

through existing programs and activities, shall support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

(Pub. L. 113-274, title II, §201, Dec. 18, 2014, 128 Stat. 2974.)

CODIFICATION

Section is comprised of section 201 of Pub. L. 113-274. Subsec. (e) of section 201 of Pub. L. 113-274 amended section 7403 of this title.

SUBCHAPTER II—EDUCATION AND WORKFORCE DEVELOPMENT

§ 7441. Cybersecurity competitions and challenges

(a) In general

The Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, shall—

(1) support competitions and challenges under section 3719 of this title (as amended by section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989)) or any other provision of law, as appropriate—

(A) to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies, and the private sector; or

(B) to stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that has the potential for application to the information technology activities of the Federal Government; and

(2) ensure the effective operation of the competitions and challenges under this section.

(b) Participation

Participants in the competitions and challenges under subsection (a)(1) may include—

(1) students enrolled in grades 9 through 12;

(2) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(3) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(4) institutions of higher education and research institutions;

(5) veterans; and

(6) other groups or individuals that the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security determine appropriate.

(c) Affiliation and cooperative agreements

Competitions and challenges under this section may be carried out through affiliation and cooperative agreements with—

(1) Federal agencies;

(2) regional, State, or school programs supporting the development of cyber professionals;

(3) State, local, and tribal governments; or

(4) other private sector organizations.

(d) Areas of skill

Competitions and challenges under subsection (a)(1)(A) shall be designed to identify, develop, and recruit exceptional talent relating to—

(1) ethical hacking;

(2) penetration testing;

(3) vulnerability assessment;

(4) continuity of system operations;

(5) security in design;

(6) cyber forensics;

(7) offensive and defensive cyber operations; and

(8) other areas the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security consider necessary to fulfill the cybersecurity mission.

(e) Topics

In selecting topics for competitions and challenges under subsection (a)(1), the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security—

(1) shall consult widely both within and outside the Federal Government; and

(2) may empanel advisory committees.

(f) Internships

The Director of the Office of Personnel Management may support, as appropriate, internships or other work experience in the Federal Government to the winners of the competitions and challenges under this section.

(Pub. L. 113-274, title III, §301, Dec. 18, 2014, 128 Stat. 2981.)

REFERENCES IN TEXT

Section 3719 of this title (as amended by section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989)), referred to in subsec. (a)(1), probably means section 3719 of this title as enacted by section 105(a) of Pub. L. 111-358.

§ 7442. Federal Cyber Scholarship-for-Service Program

(a) In general

The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management and Secretary of Homeland Security, shall continue a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

(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 workforce; and

(3) prioritize the employment placement of scholarship recipients in the Federal Government.

(c) Scholarship amounts

Each scholarship under subsection (b) shall be in an amount that covers the student's tuition and fees at the institution under subsection (b)(1) for not more than 3 years and provides the student with an additional stipend.

(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 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.

(e) Hiring authority

(1) Appointment in excepted service

Notwithstanding any provision of chapter 33 of title 5 governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the eligible degree program for which a scholarship was awarded.

(2) Noncompetitive conversion

Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) Timing of conversion

An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) Authority to decline conversion

An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

(f) Eligibility

To be eligible to receive a scholarship under this 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 proficiency in mathematics, engineering, or computer sciences;

(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; and

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

(g) Conditions of support

(1) In general

As a condition of receiving a scholarship under this section, a recipient shall agree to provide the qualified institution of higher edu-

cation with annual verifiable documentation of post-award employment and up-to-date contact information.

(2) Terms

A scholarship recipient under this section shall be liable to the United States as provided in subsection (i) if the individual—

(A) fails to maintain an acceptable level of academic standing at the applicable institution of higher education, as determined by the Director of the National Science Foundation;

(B) is dismissed from the applicable institution of higher education for disciplinary reasons;

(C) withdraws from the eligible degree program before completing the program;

(D) declares that the individual does not intend to fulfill the post-award employment obligation under this section; or

(E) fails to fulfill the post-award employment obligation of the individual under this section.

(h) Monitoring compliance

As a condition of participating in the program, a qualified institution of higher education shall—

(1) enter into an agreement with the Director of the National Science Foundation, to monitor the compliance of scholarship recipients with respect to their post-award employment obligations; and

(2) provide to the Director of the National Science Foundation, on an annual basis, the post-award employment documentation required under subsection (g)(1) for scholarship recipients through the completion of their post-award employment obligations.

(i) Amount of repayment

(1) Less than 1 year of service

If a circumstance described in subsection (g)(2) occurs before the completion of 1 year of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(2) 1 or more years of service

If a circumstance described in subparagraph (D) or (E) of subsection (g)(2) occurs after the completion of 1 or more years of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(j) Repayments

A loan described subsection (i) shall—

(1) be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a et seq.); and

(2) be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director of the National Science Foundation (in consultation with the Secretary of Education) in regulations promulgated to carry out this subsection.

(k) Collection of repayment

(1) In general

In the event that a scholarship recipient is required to repay the scholarship award under this section, the qualified institution of higher education providing the scholarship shall—

(A) determine the repayment amounts and notify the recipient and the Director of the National Science Foundation of the amounts owed; and

(B) collect the repayment amounts within a period of time as determined by the Director of the National Science Foundation, or the repayment amounts shall be treated as a loan in accordance with subsection (j).

(2) Returned to Treasury

Except as provided in paragraph (3), any repayment under this subsection shall be returned to the Treasury of the United States.

(3) Retain percentage

A qualified institution of higher education may retain a percentage of any repayment the institution collects under this subsection to defray administrative costs associated with the collection. The Director of the National Science Foundation shall establish a single, fixed percentage that will apply to all eligible entities.

(l) Exceptions

The Director of the National Science Foundation may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(m) Evaluation and report

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.

(Pub. L. 113–274, title III, §302, Dec. 18, 2014, 128 Stat. 2982.)

REFERENCES IN TEXT

The Higher Education Act of 1965, referred to in subsec. (j)(1), is Pub. L. 89–329, Nov. 8, 1965, 79 Stat. 1219. Part D of title IV of the Act is classified to part C (§1087a et seq.) of subchapter IV of chapter 28 of Title 20, Education. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 20 and Tables.

SUBCHAPTER III—CYBERSECURITY
AWARENESS AND PREPAREDNESS

§ 7451. 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) 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

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).

(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