

(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—

(1) for activities under section 278h of this title—

(A) \$25,000,000 for fiscal year 2003;

(B) \$40,000,000 for fiscal year 2004;

(C) \$55,000,000 for fiscal year 2005;

(D) \$70,000,000 for fiscal year 2006;

(E) \$85,000,000 for fiscal year 2007; and

(2) for activities under section 278g-3(f)¹ of this title—

(A) \$6,000,000 for fiscal year 2003;

(B) \$6,200,000 for fiscal year 2004;

(C) \$6,400,000 for fiscal year 2005;

(D) \$6,600,000 for fiscal year 2006; and

(E) \$6,800,000 for fiscal year 2007.

(Pub. L. 107-305, § 11, Nov. 27, 2002, 116 Stat. 2379.)

REFERENCES IN TEXT

Section 278g-3 of this title, referred to in par. (2), was amended by Pub. L. 107-347, title III, § 303, Dec. 17, 2002, 116 Stat. 2957, and, as so amended, did not contain a subsec. (f). A later amendment by Pub. L. 113-274, title II, § 204(1), Dec. 18, 2014, 128 Stat. 2980, redesignated subsec. (e) of section 278g-3 of this title, relating to definitions, as (f).

§ 7408. National Academy of Sciences study on computer and network security in critical infrastructures

(a) Study

Not later than 3 months after November 27, 2002, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) Report

The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after November 27, 2002.

(c) Security

The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

¹ See References in Text note below.