

.....
(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.

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) Federal Cybersecurity Improvement Act of 2018”.

6 **SEC. 2. FINDINGS; SENSE OF CONGRESS.**

7 (a) FINDINGS.—Congress finds the following:

1 (1) The trust of the American people in the
2 safety and security of their Government’s digital
3 technologies, including the Internet of Things, is
4 vital for advancing digital technology trans-
5 formation.

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

10 (3) The risk of exposure of Government, busi-
11 nesses, and individual citizens to malicious cyber-at-
12 tacks grows dramatically if digital transformation is
13 not managed with vigorous attention to cybersecu-
14 rity concerns, and failure to protect the Government
15 systems that control our critical infrastructure and
16 essential Government networks could have dev-
17 astating consequences.

18 (4) Intelligence and national security leaders,
19 including the Director of the Defense Intelligence
20 Agency, have described Internet of Things (IoT) de-
21 vices as among the “most important emerging
22 cyberthreats to our national security”.

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

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

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

9 (b) SENSE OF CONGRESS.—It is the sense of Con-
10 gress that—

11 (1) ensuring the highest level of cybersecurity
12 at Government agencies is the responsibility of the
13 President, followed by the Director of the Office of
14 Management and Budget, and the head of each ex-
15 ecutive agency;

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

19 (3) the strength of the Government's cybersecu-
20 rity and the positive benefits of digital technology
21 transformation depend on proactively addressing cy-
22 bersecurity throughout the Government's acquisition
23 and operation of IoT devices.

1 **SEC. 3. CONTRACTOR MINIMUM SECURITY REQUIREMENTS**
2 **FOR COVERED DEVICES.**

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

5 (1) IN GENERAL.—Not later than 180 days
6 after the date of the enactment of this Act, the Di-
7 rector in consultation with the Secretary of Defense,
8 the Administrator of General Services, the Secretary
9 of Commerce, the Secretary of Homeland Security,
10 and any other intelligence or national security agen-
11 cy that the Director determines to be necessary shall
12 issue guidelines for each executive agency that re-
13 quire the inclusion of a standard security clause in
14 any contract (except as provided in paragraph (4))
15 for the acquisition of covered devices.

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

19 (A) establish baseline security require-
20 ments that address aspects of device security
21 relating to covered devices, including—

22 (i) a requirement that software or
23 firmware components accept properly au-
24 thenticated and trusted updates from the
25 vendor;

1 (ii) requirements relating to identity
2 and access management, including a prohi-
3 bition of the use of fixed or hard-coded
4 credentials used for remote administration,
5 the delivery of updates, or communication;

6 (iii) a requirement that the contractor
7 participate in a coordinated vulnerability
8 disclosure program training on the guide-
9 lines issued pursuant to subsection (f); and

10 (iv) any other requirement the Direc-
11 tor determines to be appropriate;

12 (B) require contractors to provide written
13 attestation that the device meets such require-
14 ments as established under subparagraph (A);

15 (C) to the maximum extent practicable, en-
16 sure that the requirements established under
17 subparagraph (A) are—

18 (i) tailored to address the characteris-
19 ties of different types of devices, including
20 risk and intended function;

21 (ii) based on technology-neutral, out-
22 come-based security principles;

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

1 evant stakeholders in industry and aca-
2 demia;

3 (iv) aligned with internationally recog-
4 nized technical standards; and

5 (v) updated regularly based on devel-
6 opments in technology and security meth-
7 odologies;

8 (D) an identification of contractor respon-
9 sibilities to ensure that a covered device soft-
10 ware or firmware component is updated or re-
11 placed, consistent with other provisions in the
12 contract governing the term of support, in a
13 manner that allows for any future security vul-
14 nerability or defect in any part of the software
15 or firmware to be patched, based on risk, in
16 order to fix or remove a vulnerability or defect
17 in the software or firmware component in a
18 properly authenticated and secure manner; and

19 (E) a requirement for the contractor to
20 provide the purchasing agency with general in-
21 formation on the ability of the device to be up-
22 dated, such as—

23 (i) the manner in which the device re-
24 ceives security updates;

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

5 (iii) the anticipated timeline for end-
6 ing security support associated with the
7 covered device;

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

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

12 (3) VOLUNTARY CONSENSUS STANDARDS.—The
13 Director shall ensure that, to the maximum extent
14 practicable, the baseline security described in para-
15 graph (2)(A) reflects and aligns with existing vol-
16 untary consensus standards.

