15 USC 278g-3: Computer standards program
Text contains those laws in effect on December 9, 2020

From Title 15-COMMERCE AND TRADE
CHAPTER 7-NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Jump To:
Source Credit
Codification
Prior Provisions
Amendments
Effective Date

§278g–3. Computer standards program

(a) In general

The Institute shall-

(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3552(b)(5) [1] of title 44);

(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems; and

(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division.

(b) Minimum requirements for standards and guidelines

The standards and guidelines required by subsection (a) shall include, at a minimum-

(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

(B) guidelines recommending the types of information and information systems to be included in each such category; and

(C) minimum information security requirements for information and information systems in each such category;

(2) a definition of and guidelines concerning detection and handling of information security incidents; and

(3) guidelines developed in coordination with the National Security Agency for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

(c) Development of standards and guidelines

In developing standards and guidelines required by subsections (a) and (b), the Institute shall-

(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the Government Accountability Office, and the Secretary of Homeland Security) to assure-

(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

(2) provide the public with an opportunity to comment on proposed standards and guidelines;

(3) submit to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40-

(A) standards, as required under subsection (b)(1)(A), no later than 12 months after November 25, 2002; and

(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after November 25, 2002;

(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after November 25, 2002;

(5) ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions;

(6) ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

(7) use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.

(d) Information security functions

The Institute shall-

(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40;

(2) provide assistance to agencies regarding-

(A) compliance with the standards and guidelines developed under subsection (a);

(B) detecting and handling information security incidents; and

(C) information security policies, procedures, and practices;

(3) conduct research and analysis-

(A) to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

(B) to review and determine prevalent information security challenges and deficiencies identified by agencies or the Institute, including any challenges or deficiencies described in any of the annual reports under section 3553 or 3554 of title 44, and in any of the reports and the independent evaluations under section 3555 of that title, that may undermine the effectiveness of agency information security programs and practices; and

(C) to evaluate the effectiveness and sufficiency of, and challenges to, Federal agencies' implementation of standards and guidelines developed under this section and policies and standards promulgated under section 11331 of title 40;

(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

(6) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

(7) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

(8) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 278g–4 of this title, regarding standards and guidelines developed under subsection (a) and submit such recommendations to the Director of the Office of Management and Budget with such standards submitted to the Director; and

(9) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

(e) Intramural security research

As part of the research activities conducted in accordance with subsection (d)(3), the Institute shall, to the extent practicable and appropriate-

(1) conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computing environments;

(2) carry out research associated with improving the security of information systems and networks;

(3) carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks;

(4) carry out research associated with improving security of industrial control systems;

(5) carry out research associated with improving the security and integrity of the information technology supply chain; and

(6) carry out any additional research the Institute determines appropriate.

(f) Definitions

As used in this section-

(1) the term "agency" has the same meaning as provided in section 3502(1) of title 44;

(2) the term "information security" has the same meaning as provided in section 3552(b)(2) [2] of such title;

(3) the term "information system" has the same meaning as provided in section 3502(8) of such title;

(4) the term "information technology" has the same meaning as provided in section 11101 of title 40; and

(5) the term "national security system" has the same meaning as provided in section 3552(b)(5) [1] of such title.[3]

(Mar. 3, 1901, ch. 872, §20, as added Pub. L. 100–235, §3(2), Jan. 8, 1988, 101 Stat. 1724 ; amended Pub. L. 100–418, title V, §5115(a)(1), Aug. 23, 1988, 102 Stat. 1433 ; Pub. L. 104–106, div. E, title LVI, §5607(a), Feb. 10, 1996, 110 Stat. 701 ; Pub. L. 105–85, div. A, title X, §1073(h)(1), Nov. 18, 1997, 111 Stat. 1906 ; Pub. L. 107–296, title X, §1003, Nov. 25, 2002, 116 Stat. 2269 ; Pub. L. 107–305, §§8(b), 9, 10, Nov. 27, 2002, 116 Stat. 2378 , 2379; Pub. L. 107–347, title III, §303, Dec. 17, 2002, 116 Stat. 2957 ; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814 ; Pub. L. 113–274, title II, §204, Dec. 18, 2014, 128 Stat. 2980 ; Pub. L. 113–283, §2(e)(4), Dec. 18, 2014, 128 Stat. 3087 ; Pub. L. 114–329, title I, §104(b)(3), Jan. 6, 2017, 130 Stat. 2976 .)

