ISM ORIGINAL WORK

S. 1691 [REVISED]

MANAV SOOD, AKASH BASKARAN

To provide minimal cybersecurity operational standards for Internet-connected devices purchased and operated within U.S. territory, and for other purposes.

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased and operated within U.S. territory, 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) Cybersecurity Improvement Act of 2018”.

SEC. 2. DEFINITIONS.

In this Act:

(1) Director.--The term ``Director'' means the Director of the Office of Management and Budget.

(2) Executive agency.--The term ``executive agency'' has the meaning given the term in section 133 of title 41, United States Code.

(3) Firmware.--The term ``firmware'' means a computer program and the data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the

program and data cannot be dynamically written or modified during execution of the program.

(4) 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 its information, 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 via a firmware update.

(5) Hardware.--The term ``hardware'' means the physical components of an information system.

(6) Internet-connected device.--The term ``Internet- connected device'' means a physical object that--

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

(B) has computer processing capabilities that can collect, send, or receive data.

(7) NIST.--The term ``NIST'' means the National Institute of Standards and Technology.

(8) 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 can be automatically detected and rejected.

(9) Security vulnerability.--The term ``security vulnerability'' means any attribute of hardware, firmware, software, process, or procedure or combination of 2 or more of these factors that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected.

(10) Software.--The term ``software'' means a computer program and associated data that may be dynamically written or Modified.

(11) U.S. Territory.--The term “U.S. Territory” means any extent of region under the sovereign jurisdiction of the federal government of the United States, including all waters

(around islands or continental tracts) and all U.S. naval vessels.
(12) Commercial Enterprise.--The term “Commercial Enterprise” means any for-profit entity formed for the ongoing conduct of lawful business with evidenced use of internet connected devices that sends, receives, or stores consumer data.
(13) Purchasing Entity.--The term “Purchasing Agency” means any entity, including executive agencies, commercial enterprise, and consumers, purchasing an internet-connected device for use.
(14) IoMT Device.--The term ``IoMT device'' means an internet-connected device that is used in the context of medical or healthcare-related applications.
(15) IoFT Device.--Internet-connected device.--The term ``IoFT device'' means an internet-connected device that is used in the context of financial related applications such as insurance or banking.
(16) Threat Actor.--The term “Threat Actor” means an entity that is partially or wholly responsible for an incident that negatively impacts, or has the potential to impact the security or operation of a commercial enterprise.
(17) Secure boot.--The term “Secure boot” means the firmware functionality that prevents malicious software applications and unauthorized operating systems from loading during the start-up process of the internet-connected device.
(18) Encryption.--The term “Encryption” means the process of converting information or data into a code, especially to prevent unauthorized access.
(19) Two-Factor Authentication.--The term “Two-factor Authentication” refers to the practice of securing devices with two authentication or user-verification methods.
(20) PHI.--The acronym “PHI” stands for Protected Health Information, which means information about health status, provision of health care, or payment for health care that is created or collected by health plans,health care clearinghouses, or health care providers who electronically transmit any health information and can be linked to a specific individual.
(21) BYOD.-- The acronym “BYOD” stands for “Bring Your Own Device”, which means the practice of allowing the employees of an organization to use their own computers, smartphones, or other internet-connected devices for work purposes.

(22) Biometric.-- The term “Biometric” means the measurement and statistical analysis of people's unique physical and behavioral characteristics.
(23) Medical Organization.-- The term “Medical Organization” refers to an institution dealing with human condition and health, such as hospitals, health centers, clinics, etc.
(24) Financial Organization.-- The term “Financial Institution” means a company engaged in the business of dealing with monetary transactions, such as deposits, loans, investments and currency exchange.

SEC. 3. CONTRACTOR RESPONSIBILITIES WITH RESPECT TO INTERNET-CONNECTED DEVICE CYBERSECURITY.