17 (4) WAIVER OF REQUIREMENT BY AGENCIES.—

18 The Director may establish a process for the Chief
19 Information Officer of an executive agency to waive
20 the requirements under this subsection for a case in
21 which a petition is submitted by an entity seeking to
22 enter into a contract with the executive agency and
23 the following requirements are met:

24 (A) A waiver is granted only in limited cir-
25 cumstances, including when an entity dem-

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

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

13 (5) ALIGNMENT WITH FISMA.—In issuing the
14 guidelines required under paragraph (1), the Direc-
15 tor, in consultation with the Administrator of Gen-
16 eral Services, shall ensure that such guidelines are,
17 to the greatest extent practicable, consistent with,
18 non-duplicative of, and in compliance with any appli-
19 cable established information security policies, proce-
20 dures, standards, and compliance requirements
21 under the subchapter II of chapter 35 of title 44,
22 United States Code.

23 (b) ALTERNATE CONDITIONS TO MITIGATE CYBER-
24 SECURITY RISKS.—

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

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

9 (B) shall be met in order for an executive
10 agency to purchase such a non-compliant de-
11 vice.

12 (2) REQUIREMENTS.—In defining the set of
13 conditions that must be met for non-compliant de-
14 vices required under paragraph (1), the Director, in
15 consultation with NIST and relevant industry enti-
16 ties, may consider the use of conditions, including—

17 (A) network segmentation or micro-seg-
18 mentation;

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

22 (C) multi-factor authentication; and

23 (D) intelligent network solutions and edge
24 systems, such as gateways, that can isolate, dis-
25 able, or remediate connected devices.

1 (3) SPECIFICATION OF ADDITIONAL PRE-
2 CAUTIONS.—To address the long-term risk of non-
3 compliant devices acquired in accordance with an ex-
4 ception under this subsection, the Director, in con-
5 sultation with NIST and private-sector industry ex-
6 perts and, with respect to medical devices regulated
7 under the Federal Food, Drug, and Cosmetics Act,
8 in consultation with the Commissioner of Food and
9 Drugs, may stipulate additional requirements for
10 management and use of non-compliant devices, in-
11 cluding deadlines for the removal, replacement, or
12 disabling of non-compliant devices (or their Internet-
13 connectivity), as well as minimal requirements for
14 gateway products to ensure the integrity and secu-
15 rity of the non-compliant devices.

16 (4) EXISTING THIRD-PARTY SECURITY STAND-
17 ARD.—

18 (A) IN GENERAL.—If a voluntary con-
19 sensus standard for the security of covered de-
20 vices provides an equivalent or greater level of
21 security to that described in subsection (a)(2),
22 the Director shall modify the requirements
23 under subsection (a)(1) and the security clause
24 under subsection (a)(2) to reflect conformity
25 with that voluntary consensus standard .

1 (B) WRITTEN CERTIFICATION.—A con-
2 tractor providing a covered device shall provide
3 third-party written certification that the device
4 complies with the security requirements of the
5 industry certification method of the third party.

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

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

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

15 (5) EXISTING AGENCY SECURITY EVALUATION
16 STANDARDS.—

17 (A) IN GENERAL.—If an executive agency
18 employs a security evaluation process or criteria
19 for covered devices that the agency believes pro-
20 vides an equivalent or greater level of security
21 to the baseline security requirements described
22 in subsection (a)(2), an executive agency may,
23 upon the approval of the Director, continue to
24 use that process or criteria in lieu of the re-
25 quirements under subsection (a)(2).

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

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

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

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

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

4 (f) GUIDELINES REGARDING THE COORDINATED
5 DISCLOSURE OF SECURITY VULNERABILITIES AND DE-
6 FECTS.—

7 (1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this Act, the Di-
9 rector, in consultation with the Department of
10 Homeland Security and the Department of Justice,
11 and cybersecurity researchers and private-sector in-
12 dustry experts, shall issue guidelines for each execu-
13 tive agency with respect to any covered device in use
14 by the United States Government regarding cyberse-
15 curity coordinated disclosure requirements that shall
16 be required of contractors providing such covered de-
17 vices to those executive agencies.

18 (2) CONTENTS.—The guidelines required under
19 paragraph (1) shall include policies and procedures
20 for the processing and resolving of potential vulner-
21 ability information relating to a covered device,
22 which shall be, to the maximum extent practicable,
23 aligned with Standards 29147 and 30111 of the
24 International Standards Organization, or any suc-
25 cessor standard, such as—

1 (A) procedures for the provision of a cov-
2 ered device to executive agencies by a con-
3 tractor on how to—

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

7 (ii) disseminate resolution information
8 about vulnerabilities in the product or on-
9 line service of the contractor; and

10 (B) guidance, including example content,
11 on the information items that should be pro-
12 duced through the implementation of the vul-
13 nerability disclosure process of the contractor.

