.....

(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. _____

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Ms. KELLY of Illinois introduced the following bill; which was referred to the Committee on _____

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Internet of Things (IoT) Federal Cybersecurity Improvement Act of 2018''.

SEC. 2. FINDINGS; SENSE OF CONGRESS.

(a) FINDINGS.—Congress finds the following:

(1) The trust of the American people in the safety and security of their Government's digital technologies, including the Internet of Things, is vital for advancing digital technology transformation.

(2) Digital technology transformation portends tremendous opportunity for our nation to improve the daily lives of the American people and grow the economy.

(3) The risk of exposure of Government, businesses, and individual citizens to malicious cyber-attacks grows dramatically if digital transformation is not managed with vigorous attention to cybersecurity concerns, and failure to protect the Government systems that control our critical infrastructure and essential Government networks could have devastating consequences.

(4) Intelligence and national security leaders, including the Director of the Defense Intelligence Agency, have described Internet of Things (IoT) devices as among the ''most important emerging cyberthreats to our national security''.

(5) The Federal Government cannot achieve a high level of cybersecurity unless cybersecurity be-

comes the task of every person involved with Federal networks and devices.

(6) Anchoring responsibility for cybersecurity at the top of governmental organizations is critical to set the correct mindset that enhancing cybersecurity of the Federal Government's networks and devices is the responsibility of every Government employee to the extent practicable.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) ensuring the highest level of cybersecurity at Government agencies is the responsibility of the President, followed by the Director of the Office of Management and Budget, and the head of each executive agency;

(2) this responsibility is to be carried out by working collaboratively within and among executive agencies, industry, and academia; and

(3) the strength of the Government's cybersecurity and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the Government's acquisition and operation of IoT devices.

SEC. 3. CONTRACTOR MINIMUM SECURITY REQUIREMENTS FOR COVERED DEVICES.

(a) STANDARD SECURITY CLAUSE REQUIRED IN COVERED DEVICES.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director in consultation with the Secretary of Defense, the Administrator of General Services, the Secretary of Commerce, the Secretary of Homeland Security, and any other intelligence or national security agency that the Director determines to be necessary shall issue guidelines for each executive agency that require the inclusion of a standard security clause in any contract (except as provided in paragraph (4)) for the acquisition of covered devices.

(2) CONTENTS OF STANDARD SECURITY CLAUSE.—The standard security clause required under paragraph (1) shall—

(A) establish baseline security requirements that address aspects of device security relating to covered devices, including—

(i) a requirement that software or firmware components accept properly authenticated and trusted updates from the vendor;

(ii) requirements relating to identity and access management, including a prohibition of the use of fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication;

(iii) a requirement that the contractor participate in a coordinated vulnerability disclosure program training on the guidelines issued pursuant to subsection (f); and

(iv) any other requirement the Director determines to be appropriate;

(B) require contractors to provide written attestation that the device meets such requirements as established under subparagraph (A);

(C) to the maximum extent practicable, ensure that the requirements established under subparagraph (A) are—

(i) tailored to address the characteristics of different types of devices, including risk and intended function;

(ii) based on technology-neutral, outcome-based security principles;

(iii) developed through a transparent process that incorporates input from rel-

evant stakeholders in industry and academia;

(iv) aligned with internationally recognized technical standards; and

(v) updated regularly based on developments in technology and security methodologies;

(D) an identification of contractor responsibilities to ensure that a covered device software or firmware component is updated or replaced, consistent with other provisions in the contract governing the term of support, in a manner that allows for any future security vulnerability or defect in any part of the software or firmware to be patched, based on risk, in order to fix or remove a vulnerability or defect in the software or firmware component in a properly authenticated and secure manner; and

(E) a requirement for the contractor to provide the purchasing agency with general information on the ability of the device to be updated, such as—

(i) the manner in which the device receives security updates;

(ii) the business terms, including any fees for ongoing security support, under which security updates will be provided for a covered device;

(iii) the anticipated timeline for ending security support associated with the covered device;

(iv) formal notification when security support has ceased; and

(v) any other information the Director determines to be necessary.

(3) VOLUNTARY CONSENSUS STANDARDS.—The Director shall ensure that, to the maximum extent practicable, the baseline security described in paragraph (2)(A) reflects and aligns with existing voluntary consensus standards.

(4) WAIVER OF REQUIREMENT BY AGENCIES.—The Director may establish a process for the Chief Information Officer of an executive agency to waive the requirements under this subsection for a case in which a petition is submitted by an entity seeking to enter into a contract with the executive agency and the following requirements are met:

(A) A waiver is granted only in limited circumstances, including when an entity dem-

onstrates that a covered device meets a desired level of security through means other than those required under paragraph (2)(A) or when the executive agency reasonably believes that procurement of a covered device with limited data processing and software functionality would be unfeasible or economically impractical.

