AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 1668 OFFERED BY MS. KELLY OF ILLINOIS

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Internet of Things Cybersecurity Improvement Act of 2019'' or the ''IoT Cybersecurity Improvement Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act:

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

(2) COVERED DEVICE.—The term ''covered device'' means a physical object that—

(A) is capable of being in regular connection with—

(i) the Internet; or

(ii) a network that is connected to the Internet on a recurring basis;

(B) has computer processing capabilities of collecting, sending, or receiving data; and

(C) is not a—

(i) general-purpose computing device;

(ii) personal computing system;

(iii) smart mobile communications device;

(iv) programmable logic controller with an industrial control system specifically not designed for connection to the internet;

(v) mainframe computing system; or

(vi) subcomponent of a device.

(3) DIRECTOR OF OMB.—The term ''Director of OMB'' means the Director of the Office of Management and Budget.

(4) DIRECTOR OF THE INSTITUTE.—The term ''Director of the Institute'' means the Director of the National Institute of Standards and Technology.

(5) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given that term under section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)).

SEC. 3. COMPLETION OF ONGOING EFFORTS RELATING TO CONSIDERATIONS FOR MANAGING INTERNET OF THINGS CYBERSECURITY RISKS.

Not later than December 31, 2019, the Director of the National Institute of Standards and Technology shall complete the efforts of the Institute in effect on the date of the enactment of this Act regarding considerations for managing the security vulnerabilities of Internet of Things devices and examples of possible cybersecurity capabilities of such devices by publishing a report that includes, at a minimum, the following considerations for covered devices:

(1) Secure development.

(2) Identity management.

(3) Patching.

(4) Configuration management.

SEC. 4. SECURITY STANDARDS FOR USE OF COVERED DEVICES BY THE FEDERAL GOVERNMENT.

(a) GUIDELINES REQUIRED.—

(1) GUIDELINES.—Not later than 6 months after the date on which the report under section 3 is completed, the Director of the Institute shall develop under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), and submit to the Director of OMB, guidelines on—

(A) the appropriate use and management by the agencies of covered devices owned or controlled by the agencies; and

(B) minimum information security requirements for managing security vulnerabilities associated with such devices.

(2) DEVELOPMENT OF GUIDELINES.—In developing the guidelines submitted under paragraph (1), the Director of the Institute shall—

(A) consider relevant standards and best practices developed by the private sector, agencies, and public-private partnerships; and

(B) ensure that such guidelines are consistent with the considerations published in the report described under section 3.

(b) PROMULGATION OF STANDARDS.—

(1) STANDARDS.—Not later than 180 days after the date on which the Director of the Institute completes the development of the guidelines required under subsection (a), the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall—

(A) promulgate standards on the basis of the guidelines submitted under subsection (a)

pertaining to covered devices owned or controlled by agencies, except those considered national security systems as defined by section 3552(b)(6) of title 44, United States Code; and

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

(2) QUINQUENNIAL REVIEW AND REVISION.—Not later than 5 years after the date on which the Director of OMB promulgates the standards under paragraph (1), and not less frequently than once every 5 years thereafter, the Director of OMB, in consultation with and the Director of the Institute and the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall—

(A) review such standards; and

(B) revise such standards as appropriate.

(c) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised to implement any standard promulgated under subsection (b).

SEC. 5. PETITION TO EXCLUDE CERTAIN DEVICES.

(a) PETITION.—The Director of OMB shall establish a process by which an interested party may petition the Director of OMB for a device described in section 2(2) to not be considered a covered device for the purpose of standards promulgated under section 4(b).

(b) GRANTS OF PETITION.—The Director of OMB shall grant a petition under subsection (a)—

(1) on a limited basis;

(2) in a timely manner; and

(3) only if the interested party demonstrates that—

(A) the procurement of such a covered device with limited data processing and software functionality would be unfeasible; or

(B) the procurement of a covered device that does not meet the standards promulgated by the Director of OMB under this Act is necessary for national security or for research purposes.

