Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

§ 7423. No additional funds authorized

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

(Pub. L. 113–274, § 4, Dec. 18, 2014, 128 Stat. 2972.)

Editorial Notes

REFERENCES IN TEXT

This Act, and the amendments made by this Act, referred to in text, is Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which enacted this chapter and amended sections 272, 278g–3, 7403, and 7406 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

SUBCHAPTER I—CYBERSECURITY RESEARCH AND DEVELOPMENT

§ 7431. Federal cybersecurity research and development

(a) Fundamental cybersecurity research

(1) Federal cybersecurity research and development strategic plan

The heads of the applicable agencies and departments, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, shall develop and update every 4 years a Federal cybersecurity research and development strategic plan (referred to in this subsection as the ''strategic plan'') based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. The heads of the applicable agencies and departments shall build upon existing programs and plans to develop the strategic plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;

(D) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services;

(K) implementation of section 7432 of this title through research and development on the topics identified under subsection (a) of such section; and

(L) any additional objectives the heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate.

(2) Requirements

(A) Contents of plan

The strategic plan shall—

(i) specify and prioritize near-term, mid-term, and long-term research objectives, including objectives associated with the research identified in section 7403(a)(1) of this title;

(ii) specify how the near-term objectives described in clause (i) complement research and development areas in which the private sector is actively engaged;

(iii) describe how the heads of the applicable agencies and departments will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(iv) describe how the heads of the applicable agencies and departments will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(v) describe how the heads of the applicable agencies and departments will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems; and

(vi) describe how the heads of the applicable agencies and departments will facilitate access by academic researchers to the infrastructure described in clause (v), as well as to relevant data, including event data.

(B) Private sector efforts

In developing, implementing, and updating the strategic plan, the heads of the applica-

ble agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall work in close cooperation with industry, academia, and other interested stakeholders to ensure, to the extent possible, that Federal cybersecurity research and development is not duplicative of private sector efforts.

(C) Recommendations

In developing and updating the strategic plan the heads of the applicable agencies and departments shall solicit recommendations and advice from—

(i) the advisory committee established under section 5511(b)(1) of this title; and

(ii) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, National Laboratories, and other relevant organizations and institutions.

(D) Implementation roadmap

The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall develop and annually update an implementation roadmap for the strategic plan. The implementation roadmap shall—

(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year;

(iii) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years; and

(iv) track ongoing and completed Federal cybersecurity research and development projects.

(3) Reports to Congress

The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall submit 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) the strategic plan not later than 1 year after December 18, 2014;

(B) each quadrennial update to the strategic plan; and

(C) the implementation roadmap under subparagraph (D), and its annual updates, which shall be appended to the annual report required under section 5511(a)(2)(D) of this title.

(4) Definition of applicable agencies and departments

In this subsection, the term ''applicable agencies and departments'' means the agencies and departments identified in clauses (i) through (xi) of section 5511(a)(3)(B)[1] of this title or designated under clause (xii) of that section.

(b) Cybersecurity practices research

The Director of the National Science Foundation shall support research that—

(1) develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs; and

(2) develops new models for professional development of faculty in cybersecurity education, including secure coding development.

(c) Cybersecurity modeling and test beds

(1) Review

Not later than 1 year after December 18, 2014, the Director of the National Science Foundation, in coordination with the Director of the Office of Science and Technology Policy, shall conduct a review of cybersecurity test beds in existence on December 18, 2014, to inform the grants under paragraph (2). The review shall include an assessment of whether a sufficient number of cybersecurity test beds are available to meet the research needs under the Federal cybersecurity research and development strategic plan. Upon completion, the Director shall submit the review to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(2) Additional cybersecurity modeling and test beds

(A) In general

If the Director of the National Science Foundation, after the review under paragraph (1), determines that the research needs under the Federal cybersecurity research and development strategic plan require the establishment of additional cybersecurity test beds, the Director of the 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.

[1] See References in Text note below.

(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.