

[DISCUSSION DRAFT]115TH CONGRESS
1ST 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.

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) BOARD.—The term “Board” means the
2 Emerging Technologies Advisory Board established
3 pursuant to section 3(a)(4)(A).

4 (2) COORDINATED VULNERABILITY DISCLO-
5 SURE.—The term “coordinated vulnerability disclo-
6 sure” means a reporting methodology under which a
7 third party—

8 (A) privately discloses information relating
9 to a newly discovered vulnerability directly to a
10 product vendor or service provider; and

11 (B) allows the affected party time to inves-
12 tigate the claim, and identify and test a remedy
13 or recourse, before coordinating the release of a
14 public disclosure of the vulnerability with the
15 third party.

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

19 (4) EXECUTIVE AGENCY.—The term “executive
20 agency” has the meaning given the term in section
21 133 of title 41, United States Code.

22 (5) FIRMWARE.—The term “firmware” means a
23 computer program and the data stored in hardware,
24 typically in read-only memory (ROM) or program-
25 mable read-only memory (PROM), such that the

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

3 (6) **FIXED OR HARD-CODED CREDENTIAL.**—The
4 term “fixed or hard-coded credential” means input,
5 such as a password, username, token, cryptographic
6 key, or other data element used as part of an au-
7 thentication mechanism for granting remote access
8 to an information system or its information, that
9 is—

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

12 (B) incapable of being modified or revoked
13 by the user or manufacturer lawfully operating
14 the information system.

15 (7) **HARDWARE.**—The term “hardware” means
16 the physical components of an information system.

17 (8) **INTERNET-CONNECTED DEVICE.**—The term
18 “Internet-connected device” means a physical object
19 that—

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

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

24 (9) **NIST.**—The term “NIST” means the Na-
25 tional Institute of Standards and Technology.

1 (10) PROPERLY AUTHENTICATED UPDATE.—

2 The term “properly authenticated update” means an
3 update, remediation, or technical fix to a hardware,
4 firmware, or software component issued by a prod-
5 uct vendor or service provider used to correct par-
6 ticular problems with the component, and that, in
7 the case of software or firmware, is authenticated
8 and features tamper-evident integrity protection, so
9 that unauthorized updates can be detected and re-
10 jected.

11 (11) SECURITY VULNERABILITY.—The term
12 “security vulnerability” means any attribute of hard-
13 ware, firmware, software, process, or procedure that
14 could enable or facilitate the defeat or compromise
15 of the integrity, confidentiality, or availability of an
16 information system or its information.

17 (12) SOFTWARE.—The term “software” means
18 a computer program and associated data that may
19 be dynamically written or modified during execution.

20 **SEC. 3. CONTRACTOR RESPONSIBILITIES WITH RESPECT**
21 **TO INTERNET-CONNECTED DEVICE CYBERSE-**
22 **CURITY.**

23 (a) CLAUSES REQUIRED IN INTERNET-CONNECTED
24 DEVICES.—

1 (1) IN GENERAL.—Not later than 180 days
2 after the date of the enactment of this Act, the Di-
3 rector, in consultation with the Secretary of Defense,
4 the Secretary of Commerce, the Secretary of Home-
5 land Security, and any other intelligence or national
6 security agency that the Director determines to be
7 necessary, shall issue guidelines for each executive
8 agency to, require the following clauses in any con-
9 tract, except as provided in paragraph (2), for the
10 acquisition of Internet-connected devices:

11 (A) VERIFICATION REQUIRED.—

12 (i) IN GENERAL.—A clause that re-
13 quires the contractor providing the Inter-
14 net-connected device to provide written cer-
15 tification that the device—

16 (I) except as provided under
17 clause (ii), does not contain, at the
18 initiation of the procurement process,
19 any hardware, software, or firmware
20 component with any known security
21 vulnerabilities or defects listed in—

22 (aa) the National Vulner-
23 ability Database of NIST; and

24 (bb) any additional database
25 selected by the Director that

1 tracks security vulnerabilities and
2 defects, is credible, and is similar
3 to the National Vulnerability
4 Database;

5 (II) relies on software or
6 firmware components capable of ac-
7 cepting properly authenticated and
8 trusted updates from the vendor;

9 (III) uses only non-deprecated in-
10 dustry-standard protocols and tech-
11 nologies for functions such as—

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

15 (bb) encryption; and

16 (cc) interconnection with
17 other devices or peripherals; and

18 (IV) does not include any fixed
19 or hard-coded credentials used for re-
20 mote administration, the delivery of
21 updates, or communication.

