

**§ 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 Officer of each agency to follow in determining whether the waiver under paragraph (1) may be granted.

**(c) Reports to Congress**

**(1) Report**

Every 2 years during the 6-year period beginning on December 4, 2020, 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);
- (B) that contains recommended best practices for the procurement of Internet of Things devices; and
- (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 December 4, 2020.

(Pub. L. 116-207, § 7, Dec. 4, 2020, 134 Stat. 1005.)

**Editorial Notes**

**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.

**Statutory Notes and Related Subsidiaries**

**DEFINITIONS**

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

**§ 278g-4. Information Security and Privacy Advisory Board**

**(a) Establishment and composition**

There is hereby established a<sup>1</sup> Information Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

- (1) four members from outside the Federal Government who are eminent in the information technology industry, at least one of whom is representative of small or medium sized companies in such industries;
- (2) four members from outside the Federal Government who are eminent in the fields of information technology, or related disciplines, but who are not employed by or representative of a producer of information technology; and
- (3) four members from the Federal Government who have information system management experience, including experience in information security and privacy, at least one of whom shall be from the National Security Agency.

**(b) Duties**

The duties of the Board shall be—

- (1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- (2) to advise the Institute, the Secretary of Homeland Security, and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including through review of proposed standards

<sup>1</sup> So in original. Probably should be "an".