

§ 7406. National Institute of Standards and Technology programs

(a), (b) Omitted

(c) Security automation and checklists for Government systems

(1) In general

The Director of the National Institute of Standards and Technology shall, as necessary, develop and revise security automation standards, associated reference materials (including protocols), and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government, thereby enabling standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government.

(2) Priorities for development

The Director of the National Institute of Standards and Technology shall establish priorities for the development of standards, reference materials, and checklists under this subsection on the basis of—

(A) the security risks associated with the use of the system;

(B) the number of agencies that use a particular system or security tool;

(C) the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system;

(D) the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security; or

(E) such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate.

(3) Excluded systems

The Director of the National Institute of Standards and Technology may exclude from the application of paragraph (1) any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the lack of utility or impracticability of developing a standard, reference material, or checklist for the system.

(4) Dissemination of standards and related materials

The Director of the National Institute of Standards and Technology shall ensure that Federal agencies are informed of the availability of any standard, reference material, checklist, or other item developed under this subsection.

(5) Agency use requirements

The development of standards, reference materials, and checklists under paragraph (1) for an information technology hardware or software system or tool does not—

(A) require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system;

(B) establish conditions or prerequisites for Federal agency procurement or deployment of any such system;

(C) imply an endorsement of any such system by the Director of the National Institute of Standards and Technology; or

(D) preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified under paragraph (1).

(d) Federal agency information security programs

(1) In general

In developing the agencywide information security program required by section 3554(b) of title 44, an agency that deploys a computer hardware or software system for which the Director of the National Institute of Standards and Technology has developed a checklist under subsection (c) of this section—

(A) shall include in that program an explanation of how the agency has considered such checklist in deploying that system; and

(B) may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31).

(2) Limitation

Paragraph (1) does not apply to any computer hardware or software system for which the National Institute of Standards and Technology does not have responsibility under section 278g-3(a)(3) of this title.

(Pub. L. 107-305, § 8, Nov. 27, 2002, 116 Stat. 2375; Pub. L. 113-274, title II, § 203, Dec. 18, 2014, 128 Stat. 2979; Pub. L. 113-283, § 2(e)(2), Dec. 18, 2014, 128 Stat. 3086.)

CODIFICATION

Section is comprised of section 8 of Pub. L. 107-305. Subsec. (a) of section 8 of Pub. L. 107-305 enacted section 278h of this title and renumbered former section 278h of this title as section 278q of this title. Subsec. (b) of section 8 of Pub. L. 107-305 amended section 278g-3 of this title.

AMENDMENTS

2014—Subsec. (c). Pub. L. 113-274 amended subsec. (c) generally. Prior to amendment, text related to checklists setting forth settings and option selections that minimize the security risks associated with computer hardware or software systems likely to become widely used within the Federal Government.

Subsec. (d)(1). Pub. L. 113-283, which directed amendment of section 8 of the Cybersecurity Research and Development Act by substituting “section 3554” for “section 3534” in subsec. (d)(1), was executed to this section, which is section 8 of the Cyber Security Research and Development Act, to reflect the probable intent of Congress.

§ 7407. Authorization of appropriations

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology—