Subsec. (m)(1). Pub. L. 116–283, §9403(3)(A), substituted ''cybersecurity'' for ''cyber'' in introductory provisions.

Subsec. (m)(2). Pub. L. 116–283, §9404(5), substituted ''once every two 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—'' and subpars. (A) to (C) for ''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 cybersecurity workforce''.

Pub. L. 116–283, §9403(3)(B), substituted ''cybersecurity'' for ''cyber''. Subsequent amendment by Pub. L. 116–283, §9404(5), reenacted the word ''cyber'' in subsec. (m)(2)(C).

2017—Subsec. (b)(3), (4). Pub. L. 115–91, §1649B(a)(1), added pars. (3) and (4) and struck out former par. (3) which read as follows: ''prioritize the employment placement of scholarship recipients in the Federal Government.''

Subsec. (d). Pub. L. 115–91, §1649B(a)(2), amended subsec. (d) generally. Prior to amendment, text read as follows: ''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 in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree.''

Subsec. (f)(3). Pub. L. 115–91, §1649B(a)(3)(A), amended par. (3) generally. Prior to amendment, par. (3) read as follows: ''have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences;''.

Subsec. (f)(4). Pub. L. 115–91, §1649B(a)(3)(B), amended par. (4) generally. Prior to amendment, par. (4) read as follows: ''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; and''.

Subsec. (m). Pub. L. 115–91, §1649B(a)(4), amended subsec. (m) generally. Prior to amendment, text read as follows: ''The Director of the National Science Foundation shall evaluate and report periodically to Congress on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector workforce.''

SAVINGS PROVISION

Pub. L. 115–91, div. A, title XVI, §1649B(b), Dec. 12, 2017, 131 Stat. 1755, provided that: ''Nothing in this section [amending this section], or an amendment made by this section, shall affect any agreement, scholarship, loan, or repayment, under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), in effect on the day before the date of enactment of this subtitle [Dec. 12, 2017].''

COMMUNITY COLLEGE CYBER PILOT PROGRAM AND ASSESSMENT

Pub. L. 115–91, div. A, title XVI, §1649A, Dec. 12, 2017, 131 Stat. 1753, provided that:

''(a) PILOT PROGRAM.—Not later than 1 year after the date of enactment of this subtitle [Dec. 12, 2017], as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall develop and implement a pilot program at not more than 10, but at least 5, community colleges to provide scholarships to eligible students who—

''(1) are pursuing associate degrees or specialized program certifications in the field of cybersecurity; and

''(2)(A) have bachelor's degrees; or

''(B) are veterans of the Armed Forces.

''(b) ASSESSMENT.—Not later than 1 year after the date of enactment of this subtitle, as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall assess the potential benefits and feasibility of providing scholarships through community colleges to eligible students who are pursuing associate degrees, but do not have bachelor's degrees.''

§ 7443. 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;

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

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

(8) in coordination with the Department of Defense, the Department of Homeland Security, and other appropriate agencies, considering any specific needs of the cybersecurity workforce of critical infrastructure, including 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

(10) promoting initiatives to evaluate and forecast future cybersecurity workforce needs

of the Federal Government and develop strategies for recruitment, training, and retention.

(b) Considerations

In carrying out the authority described in subsection (a), the Director, in consultation with appropriate Federal agencies, shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently verified assessments regarding the quantification and valuation of information security risk.

(c) Strategic plan

(1) In general

The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of December 18, 2014, 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 December 18, 2014, 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 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 Department of Defense, 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

(1) In general

Pursuant to section 272(b)(4) of this title, 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 to—

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

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

(C) 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 terms 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) 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 academic institutions in the Federal Cyber Scholarships for Service Program, the 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 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, externships, apprenticeships, or cooperative education programs in conjunction with providers of education and training. Inclusion of programs that seek to include veterans, Indian Tribes, 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)(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 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.