22 (ii) LIMITED EXCEPTION FOR DIS-
23 CLOSED VULNERABILITIES.—

24 (I) APPLICATION FOR WAIVER.—

25 At the time of submitting a proposal

1 to an executive agency, a contractor
2 may submit a written application for
3 a waiver from the requirement under
4 clause (i)(I) for the purpose of dis-
5 closing a known vulnerability.

6 (II) CONTENTS.—An application
7 submitted under subclause (I) shall—

8 (aa) identify the specific
9 known vulnerability;

10 (bb) any mitigation actions
11 that may limit or eliminate the
12 ability for an adversary to exploit
13 the vulnerability; and

14 (cc) include a justification
15 for secure use of the device not-
16 withstanding the persisting vul-
17 nerability.

18 (III) APPROVAL.—If the head of
19 the purchasing executive agency ap-
20 proves the waiver, the head of the
21 purchasing executive agency shall pro-
22 vide the contractor a written state-
23 ment that the executive agency ac-
24 cepts such risks resulting from use of
25 the device with the known vulner-

1 ability as represented by the con-
2 tractor.

3 (B) NOTIFICATION REQUIRED.—A clause
4 that requires the contractor providing the Inter-
5 net-connected device software or firmware com-
6 ponent to notify the purchasing agency of any
7 known security vulnerabilities or defects discov-
8 ered through the verification required under
9 subparagraph (A)(i)(I) or subsequently dis-
10 closed to the vendor by a security researcher or
11 of which the vendor otherwise becomes aware
12 for the duration of the contract.

13 (C) UPDATES.—A clause that requires
14 such Internet-connected device software or
15 firmware component to be updated or replaced
16 in a manner that allows for any future security
17 vulnerability or defect in any part of the soft-
18 ware or firmware to be easily patched in order
19 to remove or fix a vulnerability or defect in the
20 software or firmware component in a properly
21 authenticated and secure manner.

22 (D) TIMELY REPAIR.—A clause that re-
23 quires the contractor to provide a repair or re-
24 placement in a timely manner in respect to any
25 new security vulnerability discovered through

1 any of the databases described in subparagraph
2 (A)(i)(I) or from the coordinated disclosure pro-
3 gram described in subsection (b).

4 (E) CONTINUATION OF SERVICES.—A
5 clause that requires the contractor to provide
6 the purchasing agency with general information
7 on the ability of the device to be updated, such
8 as—

9 (i) the manner in which the device re-
10 ceives security updates;

11 (ii) the anticipated timeline for ending
12 security support associated with the Inter-
13 net-connected device;

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

16 (iv) any additional information rec-
17 ommended by the National Telecommuni-
18 cations and Information Administration.

19 (2) EXCEPTION FOR DEVICES WITH SEVERELY
20 LIMITED FUNCTIONALITY.—

21 (A) IN GENERAL.—If an executive agency
22 reasonably believes that procurement of an
23 Internet-connected device with limited data
24 processing and software functionality consistent
25 with paragraph (1) would be infeasible or eco-

1 nominally impractical, the executive agency may
2 petition the Director for a waiver to the re-
3 quirements contained in paragraph (1) in order
4 to purchase a non-compliant Internet-connected
5 device.

6 (B) ALTERNATE CONDITIONS TO MITIGATE
7 CYBERSECURITY RISKS.—

8 (i) IN GENERAL.—Not later than 180
9 days after the date of the enactment of
10 this Act, the Director, in close coordination
11 with NIST, shall define a set of conditions
12 that must be met for non-compliant devices
13 to be adopted in the event an executive
14 agency wishes to purchase an Internet-con-
15 nected device that does not comply with
16 paragraph (1).

