

untary 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

Editorial Notes

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

Editorial Notes

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

(a) In general

The Director shall carry out a program of research to support the development of voluntary,