(B) The Chief Information Officer of an executive agency that approves a waiver under this paragraph shall provide the entity a written statement that the executive agency accepts any risk resulting from use of the covered device.

(5) ALIGNMENT WITH FISMA.—In issuing the guidelines required under paragraph (1), the Director, in consultation with the Administrator of General Services, shall ensure that such guidelines are, to the greatest extent practicable, consistent with, non-duplicative of, and in compliance with any applicable established information security policies, procedures, standards, and compliance requirements under the subchapter II of chapter 35 of title 44, United States Code.

(b) ALTERNATE CONDITIONS TO MITIGATE CYBERSECURITY RISKS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director, in consultation with NIST, shall define a set of conditions that—

(A) ensure a non-compliant device can be used with a level of security that is equivalent or greater to the baseline security requirements described in subsection (a)(2); and

(B) shall be met in order for an executive agency to purchase such a non-compliant device.

(2) REQUIREMENTS.—In defining the set of conditions that must be met for non-compliant devices required under paragraph (1), the Director, in consultation with NIST and relevant industry entities, may consider the use of conditions, including—

(A) network segmentation or micro-segmentation;

(B) the adoption of system level security controls, including operating system containers and microservices;

(C) multi-factor authentication; and

(D) intelligent network solutions and edge systems, such as gateways, that can isolate, disable, or remediate connected devices.

(3) SPECIFICATION OF ADDITIONAL PRECAUTIONS.—To address the long-term risk of non-compliant devices acquired in accordance with an exception under this subsection, the Director, in consultation with NIST and private-sector industry experts and, with respect to medical devices regulated under the Federal Food, Drug, and Cosmetics Act, in consultation with the Commissioner of Food and Drugs, may stipulate additional requirements for management and use of non-compliant devices, including deadlines for the removal, replacement, or disabling of non-compliant devices (or their Internet-connectivity), as well as minimal requirements for gateway products to ensure the integrity and security of the non-compliant devices.

(4) EXISTING THIRD-PARTY SECURITY STANDARD.—

(A) IN GENERAL.—If a voluntary consensus standard for the security of covered devices provides an equivalent or greater level of security to that described in subsection (a)(2), the Director shall modify the requirements under subsection (a)(1) and the security clause under subsection (a)(2) to reflect conformity with that voluntary consensus standard .

(B) WRITTEN CERTIFICATION.—A contractor providing a covered device shall provide third-party written certification that the device complies with the security requirements of the industry certification method of the third party.

(C) NIST.—NIST, in consultation with the Director and the heads of other appropriate executive agencies, shall determine—

(i) accreditation standards for third-party certifiers; and

(ii) whether the standards described in clause (i) provide appropriate security and are aligned with the guidelines issued under subsection (a).

(5) EXISTING AGENCY SECURITY EVALUATION STANDARDS.—

(A) IN GENERAL.—If an executive agency employs a security evaluation process or criteria for covered devices that the agency believes provides an equivalent or greater level of security to the baseline security requirements described in subsection (a)(2), an executive agency may, upon the approval of the Director, continue to use that process or criteria in lieu of the requirements under subsection (a)(2).

(B) NIST.—NIST, in consultation with the Director and the heads of other appropriate executive agencies, shall determine whether the process or criteria described in subparagraph (A) provides appropriate security and is aligned with the guidelines issued under subsection (a).

(c) GUIDELINES FOR LOWEST PRICE TECHNICALLY ACCEPTABLE SOURCE SELECTION.—Not later than 180 days after the date of the enactment of this Act, the Director, in consultation with the Administrator of General Services, shall issue guidelines for each executive agency to limit, to the maximum extent practicable, the use of lowest price technically acceptable source selection criteria in the case of a procurement that is predominately for the acquisition of a covered device.

(d) REPORT TO CONGRESS.—Not later than 5 years after the date of the enactment of this Act, the Director shall submit to Congress a report on the effectiveness of the guidelines required to be issued under subsections (a) and (c), which shall include recommendations, if any, for legislation necessary to improve cybersecurity in executive agency acquisition of covered devices.

(e) GENERAL WAIVER AUTHORITY FOR DIRECTOR.—Beginning on the date that is 5 years after the date of the enactment of this Act, the Director may waive, in

whole or in part, the requirements of the guidelines or set of conditions issued under this section, for an executive agency.

(f) GUIDELINES REGARDING THE COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES AND DEFECTS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director, in consultation with the Department of Homeland Security and the Department of Justice, and cybersecurity researchers and private-sector industry experts, shall issue guidelines for each executive agency with respect to any covered device in use by the United States Government regarding cybersecurity coordinated disclosure requirements that shall be required of contractors providing such covered devices to those executive agencies.