17 (ii) REQUIREMENTS.—In defining a
18 set of conditions that must be met for non-
19 compliant devices as required under clause
20 (i), the Director, in close coordination with
21 relevant industry entities and NIST, shall
22 consider the use of conditions including—

23 (I) network segmentation or
24 micro-segmentation;

1 (II) the adoption of system level
2 security controls, including operating
3 system containers and microservices;

4 (III) multi-factor authentication;
5 and

6 (IV) intelligent network solutions,
7 such as gateways, that can isolate,
8 disable, or remediate connected de-
9 vices.

10 (C) SPECIFICATION OF ADDITIONAL PRE-
11 CAUTIONS.—To address the long-term risk of
12 non-compliant Internet-connected devices ac-
13 quired in accordance with a waiver under this
14 paragraph, the Director, in coordination with
15 NIST, may stipulate additional requirements
16 for management and use of non-compliant de-
17 vices, including deadlines for the removal, re-
18 placement, or disabling of non-compliant devices
19 (or their Internet-connectivity), as well as mini-
20 mal requirements for gateway products to en-
21 sure the integrity and security of the non-com-
22 pliant devices.

23 (3) REPORT TO CONGRESS.—Not later than 5
24 years after the date of enactment of this Act, the
25 Director shall submit to Congress a report on the ef-

1 fectiveness of the guidelines required to be issued
2 under paragraph (1), which shall include rec-
3 ommendations for legislative language needed to up-
4 date the guideline requirements described in sub-
5 paragraphs (A) through (D) of paragraph (1).

6 (4) WAIVER AUTHORITY.—

7 (A) ESTABLISHMENT.—Not later than 5
8 years after the date of the enactment of this
9 Act, the Director shall establish an advisory
10 board to be known as the “Emerging Tech-
11 nologies Advisory Board”.

12 (B) DUTIES.—The Board shall evaluate
13 the guidelines issued pursuant to paragraph (1)
14 and conditions defined pursuant to paragraph
15 (2) and when necessary provide recommenda-
16 tions to the Director for updates to the guide-
17 lines and conditions. The Board may waive, in
18 whole or in part, the requirements of the guide-
19 lines under paragraph (1) and the conditions
20 under paragraph (2), for an executive agency.

21 (C) MEMBERSHIP.—The Advisory board
22 shall be composed of 14 members as follows:

23 (i) The Director of the National Insti-
24 tute of Standards and Technology, or the
25 designee of the Director.

1 (ii) The Secretary of Homeland Secu-
2 rity, or the designee of the Secretary.

3 (iii) The Administrator of the General
4 Services Administration, or the designee of
5 the Administrator.

6 (iv) The Secretary of the National
7 Telecommunications and Information Ad-
8 ministration, or the designee of the Sec-
9 retary.

10 (v) The Chairman of the Federal
11 Communication Commission, or the des-
12 ignee of the Chairman.

13 (vi) The Chairman of the Federal
14 Trade Commission, or the designee of the
15 Chairman.

16 (vii) The Attorney General, or the
17 designee of the Attorney General.

18 (viii) The following individuals who
19 shall be appointed by the Director:

20 (I) Three members who represent
21 private industry.

22 (II) Three members who rep-
23 resent non-profit entities or workforce
24 associations.

1 (III) One member from an insti-
2 tution of higher education who is a
3 scholar in the field of emerging tech-
4 nologies.

5 (D) REPORTS.—The Board shall submit to
6 the Director and to Congress annual reports
7 clarifying the progress of the Board in carrying
8 out its duties under this paragraph.

