quirements 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).

Statutory Notes and Related Subsidiaries

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.

PUBLICATION OF STANDARDS AND GUIDELINES ON CYBERSECURITY AWARENESS

Pub. L. 116–283, div. H, title XCIV, § 9402(b), Jan. 1, 2021, 134 Stat. 4810, provided that: ''Not later than three years after the date of the enactment of this Act [Jan. 1, 2021] and pursuant to section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), the Director of the National Institute of Standards and Technology shall publish standards and guidelines for improving cybersecurity awareness of employees and contractors of Federal agencies.''

§ 278g–3a. Definitions

In this Act:

(1) Agency

The term ''agency'' has the meaning given that term in section 3502 of title 44.

(2) Director of OMB

The term ''Director of OMB'' means the Director of the Office of Management and Budget.

(3) Director of the Institute

The term ''Director of the Institute'' means the Director of the National Institute of Standards and Technology.

(4) Information system

The term ''information system'' has the meaning given that term in section 3502 of title 44.

(5) National security system

The term ''national security system'' has the meaning given that term in section 3552(b)(6) of title 44.

(6) Operational technology

The term ''operational technology'' means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.

(7) Secretary

The term ''Secretary'' means the Secretary of Homeland Security.

(8) Security vulnerability

The term ''security vulnerability'' has the meaning given that term in section 650 of title 6.

(Pub. L. 116–207, § 3, Dec. 4, 2020, 134 Stat. 1001; Pub. L. 117–263, div. G, title LXXI, § 7143(d)(8), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

REFERENCES IN TEXT

This Act, referred to in text, is Pub. L. 116–207, Dec. 4, 2020, 134 Stat. 1001, known as the Internet of Things Cybersecurity Improvement Act of 2020 and also as the IoT Cybersecurity Improvement Act of 2020, which enacted this section and sections 278g–3b to 278g–3e of this title and provisions set out as a note under this section. For complete classification of this Act to the Code, see Short Title of 2020 Amendment note set out under section 271 of this title and Tables.

CODIFICATION

Section was enacted as part of the Internet of Things Cybersecurity Improvement Act of 2020, also known as the IoT Cybersecurity Improvement Act of 2020, and not as part of the National Institute of Standards and Technology Act which comprises this chapter.

AMENDMENTS

2022—Par. (8). Pub. L. 117–263 substituted ''section 650 of title 6'' for ''section 1501(17) of title 6''.

Statutory Notes and Related Subsidiaries

SENSE OF CONGRESS

Pub. L. 116–207, § 2, Dec. 4, 2020, 134 Stat. 1001, provided that: ''It is the sense of Congress that—

''(1) ensuring the highest level of cybersecurity at agencies in the executive branch is the responsibility of the President, followed by the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the head of each such agency;

''(2) this responsibility is to be carried out by working collaboratively within and among agencies in the executive branch, industry, and academia;

''(3) the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government; and

''(4) consistent with the second draft National Institute for Standards and Technology Interagency or Internal Report 8259 titled 'Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline', published in January 2020, Internet of Things devices are devices that—

''(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

''(B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.''

§ 278g–3b. Security standards and guidelines for agencies on use and management of Internet of Things devices

(a) National Institute of Standards and Technology development of standards and guidelines for use of Internet of Things devices by agencies

(1) In general

Not later than 90 days after December 4, 2020, the Director of the Institute shall develop and publish under section 278g–3 of this title standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) Consistency with ongoing efforts

The Director of the Institute shall ensure that the standards and guidelines developed under paragraph (1) are consistent with the efforts of the National Institute of Standards and Technology in effect on December 4, 2020—

(A) regarding—

(i) examples of possible security vulnerabilities of Internet of Things devices; and

(ii) considerations for managing the security vulnerabilities of Internet of Things devices; and

(B) with respect to the following considerations for Internet of Things devices:

(i) Secure Development.

(ii) Identity management.

(iii) Patching.

(iv) Configuration management.

(3) Considering relevant standards

In developing the standards and guidelines under paragraph (1), the Director of the Institute shall consider relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships.

(b) Review of agency information security policies and principles

(1) Requirement

Not later than 180 days after the date on which the Director of the Institute completes the development of the standards and guidelines required under subsection (a), the Director of OMB shall review agency information security policies and principles on the basis of the standards and guidelines published under subsection (a) pertaining to Internet of Things devices owned or controlled by agencies (excluding agency information security policies and principles pertaining to Internet of Things of devices owned or controlled by agencies that are or comprise a national security system) for consistency with the standards and guidelines submitted under subsection (a) and