

116TH CONGRESS
1ST SESSION

H. R. 1668

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 11, 2019

Ms. KELLY of Illinois (for herself, Mr. HURD of Texas, Mr. KHANNA, Mr. BUDD, Mr. RUPPERSBERGER, Mr. MARSHALL, Mr. TED LIEU of California, Mr. RATCLIFFE, Mr. MEADOWS, Mr. SOTO, Mr. WALKER, Mr. CONNOLLY, Mr. FOSTER, and Mr. BAIRD) introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, 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 Cy-
5 bersecurity Improvement Act of 2019” or the “IoT Cyber-
6 security Improvement Act of 2019”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) AGENCY.—The term “agency” has the
4 meaning given such term in section 3502 of title 44,
5 United States Code.

6 (2) COVERED DEVICE.—

7 (A) IN GENERAL.—The term “covered de-
8 vice” means a physical object that—

9 (i) is capable of connecting to and is
10 in regular connection with the internet;

11 (ii) has computer processing capabili-
12 ties that can collect, send, or receive data;
13 and

14 (iii) is not a general-purpose com-
15 puting device, including personal com-
16 puting systems, smart mobile communica-
17 tions devices, programmable logic controls,
18 and mainframe computing systems.

19 (B) MODIFICATION OF DEFINITION.—The
20 Director of the Office of Management and
21 Budget shall establish a process by which—

22 (i) interested parties may petition for
23 a device that is not described in subpara-
24 graph (A) to be considered a device that is
25 not a covered device; and

1 (ii) the Director acts upon any peti-
 2 tion submitted under clause (i) in a timely
 3 manner.

4 (3) SECURITY VULNERABILITY.—The term “se-
 5 curity vulnerability” means any attribute of hard-
 6 ware, firmware, software, or combination of 2 or
 7 more of these factors that could enable the com-
 8 promise of the confidentiality, integrity, or avail-
 9 ability of an information system or its information
 10 or physical devices to which it is connected.

11 **SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
 12 **NOLOGY CONSIDERATIONS AND RECOMMEN-**
 13 **DATIONS REGARDING MANAGING INTERNET**
 14 **OF THINGS CYBERSECURITY RISKS.**

15 (a) COMPLETION OF ONGOING EFFORTS RELATING
 16 TO CONSIDERATIONS FOR MANAGING INTERNET OF
 17 THINGS CYBERSECURITY RISKS.—

18 (1) IN GENERAL.—The Director of the National
 19 Institute of Standards and Technology shall ensure
 20 that the efforts of the Institute in effect on the date
 21 of the enactment of this Act regarding consider-
 22 ations for managing Internet of Things cybersecurity
 23 risks, especially regarding examples of possible cy-
 24 bersecurity capabilities of Internet of Things devices,
 25 are completed no later than September 30, 2019.

1 (2) MATTERS ADDRESSED.—In ensuring efforts
2 are completed under paragraph (1), the Director
3 shall also ensure that such efforts address, at a min-
4 imum, the following considerations for covered de-
5 vices:

6 (A) Secure Development.

7 (B) Identity management.

8 (C) Patching.

9 (D) Configuration management.

10 (b) DEVELOPMENT OF RECOMMENDED STANDARDS
11 FOR USE OF INTERNET OF THINGS DEVICES BY FED-
12 ERAL GOVERNMENT.—

13 (1) IN GENERAL.—Not later than March 31,
14 2020, the Director of the Institute shall develop rec-
15 ommendations for the Federal Government on the
16 appropriate use and management by the Federal
17 Government of Internet of Things devices owned or
18 controlled by the Federal Government, including
19 minimum information security requirements for
20 managing cybersecurity risks associated with such
21 devices.

22 (2) CONSISTENCY WITH ONGOING EFFORTS.—
23 The Director of the Institute shall ensure that the
24 recommendations and standards developed under
25 paragraph (1) are consistent with the efforts re-

1 ferred to in subsection (a), especially with respect to
2 the examples of possible cybersecurity capabilities re-
3 ferred to in such subsection.

4 (c) INSTITUTE REPORT ON CYBERSECURITY CONSID-
5 ERATIONS STEMMING FROM THE CONVERGENCE OF IN-
6 FORMATION TECHNOLOGY, INTERNET OF THINGS, AND
7 OPERATIONAL TECHNOLOGY DEVICES, NETWORKS AND
8 SYSTEMS.—Not later than 180 days following the enact-
9 ment of this Act, the Director of the Institute shall publish
10 a draft report related to the increasing convergence of tra-
11 ditional Information Technology devices, networks, and
12 systems with Internet of Things devices, networks and sys-
13 tems and Operational Technology devices, networks and
14 systems, including considerations for managing cybersecu-
15 rity risks associated with such trends.