Codification

November 25, 2002, referred to in subsec. (c)(3) and (4), was in the original "the date of the enactment of this section" in subsec. (c)(3) and "the date of the enactment of this Act" in subsec. (c)(4), which were translated as meaning the date of enactment of Pub. L. 107–296, which enacted the text of this section, to reflect the probable intent of Congress.

Prior Provisions

A prior section 20 of act Mar. 3, 1901, ch. 872, was renumbered section 32 and is classified to section 278q of this title.

Amendments

2017-Subsec. (d)(3). Pub. L. 114–329 amended par. (3) generally. Prior to amendment, par. (3) read as follows: "conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;".

2014-Subsec. (a)(2). Pub. L. 113–283, §2(e)(4)(A), substituted "section 3552(b)(5)" for "section 3532(b)(2)".

Subsec. (e). Pub. L. 113–274, §204(2), added subsec. (e). Former subsec. (e) redesignated (f).

Subsec. (f). Pub. L. 113–283, §2(e)(4)(B), which directed amendment of subsec. (e) by substituting "section 3552(b)(2)" for "section 3532(1)" in par. (2) and "section 3552(b)(5)" for "section 3532(b)(2)" in par. (5), was executed to pars. (2) and (5), respectively, of subsec. (f), to reflect the probable intent of Congress and the redesignation of subsec. (e) as (f) by Pub. L. 113–274, §204(1). See below.

Pub. L. 113–274, §204(1), redesignated subsec. (e) as (f).

2004-Subsec. (c)(1). Pub. L. 108–271 substituted "Government Accountability Office" for "General Accounting Office".

2002-Pub. L. 107–296 added text of section and struck out former text, as added by Pub. L. 107–347, which read:

"(a) In General.-The Institute shall-

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

"(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3542(b)(2) of title 44); and

"(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

"(b) Minimum Requirements for Standards and Guidelines.-The standards and guidelines required by subsection (a) of this section shall include, at a minimum-

"(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

"(B) guidelines recommending the types of information and information systems to be included in each such category; and

"(C) minimum information security requirements for information and information systems in each such category;

"(2) a definition of and guidelines concerning detection and handling of information security incidents; and

"(3) guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

"(c) Development of Standards and Guidelines.-In developing standards and guidelines required by subsections (a) and (b) of this section, the Institute shall-

"(1) consult with other agencies and offices and the private sector (including the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure-

"(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

"(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

"(2) provide the public with an opportunity to comment on proposed standards and guidelines;

"(3) submit to the Secretary of Commerce for promulgation under section 11331 of title 40-

"(A) standards, as required under subsection (b)(1)(A) of this section, no later than 12 months after December 17, 2002; and

"(B) minimum information security requirements for each category, as required under subsection (b)(1)(C) of this section, no later than 36 months after December 17, 2002;

"(4) issue guidelines as required under subsection (b)(1)(B) of this section, no later than 18 months after December 17, 2002;

"(5) to the maximum extent practicable, ensure that such standards and guidelines do not require the use or procurement of specific products, including any specific hardware or software;

"(6) to the maximum extent practicable, ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

"(7) to the maximum extent practicable, use flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information security products.

"(d) Information Security Functions.-The Institute shall-

"(1) submit standards developed pursuant to subsection (a) of this section, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 11331 of title 40;

"(2) provide technical assistance to agencies, upon request, regarding-

"(A) compliance with the standards and guidelines developed under subsection (a) of this section;

"(B) detecting and handling information security incidents; and

"(C) information security policies, procedures, and practices;

"(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

"(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

"(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

"(6) assist the private sector, upon request, in using and applying the results of activities under this section;

"(7) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

"(8) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

"(9) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 278g–4 of this title, regarding standards and guidelines developed under subsection (a) of this section and submit such recommendations to the Secretary of Commerce with such standards submitted to the Secretary; and

"(10) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

"(e) Definitions.-As used in this section-

"(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44;

"(2) the term 'information security' has the same meaning as provided in section 3542(b)(1) of such title;

"(3) the term 'information system' has the same meaning as provided in section 3502(8) of such title;

"(4) the term 'information technology' has the same meaning as provided in section 11101 of title 40; and

"(5) the term 'national security system' has the same meaning as provided in section 3542(b)(2) of title 44.

