

(4) Coordination

In pursuing national cybersecurity challenges under paragraph (1), the Secretary shall coordinate with the following:

- (A) The Director of the National Science Foundation.
- (B) The Secretary of Homeland Security.
- (C) The Director of the Defense Advanced Research Projects Agency.
- (D) The Director of the Office of Science and Technology Policy.
- (E) The Director of the Office of Management and Budget.
- (F) The Administrator of the General Services Administration.
- (G) The Federal Trade Commission.
- (H) The heads of such other Federal agencies as the Secretary of Commerce considers appropriate for purposes of this section.

(5) Solicitation of acceptance of funds**(A) In general**

Pursuant to section 3719 of this title, the Secretary shall request and accept funds from other Federal agencies, State, United States territory, local, or Tribal government agencies, private sector for-profit entities, and nonprofit entities to support efforts to pursue a national cybersecurity challenge under this section.

(B) Rule of construction

Nothing in subparagraph (A) may be construed to require any person or entity to provide funds or otherwise participate in an effort or competition under this section.

(c) Recommendations**(1) In general**

In carrying out this section, the Secretary of Commerce shall designate an advisory council to seek recommendations.

(2) Elements

The recommendations required by paragraph (1) shall include the following:

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

(3) No additional compensation

The Secretary may not provide any additional compensation, except for travel expenses, to a member of the advisory council designated under paragraph (1) for participation in the advisory council.

(Pub. L. 113-274, title II, §205, as added Pub. L. 116-283, div. H, title XCIV, §9407(a), Jan. 1, 2021, 134 Stat. 4813.)

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.)

Editorial Notes

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 and cybersecurity workforce;
- (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);
 - (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.

(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 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);
- (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;
- (5) a State, local, or Tribal government-affiliated non-profit that is considered to be critical infrastructure (as defined in section 5195c(e) of title 42); or
- (6) as provided by subsection (b)(3)(B), a qualified institution of higher education.

(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—