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter for each of the following four years, the Director of OMB shall submit to the appropriate congressional committees a report on the process es-

tablished by the Director of OMB for granting or denying waivers under this section.

(2) ASSESSMENT OF IMPLEMENTATION.—The reports required under paragraph (1) shall include, at a minimum, the following:

(A) An assessment of the waiver evaluation process.

(B) A description of the methods established to carry out such assessment.

(C) A classified appendix listing the types and number of devices for each agency granted a waiver and the reasons for such waiver.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term ''appropriate congressional committees'' means the Committees on Oversight and Reform and Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

SEC. 6. COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO COVERED DEVICES.

(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 the Director of Cybersecurity

and Infrastructure Security Agency of the Department of Homeland Security, shall develop under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and submit to the Director of OMB, guidelines—

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

(A) a security vulnerability relating to a covered device owned or controlled by an agency; and

(B) the resolution of such security vulnerability; and

(2) for contractors providing a covered device to the Federal Government, and any subcontractor thereof at any tier providing such device to such contractors on—

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

(B) disseminating information about the resolution of a security vulnerability relating to the covered device;

(3) on the type of information about security vulnerabilities that should be reported to the Federal Government, including examples thereof.

(b) DEVELOPMENT OF GUIDELINES.—In developing the guidelines under subsection (a), the Director of the Institute shall—

(1) consult with such cybersecurity researchers and private sector industry experts as the Director considers appropriate;

(2) to the maximum extent practicable, align such guidelines with Standards 29147 and 30111 of the International Standards Organization, or any successor standards thereof; and

(3) ensure such guidelines are consistent with the policies and procedures developed under section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

(c) PROMULGATION OF STANDARDS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the guidelines under subsection (a) are submitted, the Director of OMB, in consultation with the Administrator of General Services and the Secretary of Homeland Security, shall promulgate standards on the basis of such guidelines.

(2) CONTRACT REQUIREMENT FOR SUBCONTRACTS.—The standards promulgated under paragraph (1) shall include a requirement for any

contract related to a covered device to include a clause that requires each contractor that provides a covered device under the contract to an agency to ensure that any covered device obtained through a subcontract, at any tier, complies with the standards and regulations promulgated under this section with respect to such covered device.

(3) CONSISTENCY WITH THE STRENGTHENING AND ENHANCING CYBER-CAPABILITIES BY UTILIZING RISK EXPOSURE TECHNOLOGY ACT.—The Director of OMB shall ensure that the standards promulgated under paragraph (1) are consistent with section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (6 U.S.C. 663 note; Public Law 115–390).

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised to implement the standards promulgated under subsection (c).

SEC. 7. CONTRACTOR COMPLIANCE WITH STANDARDS AND REGULATIONS.

(a) IN GENERAL.—

(1) DETERMINATION.—

(A) COMPLIANCE REQUIRED.—Before awarding a contract to an offeror for the pro-

curement of a covered device, or renewing a contract to procure or obtain a covered device from a contractor, the agency Chief Information Officer shall determine if such offeror or contractor has complied with each standard promulgated under section 6(c) with respect to such covered device.

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

(2) PROHIBITION ON USE OR PROCUREMENT.—The head of an agency may not procure or obtain, or renew a contract to procure or obtain, a covered device if the agency Chief Information Officer determines under paragraph (1)(A) that such offeror or contractor has not complied with a standard promulgated under section 6(c) with respect to such covered device.

(b) WAIVER.—The head of an agency may waive the prohibition under subsection (a)(2) if the procurement of such covered device is necessary for national security or for research purposes.

(c) EFFECTIVE DATE.—The prohibition under subsection (a) shall take effect one year after the date of the enactment of this Act.

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

Not later than 1 year after the date of the enactment of this Act, the Director of the Institute shall publish a report on the increasing convergence, including considerations for managing potential security vulnerabilities associated with such convergence, of traditional information technology devices, networks, and systems with—

(1) covered devices, networks and systems; and

(2) operational technology devices, networks and systems.

☒