

115TH CONGRESS
1ST SESSION

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Internet of Things
5 (IoT) Cybersecurity Improvement Act of 2017”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) DIRECTOR.—The term “Director” means
2 the Director of the Office of Management and Budg-
3 et.

4 (2) EXECUTIVE AGENCY.—The term “executive
5 agency” has the meaning given the term in section
6 133 of title 41, United States Code.

7 (3) FIRMWARE.—The term “firmware” means a
8 computer program and the data stored in hardware,
9 typically in read-only memory (ROM) or program-
10 mable read-only memory (PROM), such that the
11 program and data cannot be dynamically written or
12 modified during execution of the program.

13 (4) FIXED OR HARD-CODED CREDENTIAL.—The
14 term “fixed or hard-coded credential” means a
15 value, such as a password, token, cryptographic key,
16 or other data element used as part of an authentica-
17 tion mechanism for granting remote access to an in-
18 formation system or its information, that is—

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

21 (B) incapable of being modified or revoked
22 by the user or manufacturer lawfully operating
23 the information system, except via a firmware
24 update.

1 (5) **HARDWARE.**—The term “hardware” means
2 the physical components of an information system.

3 (6) **INTERNET-CONNECTED DEVICE.**—The term
4 “Internet-connected device” means a physical object
5 that—

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

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

10 (7) **NIST.**—The term “NIST” means the Na-
11 tional Institute of Standards and Technology.

12 (8) **PROPERLY AUTHENTICATED UPDATE.**—The
13 term “properly authenticated update” means an up-
14 date, remediation, or technical fix to a hardware,
15 firmware, or software component issued by a prod-
16 uct vendor or service provider used to correct par-
17 ticular problems with the component, and that, in
18 the case of software or firmware, contains some
19 method of authenticity protection, such as a digital
20 signature, so that unauthorized updates can be auto-
21 matically detected and rejected.

22 (9) **SECURITY VULNERABILITY.**—The term “se-
23 curity vulnerability” means any attribute of hard-
24 ware, firmware, software, process, or procedure or
25 combination of 2 or more of these factors that could

1 enable or facilitate the defeat or compromise of the
2 confidentiality, integrity, or availability of an infor-
3 mation system or its information or physical devices
4 to which it is connected.

5 (10) SOFTWARE.—The term “software” means
6 a computer program and associated data that may
7 be dynamically written or modified.

8 **SEC. 3. CONTRACTOR RESPONSIBILITIES WITH RESPECT**
9 **TO INTERNET-CONNECTED DEVICE CYBERSE-**
10 **CURITY.**

11 (a) CLAUSES REQUIRED IN INTERNET-CONNECTED
12 DEVICES.—

13 (1) IN GENERAL.—Not later than 180 days
14 after the date of the enactment of this Act, the Di-
15 rector, in consultation with the Secretary of Defense,
16 the Administrator of General Services, the Secretary
17 of Commerce, the Secretary of Homeland Security,
18 and any other intelligence or national security agen-
19 cy that the Director determines to be necessary,
20 shall issue guidelines for each executive agency to re-
21 quire the following clauses in any contract, except as
22 provided in paragraph (2), for the acquisition of
23 Internet-connected devices:

24 (A) VERIFICATION REQUIRED.—

1 (i) IN GENERAL.—A clause that re-
2 quires the contractor providing the Inter-
3 net-connected device to provide written cer-
4 tification that the device—

5 (I) except as provided under
6 clause (ii), does not contain, at the
7 time of submitting the proposal, any
8 hardware, software, or firmware com-
9 ponent with any known security
10 vulnerabilities or defects listed in—

11 (aa) the National Vulner-
12 ability Database of NIST; and

13 (bb) any additional database
14 selected by the Director that
15 tracks security vulnerabilities and
16 defects, is credible, and is similar
17 to the National Vulnerability
18 Database;

19 (II) relies on software or
20 firmware components capable of ac-
21 cepting properly authenticated and
22 trusted updates from the vendor;

23 (III) uses only non-deprecated in-
24 dustry-standard protocols and tech-
25 nologies for functions such as—

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

4 (bb) encryption; and

5 (cc) interconnection with
6 other devices or peripherals; and
7 (IV) does not include any fixed
8 or hard-coded credentials used for re-
9 mote administration, the delivery of
10 updates, or communication.

