

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,

consensus-based technical standards, best practices, benchmarks, methodologies, metrology, testbeds, and conformance criteria for identity management, taking into account appropriate user concerns to—

- (1) improve interoperability and portability among identity management technologies;
- (2) strengthen identity proofing and verification methods used in identity management systems commensurate with the level of risk, including identity and attribute validation services provided by Federal, State, and local governments;
- (3) improve privacy protection in identity management systems; and
- (4) improve the accuracy, usability, and inclusivity of identity management systems.

(b) Digital identity technical roadmap

The Director, in consultation with other relevant Federal agencies and stakeholders from the private sector, shall develop and maintain a technical roadmap for digital identity management research and development focused on enabling the voluntary use and adoption of modern digital identity solutions that align with the four criteria in subsection (a).

(c) Digital identity management guidance

(1) In general

The Director shall develop, and periodically update, in collaboration with other public and private sector organizations, common definitions and voluntary guidance for digital identity management systems, including identity and attribute validation services provided by Federal, State, and local governments.

(2) Guidance

The Guidance shall—

- (A) align with the four criteria in subsection (a), as practicable;
- (B) provide case studies of implementation of guidance;
- (C) incorporate voluntary technical standards and industry best practices; and
- (D) not prescribe or otherwise require the use of specific technology products or services.

(3) Consultation

In carrying out this subsection, the Director shall consult with—

- (A) Federal and State agencies;
- (B) industry;
- (C) potential end-users and individuals that will use services related to digital identity verification; and
- (D) experts with relevant experience in the systems that enable digital identity verification, as determined by the Director.

(Pub. L. 113-274, title V, §504, Dec. 18, 2014, 128 Stat. 2987; Pub. L. 117-167, div. B, title II, §10225, Aug. 9, 2022, 136 Stat. 1478.)

Editorial Notes

AMENDMENTS

2022—Pub. L. 117-167 amended section generally. Prior to amendment, section related to Director's continuance of program to support development of voluntary and cost-effective technical standards, metrology,

testbeds, and conformance criteria, taking into account appropriate user concerns.

CHAPTER 101—NANOTECHNOLOGY RESEARCH AND DEVELOPMENT

Sec. 7501.	National Nanotechnology Program.
7502.	Program coordination.
7503.	Advisory Panel.
7504.	Quadrennial external review of the National Nanotechnology Program.
7505.	Authorization of appropriations.
7506.	Department of Commerce programs.
7507.	Department of Energy programs.
7508.	Additional centers.
7509.	Definitions.

§ 7501. National Nanotechnology Program

(a) National Nanotechnology Program

The President shall implement a National Nanotechnology Program. Through appropriate agencies, councils, and the National Nanotechnology Coordination Office established in section 7502 of this title, the Program shall—

- (1) establish the goals, priorities, and metrics for evaluation for Federal nanotechnology research, development, and other activities;
- (2) invest in Federal research and development programs in nanotechnology and related sciences to achieve those goals; and
- (3) provide for interagency coordination of Federal nanotechnology research, development, and other activities undertaken pursuant to the Program.

(b) Program activities

The activities of the Program shall include—

- (1) developing a fundamental understanding of matter that enables control and manipulation at the nanoscale;
- (2) providing grants to individual investigators and interdisciplinary teams of investigators;
- (3) establishing a network of advanced technology user facilities and centers;
- (4) establishing, on a merit-reviewed and competitive basis, interdisciplinary nanotechnology research centers, which shall—
 - (A) interact and collaborate to foster the exchange of technical information and best practices;
 - (B) involve academic institutions or national laboratories and other partners, which may include States and industry;
 - (C) make use of existing expertise in nanotechnology in their regions and nationally;
 - (D) make use of ongoing research and development at the micrometer scale to support their work in nanotechnology; and
 - (E) to the greatest extent possible, be established in geographically diverse locations, encourage the participation of Historically Black Colleges and Universities that are part B institutions as defined in section 1061(2) of title 20 and minority institutions (as defined in section 1067k(3) of title 20), and include institutions located in States participating in the Experimental Program to Stimulate Competitive Research (EPSCoR);