9 (b) GUIDELINES REGARDING THE COORDINATED
10 DISCLOSURE OF SECURITY VULNERABILITIES AND DE-
11 FECTS.—

12 (1) IN GENERAL.—Not later than 60 days after
13 the date of the enactment of this Act, the National
14 Protection and Programs Directorate, in consulta-
15 tion with private-sector industry experts, shall issue
16 guidelines for each agency with respect to any Inter-
17 net-connected device in use by the United States
18 Government regarding cybersecurity coordinated dis-
19 closure requirements that shall be required of con-
20 tractors providing such software devices to the
21 United States Government.

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

24 (A) include policies and procedures for
25 conducting research on the cybersecurity of an

1 Internet-connected device, which shall be based,
2 in part, on Standard 29147 of the International
3 Standards Organization, or any successor
4 standard, relating to the processing and resolv-
5 ing of potential vulnerability information in a
6 product or online service, such as—

7 (i) procedures for a contractor pro-
8 viding an Internet-connected device to the
9 United States Government on how to—

10 (I) receive information about po-
11 tential vulnerabilities in the product
12 or online service of the contractor;
13 and

14 (II) disseminate resolution infor-
15 mation about vulnerabilities in the
16 product or online service of the con-
17 tractor; and

18 (ii) guidance, including example con-
19 tent, on the information items that should
20 be produced through the implementation of
21 the vulnerability disclosure process of the
22 contractor; and

23 (B) require that research on the cybersecu-
24 rity of an Internet-connected device provided by
25 a contractor to the United States Government

1 shall be conducted on the same model, class, or
2 type of the device provided to the United States
3 Government and not on the actual device pro-
4 vided to the United States Government.

5 (c) LIMITATION OF LIABILITY.—

6 (1) COMPUTER FRAUD AND ABUSE ACT.—Sec-
7 tion 1030 of title 18, United States Code, is amend-
8 ed—

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

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

13 “(k) This section shall not apply to an individual who
14 is—

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

19 “(2) acting in compliance with the guidelines
20 required to be issued by the National Protection and
21 Programs Directorate, and adopted by the con-
22 tractor described in paragraph (1), under section
23 3(b) of the Internet of Things (IoT) Cybersecurity
24 Improvement Act of 2017.”.

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

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

6 “(d) LIMITATION OF LIABILITY.—An individual shall
7 not be held liable under this section if the individual is—
8 “(1) in good faith engaged in researching the
9 cybersecurity of an Internet-connected device of the
10 model, class, or type provided by a contractor to a
11 department or agency of the United States; and

12 “(2) acting in compliance with the guidelines
13 required to be issued by the National Protection and
14 Programs Directorate, and adopted by the con-
15 tractor described in paragraph (1), under section
16 3(b) of the Internet of Things (IoT) Cybersecurity
17 Improvement Act of 2017.”; and

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

20 “(d) LIMITATION OF LIABILITY.—Subsection (a)
21 shall not apply to an individual who is—

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

1 “(2) acting in compliance with the guidelines
2 required 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.”.

7 (d) INVENTORY OF DEVICES.—

8 (1) IN GENERAL.—Not later than 180 days
9 after the date of the enactment of this Act, the head
10 of each executive agency shall establish and main-
11 tain an inventory of Internet-connected devices used
12 by the agency.

13 (2) GUIDELINES.—Not later than 30 days after
14 the date of the enactment of this Act, the Director
15 of the Office of Management and Budget, in con-
16 sultation with the Secretary of Homeland Security,
17 shall issue guidelines for executive agencies to de-
18 velop and manage the inventories required under
19 paragraph (1), based on the Continuous Diagnostics
20 and Mitigation (CDM) program used by the Depart-
21 ment of Homeland Security.

1 **SEC. 4. USE OF BEST PRACTICES IN IDENTIFICATION AND**
2 **TRACKING OF VULNERABILITIES FOR PUR-**
3 **POSES OF THE NATIONAL VULNERABILITY**
4 **DATABASE.**

5 The Director of NIST shall ensure that NIST estab-
6 lishes, maintains, and uses best practices in the identifica-
7 tion and tracking of vulnerabilities for purposes of the Na-
8 tional Vulnerability Database of NIST.