Public Law 116–207
116th Congress

An Act

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.

Dec. 4, 2020
[H.R. 1668]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

Internet of Things Cybersecurity Improvement Act of 2020.
15 USC 271 note.

This Act may be cited as the "Internet of Things Cybersecurity Improvement Act of 2020" or the "IoT Cybersecurity Improvement Act of 2020".

SEC. 2. SENSE OF CONGRESS.

15 USC 278g–3a note.

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.

SEC. 3. DEFINITIONS.

15 USC 278g–3a.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given that term in section 3502 of title 44, United States Code.

(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, United States Code.

(5) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3552(b)(6) of title 44, United States Code.

(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 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)).

15 USC 278g–3b.

SEC. 4. 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.—

Deadline. Publication.

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Institute shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) 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 the date of the enactment of this Act—

(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 issue such policies and principles as may be necessary to ensure those policies and principles are consistent with such standards and guidelines. Deadline.

(2) REVIEW.—In reviewing agency information security policies and principles under paragraph (1) and issuing policies and principles under such paragraph, as may be necessary, the Director of OMB shall—

(A) consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; and Consultation.

(B) ensure such policies and principles are consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code.

(3) NATIONAL SECURITY SYSTEMS.—Any policy or principle issued by the Director of OMB under paragraph (1) shall not apply to national security systems.

(c) QUINQUENNIAL REVIEW AND REVISION.— Deadlines.

(1) REVIEW AND REVISION OF NIST STANDARDS AND GUIDELINES.—Not later than 5 years after the date on which the Director of the Institute publishes the standards and guidelines under subsection (a), and not less frequently than once every 5 years thereafter, the Director of the Institute, shall—

(A) review such standards and guidelines; and

(B) revise such standards and guidelines as appropriate.

(2) UPDATED OMB POLICIES AND PRINCIPLES FOR AGENCIES.—Not later than 180 days after the Director of the Institute makes a revision pursuant to paragraph (1), the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall update any policy or principle issued under subsection (b)(1) as necessary to ensure those policies and principles are consistent with the review and any revision under paragraph (1) under this subsection and paragraphs (2) and (3) of subsection (b). Consultation.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement any standards and guidelines promulgated in this section.

15 USC 278g–3c.

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

Deadline. Consultation. Publication.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Institute, in consultation with such cybersecurity researchers and private sector industry experts as the Director considers appropriate, and in consultation with the Secretary, shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) guidelines—

(1) for the reporting, coordinating, publishing, and receiving of information about—

(A) a security vulnerability relating to information systems owned or controlled by an agency (including Internet of Things devices owned or controlled by an agency); and

(B) the resolution of such security vulnerability; and

(2) for a contractor providing to an agency an information system (including an Internet of Things device) and any subcontractor thereof at any tier providing such information system to such contractor, on—

(A) receiving information about a potential security vulnerability relating to the information system; and

(B) disseminating information about the resolution of a security vulnerability relating to the information system.

(b) ELEMENTS.—The guidelines published under subsection (a) shall—

(1) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely-used standard;

(2) incorporate guidelines on—

(A) receiving information about a potential security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(B) disseminating information about the resolution of a security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(3) be consistent with the policies and procedures produced under section 2009(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

(c) INFORMATION ITEMS.—The guidelines published under subsection (a) shall include example content, on the information items that should be reported, coordinated, published, or received pursuant to this section by a contractor, or any subcontractor thereof at any tier, providing an information system (including Internet of Things device) to the Federal Government.

(d) OVERSIGHT.—The Director of OMB shall oversee the implementation of the guidelines published under subsection (a).

Consultation.

(e) OPERATIONAL AND TECHNICAL ASSISTANCE.—The Secretary, in consultation with the Director of OMB, shall administer the implementation of the guidelines published under subsection (a) and provide operational and technical assistance in implementing such guidelines.

SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

Consultation.
15 USC 278g–3d.

(a) AGENCY GUIDELINES REQUIRED.—Not later than 2 years after the date of the enactment of this Act, the Director of OMB, in consultation with the Secretary, shall develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including Internet of Things devices).

Deadline.

(b) OPERATIONAL AND TECHNICAL ASSISTANCE.—Consistent with section 3553(b) of title 44, United States Code, the Secretary, in consultation with the Director of OMB, shall provide operational and technical assistance to agencies on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems (including Internet of Things devices).

(c) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the assistance provided under subsection (b) is consistent with applicable standards and publications developed by the Director of the Institute.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INTERNET OF THINGS DEVICES.

15 USC 278g–3e.

(a) PROHIBITION ON PROCUREMENT AND USE.—

(1) IN GENERAL.—The head of an agency is prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an Internet of Things device, if the Chief Information Officer of that agency determines during a review required by section 11319(b)(1)(C) of title 40, United States Code, of a contract for such device that the use of such device prevents compliance with the standards and guidelines developed under section 4 or the guidelines published under section 5 with respect to such device.

Determination.

(2) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under paragraph (1) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

Applicability.

(b) WAIVER.—

(1) AUTHORITY.—The head of an agency may waive the prohibition under subsection (a)(1) with respect to an Internet of Things device if the Chief Information Officer of that agency determines that—

Determination.

(A) the waiver is necessary in the interest of national security;

(B) procuring, obtaining, or using such device is necessary for research purposes; or

(C) such device is secured using alternative and effective methods appropriate to the function of such device.

(2) AGENCY PROCESS.—The Director of OMB shall establish a standardized process for the Chief Information Officer of each agency to follow in determining whether the waiver under paragraph (1) may be granted.

(c) REPORTS TO CONGRESS.—

Time period.

(1) REPORT.—Every 2 years during the 6-year period beginning on the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report—

(A) on the effectiveness of the process established under subsection (b)(2);

Recommendations.

(B) that contains recommended best practices for the procurement of Internet of Things devices; and

Lists.

Time period.

(C) that lists—

(i) the number and type of each Internet of Things device for which a waiver under subsection (b)(1) was granted during the 2-year period prior to the submission of the report; and

(ii) the legal authority under which each such waiver was granted, such as whether the waiver was granted pursuant to subparagraph (A), (B), or (C) of such subsection.

(2) CLASSIFICATION OF REPORT.—Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex that contains the information described under paragraph (1)(C).

(d) EFFECTIVE DATE.—The prohibition under subsection (a)(1) shall take effect 2 years after the date of the enactment of this Act.

SEC. 8. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON CYBERSECURITY CONSIDERATIONS STEMMING FROM THE CONVERGENCE OF INFORMATION TECHNOLOGY, INTERNET OF THINGS, AND OPERATIONAL TECHNOLOGY DEVICES, NETWORKS, AND SYSTEMS.

Deadline.

(a) BRIEFING.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall provide a briefing to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts, including projects designed to assist in managing potential security vulnerabilities associated with the use of traditional information technology devices, networks, and systems with—

(1) Internet of Things devices, networks, and systems; and

(2) operational technology devices, networks, and systems.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General shall submit a report to the

Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts addressed in subsection (a).

Approved December 4, 2020.

LEGISLATIVE HISTORY—H.R. 1668 (S. 734):

HOUSE REPORTS: No. 116–501, Pt. 1 (Comm. on Oversight and Reform).
SENATE REPORTS: No. 116–112 (Comm. on Homeland Security and Governmental Affairs) accompanying S. 734.
CONGRESSIONAL RECORD, Vol. 166 (2020):
Sept. 14, considered and passed House.
Nov. 17, considered and passed Senate.

○