11 (ii) LIMITED EXCEPTION FOR DIS-
12 CLOSED VULNERABILITIES.—

13 (I) APPLICATION FOR WAIVER.—

14 At the time of submitting a proposal
15 to an executive agency, a contractor
16 may submit a written application for
17 a waiver from the requirement under
18 clause (i)(I) for the purpose of dis-
19 closing a known vulnerability to the
20 executive agency.

21 (II) CONTENTS.—An application
22 submitted under subclause (I) shall—

23 (aa) identify the specific
24 known vulnerability;

1 (bb) include any mitigation
2 actions that may limit or elimi-
3 nate the ability for an adversary
4 to exploit the vulnerability; and

5 (cc) include a justification
6 for secure use of the device not-
7 withstanding the persisting vul-
8 nerability.

9 (III) APPROVAL.—If the head of
10 the purchasing executive agency ap-
11 proves the waiver, the head of the
12 purchasing executive agency shall pro-
13 vide the contractor a written state-
14 ment that the executive agency ac-
15 cepts such risks resulting from use of
16 the device with the known vulner-
17 ability as represented by the con-
18 tractor.

19 (B) NOTIFICATION REQUIRED.—A clause
20 that requires the contractor providing the Inter-
21 net-connected device software or firmware com-
22 ponent to notify the purchasing agency of any
23 known security vulnerabilities or defects subse-
24 quently disclosed to the vendor by a security re-

1 searcher or of which the vendor otherwise be-
2 comes aware for the duration of the contract.

3 (C) UPDATES.—A clause that requires
4 such Internet-connected device software or
5 firmware component to be updated or replaced,
6 consistent with other provisions in the contract
7 governing the term of support, in a manner
8 that allows for any future security vulnerability
9 or defect in any part of the software or
10 firmware to be patched in order to fix or re-
11 move a vulnerability or defect in the software or
12 firmware component in a properly authenticated
13 and secure manner.

14 (D) TIMELY REPAIR.—A clause that re-
15 quires the contractor to provide a repair or re-
16 placement in a timely manner in respect to any
17 new security vulnerability discovered through
18 any of the databases described in subparagraph
19 (A)(i)(I) or from the coordinated disclosure pro-
20 gram described in subsection (b) in the event
21 the vulnerability cannot be remediated through
22 an update described in subparagraph (C).

23 (E) CONTINUATION OF SERVICES.—A
24 clause that requires the contractor to provide
25 the purchasing agency with general information

1 on the ability of the device to be updated, such
2 as—

3 (i) the manner in which the device re-
4 ceives security updates;

5 (ii) the anticipated timeline for ending
6 security support associated with the Inter-
7 net-connected device;

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

10 (iv) any additional information rec-
11 ommended by the National Telecommuni-
12 cations and Information Administration.

13 (2) EXCEPTIONS.—

14 (A) DEVICES WITH SEVERELY LIMITED
15 FUNCTIONALITY.—

16 (i) IN GENERAL.—If an executive
17 agency reasonably believes that procure-
18 ment of an Internet-connected device with
19 limited data processing and software
20 functionality consistent with paragraph (1)
21 would be unfeasible or economically im-
22 practical, the executive agency may peti-
23 tion the Director for a waiver to the re-
24 quirements contained in paragraph (1) in

1 order to purchase a non-compliant Inter-
2 net-connected device.

3 (ii) ALTERNATE CONDITIONS TO MITI-
4 GATE CYBERSECURITY RISKS.—

5 (I) IN GENERAL.—Not later than
6 180 days after the date of the enact-
7 ment of this Act, the Director, in
8 close coordination with NIST, shall
9 define a set of conditions that—

10 (aa) ensure an Internet-con-
11 nected device that does not com-
12 ply with paragraph (1) can be
13 used with a level of security that
14 is equivalent to the level of secu-
15 rity described in paragraph
16 (1)(A); and

17 (bb) shall be met in order
18 for an executive agency to pur-
19 chase such a non-compliant de-
20 vice.

21 (II) REQUIREMENTS.—In defin-
22 ing a set of conditions that must be
23 met for non-compliant devices as re-
24 quired under subclause (I), the Direc-
25 tor, in close coordination with NIST

1 and relevant industry entities, may
2 consider the use of conditions includ-
3 ing—

4 (aa) network segmentation
5 or micro-segmentation;

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

10 (cc) multi-factor authentica-
11 tion; and

12 (dd) intelligent network so-
13 lutions and edge systems, such as
14 gateways, that can isolate, dis-
15 able, or remediate connected de-
16 vices.

