(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.

**(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

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

**(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**

**(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).

**(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.

(Pub. L. 116–207, § 4, Dec. 4, 2020, 134 Stat. 1002.)

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.

DEFINITIONS

For definitions of terms used in this section, see section 278g–3a of this title.

### § 278g–3c. Guidelines on the disclosure process for security vulnerabilities relating to information systems, including Internet of Things devices

**(a) In general**

Not later than 180 days after December 4, 2020, 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 278g–3 of this title 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 659(m) of title 6.

**(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).

**(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.

(Pub. L. 116–207, § 5, Dec. 4, 2020, 134 Stat. 1004.)

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.

DEFINITIONS

For definitions of terms used in this section, see section 278g–3a of this title.

### § 278g–3d. Implementation of coordinated disclosure of security vulnerabilities relating to agency information systems, including Internet of Things devices

**(a) Agency guidelines required**

Not later than 2 years after December 4, 2020, 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).

**(b) Operational and technical assistance**

Consistent with section 3553(b) of title 44, 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.

(Pub. L. 116–207, § 6, Dec. 4, 2020, 134 Stat. 1005.)

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.

DEFINITIONS

For definitions of terms used in this section, see section 278g–3a of this title.

### § 278g–3e. Contractor compliance with coordinated disclosure of security vulnerabilities relating to agency Internet of Things devices

**(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 of a contract for such device that the use of such device prevents compliance with the standards and guidelines developed under section 278g–3b of this title or the guidelines published under section 278g–3c of this title with respect to such device.

**(2) Simplified acquisition threshold**

Notwithstanding section 1905 of title 41, the requirements under paragraph (1) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

**(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—

(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 Offi-