(Pub. L. 113–274, title III, §303, formerly title IV, §401, Dec. 18, 2014, 128 Stat. 2985; renumbered title III, §303, and amended Pub. L. 116–283, div. H, title XCIV, §9401(a), (b), (e)–(g)(1), Jan. 1, 2021, 134 Stat. 4805–4807, 4809.)

CODIFICATION

Section was classified to section 7451 of this title prior to renumbering by Pub. L. 116–283.

AMENDMENTS

2021—Subsec. (a)(6) to (10). Pub. L. 116–283, §9401(a), added pars. (6) to (9) and redesignated former par. (6) as (10).

Subsec. (c). Pub. L. 116–283, §9401(b), designated existing provisions as par. (1), inserted heading, and added par. (2).

Subsec. (e). Pub. L. 116–283, §9401(e), added subsec. (e).

Subsec. (f). Pub. L. 116–283, §9401(f), added subsec. (f).

CYBERSECURITY CAREER PATHWAYS

Pub. L. 116–283, div. H, title XCIV, §9401(c), Jan. 1, 2021, 134 Stat. 4806, provided that:

''(1) IDENTIFICATION OF MULTIPLE CYBERSECURITY CAREER PATHWAYS.—In carrying out subsection (a) of such section [meaning 15 U.S.C. 7451(a), now 15 U.S.C. 7443(a)] and not later than 540 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, the Director of the Office of Personnel Management, and the heads of other appropriate agencies, 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, 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.''

PROFICIENCY TO PERFORM CYBERSECURITY TASKS

Pub. L. 116–283, div. H, title XCIV, §9401(d), Jan. 1, 2021, 134 Stat. 4806, provided that: ''Not later than 540 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the heads of other appropriate agencies—

''(1) in carrying out subsection (a) of such section [meaning 15 U.S.C. 7451(a), now 15 U.S.C. 7443(a)], 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) 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.''

SUBCHAPTER III—CYBERSECURITY AWARENESS AND PREPAREDNESS

CODIFICATION

This subchapter was comprised of title IV of Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2985, prior to its repeal by Pub. L. 116–283, div. H, title XCIV, § 9401(g)(2), Jan. 1, 2021, 134 Stat. 4809.

§ 7451. Transferred

CODIFICATION

Section, Pub. L. 113–274, title IV, § 401, Dec. 18, 2014, 128 Stat. 2985, which related to national cybersecurity awareness and education program, was renumbered § 303 of title III of Pub. L. 113–274, by Pub. L. 116–283, div. H, title XCIV, § 9401(g)(1), Jan. 1, 2021, 134 Stat. 4809, and transferred to section 7443 of this title.

SUBCHAPTER IV—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

§ 7461. Definitions

In this subchapter:

(1) Director

The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) Institute

The term ''Institute'' means the National Institute of Standards and Technology.

(Pub. L. 113–274, title V, § 501, Dec. 18, 2014, 128 Stat. 2986.)

§ 7462. International cybersecurity technical standards

(a) In general

The Director, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after December 18, 2014, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) Consultation with the private sector

In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

(Pub. L. 113–274, title V, § 502, Dec. 18, 2014, 128 Stat. 2986.)

§ 7463. Cloud computing strategy

(a) In general

The Director, in coordination with the Office of Management and Budget, in collaboration with the Federal Chief Information Officers Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(b) Activities

In carrying out the strategy described under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(3) support, in coordination with the Office of Management and Budget, and in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(A) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(B) to ensure secure access to the data stored in cloud computing data centers;

(C) to develop security standards as required under section 278g–3 of this title; and

(D) to support the development of the automation of continuous monitoring systems.

(Pub. L. 113–274, title V, § 503, Dec. 18, 2014, 128 Stat. 2986.)

§ 7464. Identity management research and development

The Director shall continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

(Pub. L. 113–274, title V, § 504, Dec. 18, 2014, 128 Stat. 2987.)

CHAPTER 101—NANOTECHNOLOGY RESEARCH AND DEVELOPMENT

Sec.