6/1/18 (redlines + bluelines)

S. 1691

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

IN THE SENATE OF THE UNITED STATES

AUGUST 1, 2017

Mr. WARNER (for himself, Mr. GARDNER, Mr. WYDEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

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) Cybersecurity Improvement Act of 2017".

SEC. 2. SENSE OF CONGRESS.

Whereas 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;

Whereas digital technology transformation portends tremendous opportunity for our nation to improve the daily lives of the American people and grow the economy;

Whereas 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;

Whereas intelligence and national security leaders, including the Director of the Defense Intelligence Agency, have described Internet of Things (IoT) devices as ~~"our weakest technology components" due to their insecurity, and described exploitation of IoT as~~ among the "most important emerging cyberthreats to our national security";

Whereas the federal government cannot achieve a high level of cybersecurity unless cybersecurity becomes the task of every person involved with federal networks and devices;

Whereas 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: Now, therefore, be it –

Resolved by the Senate (the House of Representatives concurring) That 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 federal Department or agency;

(2) This responsibility is to be carried out by working collaboratively within and among government 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. DEFINITIONS.

In this Act:

(1) DIRECTOR.—The term "Director" means the Director of the Office of Management and Budget (OMB).

(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~~COVERED DEVICE.—The term "~~Internet-connected~~covered device" ~~means a physical object that~~ —

(A) means a physical object that –

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

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

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

(C) OMB shall establish a process by which interested parties may petition for other devices not stated in Section 3(6)(B) to be included in the list of devices outside the scope of covered devices. OMB shall ensure that it acts on those petitions in an expedited manner.

(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.

Formatted: Indent: Left: 1.17"

Formatted: Indent: Left: 1", First line: 0.5"

Formatted: Indent: Left: 0.5", First line: 0.5"

Formatted: Indent: Left: 1", First line: 0"

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

SEC. ~~3~~4. CONTRACTOR RESPONSIBILITIES WITH RESPECT TO ~~INTERNET-CONNECTED~~COVERED DEVICE CYBERSECURITY.

(a) STANDARD SECURITY CLAUSE~~S~~ REQUIRED IN ~~INTERNET-CONNECTED~~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 to require ~~the following~~the inclusion of a standard security clause~~s~~ in any contract, except as provided in paragraph (2), for the acquisition of ~~Internet-connected~~covered devices:

(~~A~~2) ~~VERIFICATION REQUIRED~~CONTENT OF STANDARD SECURITY CLAUSE.— The standard security clause required under paragraph (1):

(A) shall establish baseline security requirements that address aspects of device security including:

~~(i) IN GENERAL.—A clause that requires the contractor providing the Internet-connected device to provide written certification that the device~~inclusion in any hardware, software, or firmware components of, and mitigation of, ~~—~~

~~(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;~~

(~~I~~ii) ~~relies on~~ability of software or firmware components ~~capable of~~to accept~~ing~~ properly authenticated and trusted updates from the vendor;

~~(II~~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~~

Formatted: Indent: Left: 0.17", First line: 0.5"

Formatted: Indent: Left: 0.67"

Formatted: Indent: First line: 0.5"

~~(cc) interconnection with other devices or peripherals; and~~

(~~I~~Viv) ~~does not include any~~identity and access management, including prohibiting the use of fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication.

(v) participation in a Coordinated Vulnerability Disclosure program in accordance with section 3(e) of this Act

(vi) such other aspects as the Director deems appropriate.

(vii) The Director shall ensure that, to the maximum extent practicable, such baseline security requirements reflect and align with existing voluntary consensus standards.

(B) shall require vendors to provide written attestation that the device meets such requirements as established under subsection (a).

(C) shall, 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 relevant stakeholders in industry and academia.

(iv) aligned with internationally recognized technical standards.

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

(D) may establish a process for a purchasing executive agency to waive the requirements under subsection (a) when a contractor

~~(ii) LIMITED EXCEPTION FOR DISCLOSED VULNERABILITIES.~~

~~(I) APPLICATION FOR WAIVER. At the time of submitting a proposal to an executive agency, a contractor may~~ submits a written application for a waiver ~~from the requirement under~~, provided that: ~~clause (i)(I) for the purpose of disclosing a known vulnerability to the executive agency.~~

Formatted: Indent: Left: 1", First line: 0"

Formatted: Indent: Left: 1", First line: 0"

Formatted: Indent: Left: 1.33", First line: 0"

~~(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 to exploit the vulnerability; and~~

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

(i) such a process provides for waivers to be granted only in limited circumstances, including when a vendor demonstrates that a device meets a desired level of security through means other than those required under subparagraph (A) or when the purchasing executive agency reasonably believes that procurement of a covered device with limited data processing and software functionality would be unfeasible or economically impractical.