(2) CONTENTS.—The guidelines required under paragraph (1) shall include policies and procedures for the processing and resolving of potential vulnerability information relating to a covered device, which shall be, to the maximum extent practicable, aligned with Standards 29147 and 30111 of the International Standards Organization, or any successor standard, such as—

(A) procedures for the provision of a covered device to executive agencies by a contractor on how to—

(i) receive information about potential vulnerabilities in the product or online service of the contractor; and

(ii) disseminate resolution information about vulnerabilities in the product or online service of the contractor; and

(B) guidance, including example content, on the information items that should be produced through the implementation of the vulnerability disclosure process of the contractor.

(g) REVISION OF FAR.—The Federal Acquisition Regulations System shall be revised to require the inclusion of a standard security clause consistent with the requirements of this section.

SEC. 4. INVENTORY OF DEVICES.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the head of each executive agency shall establish and maintain an inventory of covered devices used by the agency procured under the requirements of this Act.

(b) GUIDELINES.—Not later than 30 days after the date of the enactment of this Act, the Director, in con-

sultation with the Secretary of Homeland Security, shall issue guidelines for executive agencies to develop and manage the inventories required under subsection (a), based on the Continuous Diagnostics and Mitigation program used by the Department of Homeland Security.

(c) DEVICE DATABASES.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Director shall establish and maintain—

(A) a database of non-compliant devices and the manufacturers of such devices; and

(B) a database of covered devices and the manufacturers of such devices about which the Government has received formal notification of security support ceasing, as required under section 3(a)(2)(E)(iv).

(2) UPDATES.—The Secretary of Homeland Security shall update the databases established under paragraph (1) not less frequently than every 30 days.

SEC. 5. USE OF BEST PRACTICES IN IDENTIFICATION AND TRACKING OF VULNERABILITIES FOR PURPOSES OF THE NATIONAL VULNERABILITY DATABASE.

The Director of NIST shall ensure that NIST establishes, maintains, and uses best practices in the identification and tracking of vulnerabilities for purposes of the National Vulnerability Database of NIST.

SEC. 6. DEFINITIONS.

In this Act:

(1) COVERED DEVICE.—

(A) IN GENERAL.—The term ''covered device''—

(i) means a physical object that—

(I) is capable of connecting to and is in regular connection with the Internet; and

(II) has computer processing capabilities that can collect, send, or receive data; and

(ii) does not include advanced or general-purpose computing devices, including personal computing systems, smart mobile communications devices, programmable logic controls, and mainframe computing systems.

(B) OMB EXEMPTION.—The Director may exempt additional devices under subparagraph (A)(ii) through a process in which interested parties may submit a petition for the exemption. The Director shall act in an expedited manner on any such petition submitted.

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

(3) EXECUTIVE AGENCY.—The term ''executive agency'' has the meaning given the term in section 133 of title 41, United States Code.

(4) FIRMWARE.—The term ''firmware'' means a computer program and the data stored in hardware, typically in read-only memory or programmable read-only memory, such that the program and data cannot be dynamically written or modified during execution of the program.

(5) FIXED OR HARD-CODED CREDENTIAL.—The term ''fixed or hard-coded credential'' means a value, such as a password, token, cryptographic key, or other data element used as part of an authentication mechanism for granting remote access to an information system or the information of the system, that is—

(A) established by a product vendor or service provider; and

(B) incapable of being modified or revoked by the user or manufacturer lawfully operating the information system, except through a firmware update.

(6) GATEWAY PRODUCT.—The term ''gateway product'' means a node or device that connects to multiple networks using standard protocols.

(7) HARDWARE.—The term ''hardware'' means the physical components of an information system.

(8) NIST.—The term ''NIST'' means the National Institute of Standards and Technology.

(9) NON-COMPLIANT DEVICE.—The term ''non-compliant device'' means a covered device that does not meet the baseline security requirements established in section 3(a)(2)(A).

(10) PROPERLY AUTHENTICATED UPDATE.—The term ''properly authenticated update'' means an update, remediation, or technical fix to a hardware, firmware, or software component issued by a product vendor or service provider used to correct particular problems with the component, and that, in the case of software or firmware, contains some method of authenticity protection, such as a digital

signature, so that unauthorized updates and rollbacks of authorized updates can be automatically detected and rejected.

(11) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, firmware, software, process, or procedure or a combination of 2 or more of these attributes that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or the information or physical devices of an information system to which an information system is connected.

(12) SOFTWARE.—The term ''software'' means a computer program and associated data that may be dynamically written or modified.

(13) VENDOR.—The term ''vendor'', with respect to a technology, product, system, service, or application, means—

(A) in the case of a purchase by the Government, the entity that developed the technology, product, system, service, or application; or

(B) in the case of a purchase by a contractor, the entity that is responsible for main-

taining the technology, product, system, service, or application.

SEC. 7. APPLICABILITY.

This Act shall apply with respect to any contract entered into on and after the date on which the guidelines are issued pursuant to section 3(a).