"(f) Authorization of Appropriations.-There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section."

Pub. L. 107–347 added text of section and struck out former text which read as follows:

"(a) The Institute shall-

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10 or section 3502(9) of title 44;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except-

"(A) those systems excluded by section 2315 of title 10 or section 3502(9) of title 44; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 1441 of title 40;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the Institute is authorized-

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 1441 of title 40;

"(3) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(4) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(5) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)-

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) of this section are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of-

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3) of this section, and

"(2) performing research and conducting studies under subsection (b)(5) of this section,

the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the Institute determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section-

"(1) the term 'computer system'-

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes-

"(i) computers and computer networks;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources;

"(2) the term 'Federal computer system' means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5 (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 472(b) of title 40.

"(e) Intramural Security Research.-As part of the research activities conducted in accordance with subsection (b)(4) of this section, the Institute shall-

"(1) conduct a research program to address emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;

"(2) carry out research associated with improving the security of real-time computing and communications systems for use in process control; and

"(3) carry out multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.

"(f) Authorization of Appropriations.-There are authorized to be appropriated to the Secretary $1,060,000 for fiscal year 2003 and $1,090,000 for fiscal year 2004 to enable the Computer System Security and Privacy Advisory Board, established by section 278g–4 of this title, to identify emerging issues, including research needs, related to computer security, privacy, and cryptography and, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects."

Subsec. (d)(1)(B)(i). Pub. L. 107–305, §8(b), substituted "computers and computer networks" for "computers".

Subsecs. (e), (f). Pub. L. 107–305, §§9, 10, added subsecs. (e) and (f).

1997-Subsecs. (a)(4), (b)(2). Pub. L. 105–85 made technical amendment to reference in original act which appears in text as reference to section 1441 of title 40.

1996-Subsec. (a)(2), (3)(A). Pub. L. 104–106, §5607(a)(1)(A), substituted "section 3502(9) of title 44" for "section 3502(2) of title 44".

Subsec. (a)(4). Pub. L. 104–106, §5607(a)(1)(B), substituted "section 1441 of title 40" for "section 759(d) of title 40".

Subsec. (b)(2). Pub. L. 104–106, §5607(a)(2)(A), (C), redesignated par. (3) as (2) and struck out former par. (2) which read as follows: "to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 1441 of title 40;".

Subsec. (b)(3). Pub. L. 104–106, §5607(a)(2)(C), redesignated par. (4) as (3). Former par. (3) redesignated (2).

Pub. L. 104–106, §5607(a)(2)(B), substituted "section 1441 of title 40" for "section 759(d) of title 40".

Subsec. (b)(4) to (6). Pub. L. 104–106, §5607(a)(2)(C), redesignated pars. (4) to (6) as (3) to (5), respectively.

Subsec. (d)(1)(B)(v). Pub. L. 104–106, §5607(a)(3)(A), struck out "as defined by regulations issued by the Administrator for General Services pursuant to section 759 of title 40" after "related resources".

Subsec. (d)(2). Pub. L. 104–106, §5607(a)(3)(B), substituted "system' " for "system'-", struck out "(A)" before "means", substituted "function;" for "function; and", and struck out subpar. (B) which read as follows: "includes automatic data processing equipment as that term is defined in section 759(a)(2) of title 40;".

1988-Pub. L. 100–418 substituted "Institute" for "National Bureau of Standards" in introductory provisions of subsecs. (a) and (b) and wherever appearing in closing provisions of subsec. (c).

Effective Date of 2002 Amendments

Amendment by Pub. L. 107–347 effective Dec. 17, 2002, see section 402(b) of Pub. L. 107–347, set out as a note under section 3504 of Title 44, Public Printing and Documents.

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

Effective Date of 1996 Amendment

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702 .

[1] *So in original. Probably should be "3552(b)(6)".*

[2] *So in original. Probably should be "3552(b)(3)".*

[3] *So in original. "Such title" probably means title 44.*