17 (iii) SPECIFICATION OF ADDITIONAL
18 PRECAUTIONS.—To address the long-term
19 risk of non-compliant Internet-connected
20 devices acquired in accordance with an ex-
21 ception under this paragraph, the Director,
22 in coordination with NIST and private-sec-
23 tor industry experts, may stipulate addi-
24 tional requirements for management and
25 use of non-compliant devices, including

1 deadlines for the removal, replacement, or
2 disabling of non-compliant devices (or their
3 Internet-connectivity), as well as minimal
4 requirements for gateway products to en-
5 sure the integrity and security of the non-
6 compliant devices.

7 (B) EXISTING THIRD-PARTY SECURITY
8 STANDARD.—

9 (i) IN GENERAL.—If an existing third-
10 party security standard for Internet-con-
11 nected devices provides an equivalent or
12 greater level of security to that described
13 in paragraph (1)(A), an executive agency
14 may allow a contractor to demonstrate
15 compliance with that standard in lieu of
16 the requirements under paragraph (1).

17 (ii) WRITTEN CERTIFICATION.—A
18 contractor providing the Internet-connected
19 device shall provide third-party written cer-
20 tification that the device complies with the
21 security requirements of the industry cer-
22 tification method of the third party.

23 (iii) NIST.—NIST, in coordination
24 with the Director and other appropriate
25 executive agencies, shall determine—

1 (I) accreditation standards for
2 third-party certifiers; and

3 (II) whether the standards de-
4 scribed in subclause (I) provide appro-
5 priate security and is aligned with the
6 guidelines issued under this sub-
7 section.

8 (C) EXISTING AGENCY SECURITY EVALUA-
9 TION STANDARDS.—

10 (i) IN GENERAL.—If an executive
11 agency employs a security evaluation proc-
12 ess or criteria for Internet-connected de-
13 vices that the agency believes provides an
14 equivalent or greater level of security to
15 that described in paragraph (1)(A), an ex-
16 ecutive agency may, upon the approval of
17 the Director, continue to use that process
18 or standard in lieu of the requirements
19 under paragraph (1).

20 (ii) NIST.—NIST, in coordination
21 with the Director and other appropriate
22 executive agencies, shall determine whether
23 the process or criteria described in clause
24 (i) provides appropriate security and are

1 aligned with the guidelines issued under
2 this subsection.

3 (3) REPORT TO CONGRESS.—Not later than 5
4 years after the date of enactment of this Act, the
5 Director shall submit to Congress a report on the ef-
6 fectiveness of the guidelines required to be issued
7 under paragraph (1), which shall include rec-
8 ommendations for legislative language needed to up-
9 date the guideline requirements described in para-
10 graph (1).

11 (4) WAIVER AUTHORITY.—Beginning on the
12 date that is 5 years after the date of enactment of
13 this Act, the Director may waive, in whole or in
14 part, the requirements of the guidelines issued under
15 this subsection, for an executive agency.

16 (b) GUIDELINES REGARDING THE COORDINATED
17 DISCLOSURE OF SECURITY VULNERABILITIES AND DE-
18 FECTS.—

19 (1) IN GENERAL.—Not later than 60 days after
20 the date of the enactment of this Act, the National
21 Protection and Programs Directorate, in consulta-
22 tion with cybersecurity researchers and private-sec-
23 tor industry experts, shall issue guidelines for each
24 agency with respect to any Internet-connected device
25 in use by the United States Government regarding

1 cybersecurity coordinated disclosure requirements
2 that shall be required of contractors providing such
3 software devices to the United States Government.