(a) Clauses Required in Internet-Connected 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 purchasing entity to require the following clauses in any contract, except as provided in paragraph (2), for the acquisition of Internet-connected devices:
(A) Verification required.--
(i) In general.--A clause that requires the contractor providing the Internet-connected device to provide written certification that the device--
(I) except as provided under clause (ii), does not contain, at the time of submitting the proposal, any hardware, software, or firmware component with any known security vulnerabilities or defects listed in--
(aa) the National Vulnerability Database of NIST; and
(bb) any additional database selected by the Director that tracks security vulnerabilities and defects, is credible, and is similar to the National Vulnerability Database;

(II) relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;

(III) uses only non-deprecated industry-standard protocols and technologies for functions such as--

(aa) communications, such as standard ports for network traffic;

(bb) encryption; and

(cc) interconnection with other devices or peripherals; and

(IV) does not include any fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication.

(ii) Limited exception for disclosed vulnerabilities.--

(I) Application for waiver.--At the time of submitting a proposal to a purchasing entity, a contractor may submit a written application for a waiver from the requirement under clause (i)(I) for the purpose of disclosing a known vulnerability to the Purchasing entity.

(II) Contents.--An application submitted under subclause (I) shall--

(aa) identify the specific known vulnerability;

(bb) include any mitigation actions that may limit or eliminate the ability for an adversary or threat actor to exploit the vulnerability; and

(cc) include a justification for secure use of the device notwithstanding the persisting vulnerability.

(III) Approval.--If the head of the purchasing entity approves the waiver, the head of the purchasing entity shall provide the contractor a written statement that the purchasing entity accepts such risks resulting from use of the device with the known vulnerability as represented by the contractor.

(B) Notification required.--A clause that requires the contractor providing the Internet-connected device software or firmware component to notify the purchasing

entity of any known security vulnerabilities or defects subsequently disclosed to the vendor by a security researcher or of which the vendor otherwise becomes aware for the duration of the contract.

(C) Updates.--A clause that requires such Internet-connected device software or firmware component to be 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 in order to fix or remove a vulnerability or defect in the software or firmware component in a properly authenticated and secure manner.

(D) Timely repair.--A clause that requires the contractor to provide a repair or replacement in a timely manner in respect to any new security vulnerability discovered through any of the databases described in subparagraph (A)(i)(I) or from the coordinated disclosure program described in subsection (b) in the event the vulnerability cannot be remediated through an update described in subparagraph (C).

(E) Continuation of services.--A clause that requires the contractor to provide the purchasing entity 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 anticipated timeline for ending security support associated with the Internet-connected device;

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

(iv) any additional information recommended by the National Telecommunications and Information Administration.

(2) Exceptions.--

(A) Devices with severely limited functionality.--

(i) In general.--If an executive agency reasonably believes that procurement of an Internet-connected device with limited data processing and software

functionality consistent with paragraph (1) would be unfeasible or economically impractical, the contractor may petition the Director for a waiver to the requirements contained in paragraph (1) in order to purchase a non-compliant Internet-connected device.

(ii) Alternate conditions to mitigate cybersecurity risks.--

(I) In general.--Not later than 180 days after the date of the enactment of this Act, the Director, in close coordination with NIST, shall define a set of conditions that--

(aa) ensure an Internet-connected device that does not comply with paragraph (1) can be used with a level of security that is equivalent to the level of security described in paragraph (1)(A); and

(bb) shall be met in order for a purchasing entity to purchase such a non-compliant device.

(II) Requirements.--In defining a set of conditions that must be met for non-compliant devices as required under subclause (I), the Director, in close coordination with NIST and relevant industry entities, may consider the use of conditions including--

(aa) network segmentation or micro-segmentation;

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

(cc) multi-factor authentication; and

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

(iii) Specification of additional precautions.--To address the long-term risk of non-compliant Internet-connected devices acquired in accordance with an exception under this paragraph, the Director, in coordination with NIST and private-sector industry experts, 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.

(B) Existing third-party security standard.--

(i) In general.--If an existing third-party security standard for Internet-connected devices provides an equivalent or greater level of security to that described in paragraph (1)(A), an executive agency may allow a contractor to demonstrate compliance with that standard in lieu of the requirements under paragraph (1).

(ii) Written certification.--A contractor providing the Internet-connected device shall provide third-party written certification that the device complies with the security requirements of the industry certification method of the third party.

(iii) NIST.--NIST, in coordination with the Director and other appropriate executive agencies, shall determine--

(I) accreditation standards for third-party certifiers; and (II) whether the standards described in subclause (I) provide appropriate security and is aligned with the guidelines issued under this subsection.

