Academic Excellence in Cybersecurity, advanced technological 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 paragraph (3)(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 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.

* * * * * * *

FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT ACT OF 2015

[Pub. L. 114–113]

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

SEC. 301. SHORT TITLE.

This title may be cited as the "Federal Cybersecurity Workforce Assessment Act of 2015".

SEC. 302. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Commerce, Science, and Transportation of the Senate;

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Oversight and Government Reform of the House of Representatives; and

(H) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) DIRECTOR.—The term "Director" means the Director of the Office of Personnel Management.

(3) NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION.—The term "National Initiative for Cybersecurity Education" means the initiative under the national cybersecurity awareness and education program, as authorized [under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)] *under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)*.

(4) WORK ROLES.—The term " work roles" means a specialized set of tasks and functions requiring specific knowledge, skills, and abilities.

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

[15 U.S.C. 278g–3(a)]

SEC. 20. (a) The Institute shall—

(1) * * *

(2) * * *

(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all

agency operations and assets, but such standards and guidelines shall not apply to national security systems[; and]*;*

(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division[.]*; and*

(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.

* * * * * * *

NIST SMALL BUSINESS CYBERSECURITY ACT

[Pub. L. 115–236]

SEC. 2. IMPROVING CYBERSECURITY OF SMALL BUSINESSES.

(a) * * *

(b) * * *

(c) DISSEMINATION OF RESOURCES FOR SMALL BUSINESSES.—

(1) * * *

(2) * * *

(3) NATIONAL CYBERSECURITY AWARENESS AND EDUCATION PROGRAM.—The Director shall ensure that the resources disseminated under paragraph (1) are consistent with the efforts of the Director [under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)] *under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)*.

* * * * * * *

SCIENTIFIC AND ADVANCED-TECHNOLOGY ACT OF 1992

[42 U.S.C. 1862i(j)(9)]

SEC. 3. SCIENTIFIC AND TECHNICAL EDUCATION.

(a) * * *

(b) * * *

(c) * * *

(d) * * *

(e) * * *

(f) * * *

(g) * * *

(h) * * *

(i) * * *

(j) DEFINITIONS.—As used in this section—

(1) * * *

(2) * * *

(3) * * *

(4) * * *

(5) * * *

(6) * * *

(7) * * *
(8) * * *
(9) the terms "mathematics, science, engineering, or technology" or "STEM" mean science, technology, engineering, and mathematics, including computer science *and cybersecurity*.

* * * * * * *

○