National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, may award grants to institutions of higher education or research and development nonprofit institutions to establish cybersecurity test beds.

(B) Requirement

The cybersecurity test beds under subparagraph (A) shall be sufficiently robust in order to model the scale and complexity of real-time cyber attacks and defenses on real world networks and environments.

(C) Assessment required

The Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, shall evaluate the effectiveness of any grants awarded under this subsection in meeting the objectives of the Federal cybersecurity research and development strategic plan not later than 2 years after the review under paragraph (1) of this subsection, and periodically thereafter.

(d) Coordination with other research initiatives

In accordance with the responsibilities under section 5511 of this title, the Director of the Office of Science and Technology Policy shall coordinate, to the extent practicable, Federal research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Science Foundation;

(2) the National Institute of Standards and Technology;

(3) the Department of Homeland Security;

(4) other Federal agencies;

(5) other Federal and private research laboratories, research entities, and universities;

(6) institutions of higher education;

(7) relevant nonprofit organizations; and

(8) international partners of the United States.

(e) Omitted

(f) Research on the science of cybersecurity

The head of each agency and department identified under section 5511(a)(3)(B)[1] of this title, 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; Pub. L. 114–329, title I, §105(t), Jan. 6, 2017, 130 Stat. 2985; Pub. L. 116–283, div. H, title XCIV, §9407(b), Jan. 1, 2021, 134 Stat. 4814.)

Editorial Notes

REFERENCES IN TEXT

Section 5511(a)(3)(B) of this title, referred to in subsecs. (a)(4) and (f), was redesignated section 5511(a)(3)(C) of this title by Pub. L. 114–329, title I, §105(f)(2)(D)(i), Jan. 6, 2017, 130 Stat. 2979.

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.

AMENDMENTS

2021—Subsec. (a)(1)(K), (L). Pub. L. 116–283 added subpar. (K) and redesignated former subpar. (K) as (L).

2017—Subsec. (a)(4). Pub. L. 114–329 substituted ''clauses (i) through (xi)'' for ''clauses (i) through (x)'' and ''under clause (xii)'' for ''under clause (xi)''.

§ 7432. National cybersecurity challenges

(a) Establishment of national cybersecurity challenges

(1) In general

To achieve high-priority breakthroughs in cybersecurity by 2028, the Secretary of Commerce shall establish the following national cybersecurity challenges:

(A) Economics of a cyber attack

Building more resilient systems that measurably and exponentially raise adversary costs of carrying out common cyber attacks.

(B) Cyber training

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

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

(C) Emerging technology

Advancing cybersecurity efforts in response to emerging technology, such as artificial intelligence, quantum science, next generation communications, autonomy, data science, and computational technologies.

(D) Reimagining digital identity

Maintaining a high sense of usability while improving the privacy, security, and safety of online activity of individuals in the United States.

(E) Federal agency resilience

Reducing cybersecurity risks to Federal networks and systems, and improving the response of Federal agencies to cybersecurity incidents on such networks and systems.

(2) Coordination

In establishing the challenges under paragraph (1), the Secretary shall coordinate with the Secretary of Homeland Security on the challenges under subparagraphs (B) and (E) of such paragraph.

(b) Pursuit of national cybersecurity challenges

(1) In general

Not later than 180 days after January 1, 2021, the Secretary, acting through the Under Secretary of Commerce for Standards and Technology, shall commence efforts to pursue the national cybersecurity challenges established under subsection (a).

(2) Competitions

The efforts required by paragraph (1) shall include carrying out programs to award prizes,

including cash and noncash prizes, competitively pursuant to the authorities and processes established under section 3719 of this title or any other applicable provision of law.

(3) Additional authorities

In carrying out paragraph (1), the Secretary may enter into and perform such other transactions as the Secretary considers necessary and on such terms as the Secretary considers appropriate.

(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