16 **SEC. 4. POLICIES FOR FEDERAL AGENCIES ON USE AND**
17 **MANAGEMENT OF INTERNET OF THINGS DE-**
18 **VICES.**

19 (a) REVISIONS TO THE FEDERAL ACQUISITION REG-
20 ULATION.—Not later than 180 days after the date on
21 which the Director of the National Institute of Standards
22 and Technology completes the development of the rec-
23 ommendations required under section 3(b), the Director
24 of the Office of Management and Budget shall issue guide-

1 lines for each agency that are consistent with such rec-
2 ommendations.

3 (b) REQUIREMENT.—In issuing the guidelines re-
4 quired under subsection (a), the Director of the Office of
5 Management and Budget shall ensure that the guidelines
6 are consistent with the information security requirements
7 in subchapter II of chapter 35 of title 44, United States
8 Code.

9 (c) QUINQUENNIAL REVIEWS AND REVISIONS.—Not
10 less frequently than once every 5 years—

11 (1) the Director of the Office of Management
12 and Budget and the Director of the National Insti-
13 tute of Standards and Technology shall review the
14 policies issued under subsection (a); and

15 (2) the Director of the Office of Management
16 and Budget shall, in consultation with the Director
17 of the National Institute of Standards and Tech-
18 nology, revise such policies.

19 **SEC. 5. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
20 **NOLOGY GUIDANCE ON COORDINATED DIS-**
21 **CLOSURE OF SECURITY VULNERABILITIES**
22 **RELATING TO INTERNET OF THINGS DE-**
23 **VICES.**

24 (a) IN GENERAL.—Not later than 180 days after the
25 date of the enactment of this Act, the Director of the Na-

1 tional Institute of Standards and Technology shall, in con-
2 sultation with such cybersecurity researchers and private-
3 sector industry experts as the Director considers appro-
4 priate, publish guidance on policies and procedures for the
5 reporting, coordinating, publishing, and receiving of infor-
6 mation about—

7 (1) a security vulnerability relating to a covered
8 device used by the Federal Government; and

9 (2) the resolution of such security vulnerability.

10 (b) ELEMENTS.—The guidance published under sub-
11 section (a) shall include the following:

12 (1) Policies and procedures described in sub-
13 section (a) that, to the maximum extent practicable,
14 are aligned with Standards 29147 and 30111 of the
15 International Standards Organization, or any suc-
16 cessor standards. Such policies and procedures shall
17 include policies and procedures for a contractor or
18 vendor providing a covered device to the Federal
19 Government on—

20 (A) receiving information about a potential
21 security vulnerability relating to the covered de-
22 vice; and

23 (B) disseminating information about the
24 resolution of a security vulnerability relating to
25 the covered device.

1 (2) Guidance, including example content, on the
2 information items that should be produced through
3 the implementation of the security vulnerability dis-
4 closure process of the contractor.

5 **SEC. 6. GUIDELINES FOR FEDERAL AGENCIES ON COORDI-**
6 **NATED DISCLOSURE OF SECURITY VULNERA-**
7 **BILITIES RELATING TO INTERNET OF THINGS**
8 **DEVICES.**

9 (a) AGENCY GUIDELINES REQUIRED.—Not later
10 than 180 days after the date on which the guidance re-
11 quired under section 4 is published, the Director of the
12 Office of Management and Budget shall, in consultation
13 with the Administrator of the General Services Adminis-
14 tration, issue guidelines for each agency on reporting, co-
15 ordinating, publishing, and receiving information about—

16 (1) a security vulnerability relating to a covered
17 device used by the agency; and

18 (2) the resolution of such security vulnerability.

19 (b) CONTRACTOR AND VENDOR COMPLIANCE WITH
20 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
21 GUIDANCE.—The guidelines required by subsection (a)
22 shall include a limitation that prohibits an agency from
23 acquiring or using any covered device from a contractor
24 or vendor if the contractor or vendor fails to comply with
25 the guidance published under section 5(a).

1 (c) CONSISTENCY WITH GUIDANCE FROM NATIONAL
2 INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Di-
3 rector shall ensure that the guidelines issued under sub-
4 section (a) are consistent with the guidance published
5 under section 5(a).

○