(C) Existing agency security evaluation standards.--

(i) In general.--If an executive agency or commercial enterprise employs a security evaluation process or criteria for Internet-connected devices that the agency believes provides an equivalent or greater level of security to that described in paragraph (1)(A), an executive agency may, upon the approval of the Director, continue to use that process or standard in lieu of the requirements under paragraph (1).

(ii) NIST.--NIST, in coordination with the Director and other appropriate executive agencies, shall determine whether the process or criteria described in clause (i) provides appropriate security and are aligned with the guidelines issued under this subsection.

(3) Report to congress.--Not later than 5 years after the date of enactment of this Act, the Director shall submit to Congress a report on the effectiveness of the guidelines required to be issued under paragraph (1), which shall include recommendations for legislative language needed to update the guideline requirements described in paragraph (1).

(4) Waiver authority.--Beginning on the date that is 5 years after the date of enactment of this Act, the Director may waive, in whole or in part, the requirements of the guidelines issued under this subsection.

(b) Guidelines Regarding the Coordinated Disclosure of Security Vulnerabilities and Defects.--

(1) In general.--Not later than 60 days after the date of the enactment of this Act, the National Protection and Programs Directorate, in consultation with cybersecurity researchers and private-sector industry experts, shall issue guidelines for each agency with respect to any Internet-connected device in use by the United States Government regarding cybersecurity coordinated disclosure requirements that shall be required of contractors providing such software devices to purchasing entities.

(2) Contents.--The guidelines required to be issued under paragraph (1) shall--

(A) include policies and procedures for conducting research on the cybersecurity of an Internet-connected device, which shall be based, in part, on Standard 29147 of the International Standards Organization, or any successor standard, relating to the processing and resolving of potential vulnerability information in a product or online service, such as--

(i) procedures for a contractor providing an Internet-connected device to a purchasing entity 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

(ii) guidance, including example content, on the information items that should be produced

through the implementation of the vulnerability disclosure process of the contractor; and

(B) require that research on the cybersecurity of an Internet-connected device provided by a contractor to the United States Government and any other purchasing entity shall be conducted on the same class, model, or type of the device provided to the United States Government and not on the actual device provided to the United States Government or purchasing entity.

(c) Limitation of Liability.--

(1) Rule of construction.--Nothing in this subsection, or the amendments made by this subsection, shall be construed to establish additional obligations or criminal penalties for individuals engaged in researching the cybersecurity of Internet-connected devices.

(2) Computer fraud and abuse act.--Section 1030 of title 18, United States Code, is amended--

(A) in subsection (j)(2), by adding a period at the end; and

(B) by adding at the end the following new subsection:

``(k) This section shall not apply to a person who--

``(1) in good faith, engaged in researching the cybersecurity of an Internet-connected device of the class, model, or type provided by a contractor to a department or agency of the United States; and

``(2) acted in compliance with the guidelines required to be issued by the National Protection and Programs Directorate, and adopted by the contractor described in paragraph (1), under section 3(b) of the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.''.

(3) Digital millennium copyright act.--Chapter 12 of title 17, United States Code, is amended--

(A) in section 1203, by adding at the end the following new subsection:

``(d) Limitation of Liability.--A person shall not be held liable under this section if the individual--

``(1) in good faith, engaged in researching the cybersecurity of an Internet-connected device of the class, model, or type provided by a contractor to a department or agency of the United States; and

``(2) acted in compliance with the guidelines required to be issued by the National Protection and Programs Directorate, and adopted by the contractor described in paragraph (1), under section 3(b) of the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.''; and

(B) in section 1204, by adding at the end the following new subsection:

``(d) Limitation of Liability.--Subsection (a) shall not apply to a person who--

``(1) in good faith, engaged in researching the cybersecurity of an Internet-connected device of the class, model, or type provided by a contractor to a department or agency of the United States; and

``(2) acted in compliance with the guidelines required to be issued by the National Protection and Programs Directorate, and adopted by the contractor described in paragraph (1), under section 3(b) of the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.''.

(d) Inventory of Devices.--

(1) In general.--Not later than 180 days after the date of the enactment of this Act, the head of each purchasing entity shall establish and maintain an inventory of Internet-connected devices used by the agency procured under this Act.

