

(2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, educational institutions, and State, local, and tribal governments;

(3) increasing public awareness of cybersecurity, cyber safety, and cyber ethics;

(4) increasing the understanding of State, local, and tribal governments, institutions of higher education, and private sector entities of—

(A) the benefits of ensuring effective risk management of information technology versus the costs of failure to do so; and

(B) the methods to mitigate and remediate vulnerabilities;

(5) supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government; and

(6) promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.

(b) Considerations

In carrying out the authority described in subsection (a), the Director, in consultation with appropriate Federal agencies, shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently verified assessments regarding the quantification and valuation of information security risk.

(c) Strategic plan

The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of December 18, 2014, to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and education program under subsection (a).

(d) Report

Not later than 1 year after December 18, 2014, and every 5 years thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(Pub. L. 113–274, title IV, § 401, Dec. 18, 2014, 128 Stat. 2985.)

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

The Director shall continue a program to support the development of voluntary and cost-ef-