

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 1501(17) of title 6.

(Pub. L. 116-207, §3, Dec. 4, 2020, 134 Stat. 1001.)

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 notes under this section and section 271 of this title. 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.

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—