(ii) such a process provides that,

~~(III) APPROVAL.—I~~ if the head of the purchasing executive agency approves ~~the~~ a waiver, the head of the purchasing executive agency shall provide the contractor a written statement that the executive agency 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 agency 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~~E) ~~UPDATES.—A clause that requires such Internet-connected~~shall identify responsibilities for ensuring that a covered device software or firmware component ~~to be~~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.

~~(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).~~

Formatted: Indent: Left: 1.33"

Formatted: Indent: Left: 1.67"

Formatted: Indent: Left: 1.33"

(~~E~~F) ~~CONTINUATION OF SERVICES.—A clause that~~shall require~~s~~ 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;

(ii) the anticipated timeline for ending security support associated with the ~~Internet-connected~~covered device;

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

(~~iv~~v) ~~any additional information recommended by the National Telecommunications and Information Administration~~other information as deemed necessary by the Director.

~~(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 executive agency may petition the Director for a waiver to the requirements contained in paragraph (1) in order to purchase a non-compliant Internet-connected device.~~

(3) 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 Federal Information Security Management Act of 2002, as amended (Chapter 35 of title 44, United States Code).

Formatted: Indent: Left: 0.69"

(~~ii~~b) ALTERNATE CONDITIONS TO MITIGATE CYBERSECURITY RISKS.—

(~~I~~1) 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~~A) ensure a~~n Internet-connected~~ covered device that does not comply with ~~paragraph (1)~~the standard security clause under subsection (a) can be used with a

level of security that is equivalent to the level of security described in ~~paragraph (1)(A)~~subsection (a)(2); and

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

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

(~~aa~~A) network segmentation or micro-segmentation;

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

(~~cc~~C) multi-factor authentication; and

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

(~~iii~~C) SPECIFICATION OF ADDITIONAL PRECAUTIONS.—To address the long-term risk of non-compliant ~~Internet-connected~~covered 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.

Formatted: Indent: Left: 0.13"

Formatted: Indent: Left: 1"

(B) EXISTING THIRD-PARTY SECURITY STANDARD.—

(i) IN GENERAL.—If an existing voluntary consensus standard~~third-party security standard~~ for ~~Internet-connected~~the security of covered devices provides an equivalent or greater level of security to that described in paragraph (a)(1)(A), ~~an executive agency may allow a contractor to demonstrate compliance with that standard in lieu of~~ the Director shall sunset the requirements under paragraph (a)(1) and modify security clauses to reflect conformity with that voluntary consensus standard.

(ii) WRITTEN CERTIFICATION.—A contractor providing the ~~Internet-connected~~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.

(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 employs a security evaluation process or criteria for ~~Internet-connected~~covered devices that the agency believes provides an equivalent or greater level of security to that described in paragraph (a)(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 (a)(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.

(c) 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.

(~~3~~d) 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~~ subsections (~~1~~a) and (c), which shall include any recommendations for

Formatted: No Spacing, Indent: Left: 0", First line: 0", Space Before: 0 pt, After: 0 pt, Pattern: Clear

Formatted: Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0", First line: 0.5"

Formatted: Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0", First line: 0"

~~legislative language needed to update the guideline requirements described in paragraph (1)~~legislation necessary to improve cybersecurity in federal government acquisition of internet-connected devices.

(~~4~~e) 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 ~~sub~~section, for an executive agency.

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

Formatted: Indent: First line: 0"

(1) IN GENERAL.—Not later than ~~60~~ 180 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~~covered device in use by the United States Government regarding cybersecurity coordinated disclosure requirements that shall be required of contractors providing such ~~software~~ covered devices to the United States Government.

(2) CONTENTS.—The guidelines required to be issued under paragraph (1) shall ~~—~~

Formatted: Indent: Left: 0.33"

~~(A)~~ include policies and procedures for ~~conducting research on the cybersecurity of an Internet-connected~~the processing and resolving of potential vulnerability information relating to a covered device, which shall be ~~based, in part, on,~~ to the maximum extent practicable, aligned with Standards 29147 and 30111 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~~A) procedures for a contractor providing a~~n Internet-connected~~ covered device to the United States Government on how to—

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

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

(~~ii~~B) 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 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.~~

~~(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)~~ SECTION 5. INVENTORY OF DEVICES.—

(~~1~~a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the head of each executive agency shall establish and maintain an inventory of ~~Internet-connected~~covered devices used by the agency procured under this Act.

(~~2~~b) 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 executive agencies 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~~c) DEVICE DATABASES.—

(~~A~~1) 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) a ~~publicly accessible~~ database of devices and the respective manufacturers of such devices for which limitations of liability exist under this Act; and

(~~ii~~B) 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~~2) UPDATES.—OMB shall update the databases established under subparagraph (A) not less frequently than once every 30 days.

SEC. ~~4~~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.

Formatted: Indent: First line: 0"

Formatted: Indent: First line: 0.33"

Formatted: Indent: Left: 0"