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

6 (A) include policies and procedures for
7 conducting research on the cybersecurity of an
8 Internet-connected device, which shall be based,
9 in part, on Standard 29147 of the International
10 Standards Organization, or any successor
11 standard, relating to the processing and resolv-
12 ing of potential vulnerability information in a
13 product or online service, such as—

14 (i) procedures for a contractor pro-
15 viding an Internet-connected device to the
16 United States Government on how to—

17 (I) receive information about po-
18 tential vulnerabilities in the product
19 or online service of the contractor;
20 and

21 (II) disseminate resolution infor-
22 mation about vulnerabilities in the
23 product or online service of the con-
24 tractor; and

1 (ii) guidance, including example con-
2 tent, on the information items that should
3 be produced through the implementation of
4 the vulnerability disclosure process of the
5 contractor; and

6 (B) require that research on the cybersecu-
7 rity of an Internet-connected device provided by
8 a contractor to the United States Government
9 shall be conducted on the same class, model, or
10 type of the device provided to the United States
11 Government and not on the actual device pro-
12 vided to the United States Government.

13 (c) LIMITATION OF LIABILITY.—

14 (1) RULE OF CONSTRUCTION.—Nothing in this
15 subsection, or the amendments made by this sub-
16 section, shall be construed to establish additional ob-
17 ligations or criminal penalties for individuals en-
18 gaged in researching the cybersecurity of Internet-
19 connected devices.

20 (2) COMPUTER FRAUD AND ABUSE ACT.—Sec-
21 tion 1030 of title 18, United States Code, is amend-
22 ed—

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

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

3 “(k) This section shall not apply to a person who—

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

8 “(2) acted in compliance with the guidelines re-
9 quired to be issued by the National Protection and
10 Programs Directorate, and adopted by the con-
11 tractor described in paragraph (1), under section
12 3(b) of the Internet of Things (IoT) Cybersecurity
13 Improvement Act of 2017.”.

14 (3) DIGITAL MILLENNIUM COPYRIGHT ACT.—
15 Chapter 12 of title 17, United States Code, is
16 amended—

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

19 “(d) LIMITATION OF LIABILITY.—A person shall not
20 be held liable under this section if the individual—

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

1 “(2) acted in compliance with the guidelines re-
2 quired to be issued by the National Protection and
3 Programs Directorate, and adopted by the con-
4 tractor described in paragraph (1), under section
5 3(b) of the Internet of Things (IoT) Cybersecurity
6 Improvement Act of 2017.”; and

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

9 “(d) LIMITATION OF LIABILITY.—Subsection (a)
10 shall not apply to a person who—

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

15 “(2) acted in compliance with the guidelines re-
16 quired to be issued by the National Protection and
17 Programs Directorate, and adopted by the con-
18 tractor described in paragraph (1), under section
19 3(b) of the Internet of Things (IoT) Cybersecurity
20 Improvement Act of 2017.”.

21 (d) INVENTORY OF DEVICES.—

22 (1) IN GENERAL.—Not later than 180 days
23 after the date of the enactment of this Act, the head
24 of each executive agency shall establish and main-

1 tain an inventory of Internet-connected devices used
2 by the agency procured under this Act.

3 (2) GUIDELINES.—Not later than 30 days after
4 the date of the enactment of this Act, the Director
5 of the Office of Management and Budget, in con-
6 sultation with the Secretary of Homeland Security,
7 shall issue guidelines for executive agencies to de-
8 velop and manage the inventories required under
9 paragraph (1), based on the Continuous Diagnostics
10 and Mitigation (CDM) program used by the Depart-
11 ment of Homeland Security.

12 (3) DEVICE DATABASES.—

13 (A) IN GENERAL.—Not later than 180
14 days after the date of enactment of this Act,
15 the Director of the Office of Management and
16 Budget shall establish and maintain—

17 (i) a publicly accessible database of
18 devices and the respective manufacturers
19 of such devices for which limitations of li-
20 ability exist under this Act; and

21 (ii) a publicly accessible database of
22 devices and the respective manufacturers
23 of such devices about which the govern-
24 ment has received formal notification of se-

1 security support ceasing, as required under
2 section 3(a)(1)(E)(iii).

3 (B) UPDATES.—The Director of the Office
4 of Management and Budget shall update the
5 databases established under subparagraph (A)
6 not less frequently than once every 30 days.

7 **SEC. 4. USE OF BEST PRACTICES IN IDENTIFICATION AND**
8 **TRACKING OF VULNERABILITIES FOR PUR-**
9 **POSES OF THE NATIONAL VULNERABILITY**
10 **DATABASE.**

11 The Director of NIST shall ensure that NIST estab-
12 lishes, maintains, and uses best practices in the identifica-
13 tion and tracking of vulnerabilities for purposes of the Na-
14 tional Vulnerability Database of NIST.

○