14 (g) REVISION OF FAR.—The Federal Acquisition
15 Regulations System shall be revised to require the inclu-
16 sion of a standard security clause consistent with the re-
17 quirements of this section.

18 **SEC. 4. INVENTORY OF DEVICES.**

19 (a) IN GENERAL.—Not later than one year after the
20 date of the enactment of this Act, the head of each execu-
21 tive agency shall establish and maintain an inventory of
22 covered devices used by the agency procured under the re-
23 quirements of this Act.

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

1 sultation with the Secretary of Homeland Security, shall
2 issue guidelines for executive agencies to develop and man-
3 age the inventories required under subsection (a), based
4 on the Continuous Diagnostics and Mitigation program
5 used by the Department of Homeland Security.

6 (c) DEVICE DATABASES.—

7 (1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this Act, the Sec-
9 retary of Homeland Security, in consultation with
10 the Director shall establish and maintain—

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

13 (B) a database of covered devices and the
14 manufacturers of such devices about which the
15 Government has received formal notification of
16 security support ceasing, as required under sec-
17 tion 3(a)(2)(E)(iv).

18 (2) UPDATES.—The Secretary of Homeland Se-
19 curity shall update the databases established under
20 paragraph (1) not less frequently than every 30
21 days.

1 **SEC. 5. 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.

9 **SEC. 6. DEFINITIONS.**

10 In this Act:

11 (1) COVERED DEVICE.—

12 (A) IN GENERAL.—The term “covered de-
13 vice”—

14 (i) means a physical object that—

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

18 (II) has computer processing ca-
19 pabilities that can collect, send, or re-
20 ceive data; and

21 (ii) does not include advanced or gen-
22 eral-purpose computing devices, including
23 personal computing systems, smart mobile
24 communications devices, programmable
25 logic controls, and mainframe computing
26 systems.

1 (B) OMB EXEMPTION.—The Director may
2 exempt additional devices under subparagraph
3 (A)(ii) through a process in which interested
4 parties may submit a petition for the exemp-
5 tion. The Director shall act in an expedited
6 manner on any such petition submitted.

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

10 (3) EXECUTIVE AGENCY.—The term “executive
11 agency” has the meaning given the term in section
12 133 of title 41, United States Code.

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

19 (5) FIXED OR HARD-CODED CREDENTIAL.—The
20 term “fixed or hard-coded credential” means a
21 value, such as a password, token, cryptographic key,
22 or other data element used as part of an authentica-
23 tion mechanism for granting remote access to an in-
24 formation system or the information of the system,
25 that is—

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

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

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

10 (7) HARDWARE.—The term “hardware” means
11 the physical components of an information system.

12 (8) NIST.—The term “NIST” means the Na-
13 tional Institute of Standards and Technology.

14 (9) NON-COMPLIANT DEVICE.—The term “non-
15 compliant device” means a covered device that does
16 not meet the baseline security requirements estab-
17 lished in section 3(a)(2)(A).

18 (10) PROPERLY AUTHENTICATED UPDATE.—
19 The term “properly authenticated update” means an
20 update, remediation, or technical fix to a hardware,
21 firmware, or software component issued by a prod-
22 uct vendor or service provider used to correct par-
23 ticular problems with the component, and that, in
24 the case of software or firmware, contains some
25 method of authenticity protection, such as a digital

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

4 (11) SECURITY VULNERABILITY.—The term
5 “security vulnerability” means any attribute of hard-
6 ware, firmware, software, process, or procedure or a
7 combination of 2 or more of these attributes that
8 could enable or facilitate the defeat or compromise
9 of the confidentiality, integrity, or availability of an
10 information system or the information or physical
11 devices of an information system to which an infor-
12 mation system is connected.

13 (12) SOFTWARE.—The term “software” means
14 a computer program and associated data that may
15 be dynamically written or modified.

16 (13) VENDOR.—The term “vendor”, with re-
17 spect to a technology, product, system, service, or
18 application, means—

19 (A) in the case of a purchase by the Gov-
20 ernment, the entity that developed the tech-
21 nology, product, system, service, or application;
22 or

23 (B) in the case of a purchase by a con-
24 tractor, the entity that is responsible for main-

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

3 **SEC. 7. APPLICABILITY.**

4 This Act shall apply with respect to any contract en-
5 tered into on and after the date on which the guidelines
6 are issued pursuant to section 3(a).