(2) Guidelines.--Not later than 30 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Secretary of Homeland Security, shall issue guidelines for purchasing entities to develop and manage the inventories required under paragraph (1), based on the Continuous Diagnostics and Mitigation (CDM) program used by the Department of Homeland Security.

(3) Device databases.--

(A) In general.--Not later than 180 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall establish and maintain--

(i) a publicly accessible database of devices and the respective manufacturers of such devices for which limitations of liability exist under this Act; and

(ii) a publicly accessible database of devices and the respective manufacturers of such devices about which the government has received formal notification of security support ceasing, as required under section 3(a)(1)(E)(iii).

(B) Updates.--The Director of the Office of Management and Budget shall update the databases established under subparagraph (A) not less frequently than once every 30 days.

SEC. 4. CONTRACTOR RESPONSIBILITIES WITH RESPECT TO IOMT DEVICE CYBERSECURITY.

(a) Clauses Required in IoMT Device Security.--

(1) In general.--IoMT device contractors and purchasing entities that purchase, own, and operate IoMT devices must manage IoMT devices in accordance with the internet-connected device security practices specified by SEC. 3 of this bill, as well as the following specifications:

(A) IoMT Device Firmware and Software Requirements.--

(i) Contractors of IoMT devices must have the ability to prove that the IoMT device marketed and sold by the contractor--

(I) sense the existence of other devices;

(II) change its working state depending on the priority of itself and others;

(III) will only change the MAC and upper layer of Device network stack upon communication conflict and without accessing or modifying the PHI;

(IV) include secure boot functionality;

(V) use industry recommended encryption during data transfer or migration in accordance with NIST Cryptographic standards and;

(VI) include two-factor, non-fixed or hard-coded credential-based authentication for use of device by authorized medical users only.

(B) Medical Organization Practices Required.--

(i) Each medical organization owning and operating IoMT devices must have the ability to prove that the medical organization--

(I) segments the medical organization's network as to keep separate the internal IoMT infrastructure and IoMT devices from BYOD devices on the network of the medical organization;

(II) performs internal or external risk assessment every three months of IoMT devices in use in accordance with the HITRUST CSF Assurance Program;

(ii) Any medical organization currently operating IoMT devices with known vulnerabilities from the sources specified in section 3(a)(1)(i)(I) must either--

(I) remove the IoMT device from use until a properly authenticated update that eliminates the vulnerability or vulnerabilities from the IoMT device is available and implemented on the IoMT device or;

(II) replace the IoMT device with a similar IoMT device that is not susceptible to any vulnerabilities known to the sources specified in section 3(a)(1)(i)(I).

SEC. 5. CONTRACTOR RESPONSIBILITIES WITH RESPECT TO IOFT DEVICE CYBERSECURITY.

(a) Clauses Required in IoFT Device Security.--

(1) In general.--IoFT device contractors and purchasing entities that purchase, own, and operate IoFT devices must manage IoFT devices in accordance with the internet-connected

device security practices specified by SEC. 3 of this bill, as well as the following specifications:

(A) IoFT Accessibility and Management Requirements.--

(i) Contractors of IoFT devices must have the ability to prove that the IoFT device adheres to the following requirements:

(I) IoFT devices used for any financial transaction must be secured with two-factor biometric authentication in order for users to access the device;

(II) IoFT devices with the capability to monitor user behavior and information should be secured with secure boot and encrypt user data in accordance with the Advanced Encryption Standard and;

(III) IoFT devices with the capability to track the location of its users must allow the IoFT device user to disable location tracking if they choose.

(B) Financial Organization Practices Required.--

(i) Financial organizations owning and operating IoFT devices must adhere to the following requirements:

(I) Financial organizations are responsible for any storage of collected IoFT data pertaining to the IoFT users and customers of the financial organization in a secure manner in accordance with the NIST Cybersecurity Framework.

(II) Any financial organization currently operating IoFT devices with known vulnerabilities from the sources specified in section 3(a)(1)(i)(I) must either--

(aa) remove the IoFT device from use until a properly authenticated update that eliminates the vulnerability or vulnerabilities from the IoFT device is available and implemented on the IoFT device or;

(bb) replace the IoFT device with a similar IoFT device that is not susceptible to any vulnerabilities known to the sources specified in section 3(a)(1)(i)(I).

SEC. 6. 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.