

Union Calendar No. 402

116TH CONGRESS
2^D SESSION

H. R. 1668

[Report No. 116–501, Part I]

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

SEPTEMBER 14, 2020

Additional sponsors: Mr. OLSON, Ms. HILL of California, Mr. FITZPATRICK, Mr. O'HALLERAN, Mrs. BROOKS of Indiana, Ms. CLARKE of New York, Ms. STEVENS, Mr. HARDER of California, Mr. NORMAN, Mr. ROUDA, Mr. GRAVES of Georgia, Ms. WASSERMAN SCHULTZ, and Ms. DELBENE

SEPTEMBER 14, 2020

Reported from the Committee on Oversight and Reform with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

SEPTEMBER 14, 2020

Committee on Science, Space, and Technology discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on March 11, 2019]

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 Cyberse-*
6 *curity Improvement Act of 2019”.*

7 **SEC. 2. DEFINITIONS.**

8 *In this Act:*

9 (1) *AGENCY.*—*The term “agency” has the mean-*
10 *ing given such term in section 3502 of title 44,*
11 *United States Code.*

12 (2) *COVERED DEVICE.*—*The term “covered de-*
13 *vice” means a physical object that—*

14 (A) *is capable of being in regular connec-*
15 *tion with—*

16 (i) *the Internet; or*

17 (ii) *a network that is connected to the*
18 *Internet on a recurring basis;*

19 (B) *has computer processing capabilities of*
20 *collecting, sending, or receiving data; and*

21 (C) *is not a—*

22 (i) *general-purpose computing device;*

23 (ii) *personal computing system;*

24 (iii) *smart mobile communications de-*
25 *vice;*

1 (iv) programmable logic controller with
2 an industrial control system specifically not
3 designed for connection to the internet;

4 (v) mainframe computing system; or

5 (vi) subcomponent of a device.

6 (3) *DIRECTOR OF OMB.*—The term “Director of
7 OMB” means the Director of the Office of Manage-
8 ment and Budget.

9 (4) *DIRECTOR OF THE INSTITUTE.*—The term
10 “Director of the Institute” means the Director of the
11 National Institute of Standards and Technology.

12 (5) *SECURITY VULNERABILITY.*—The term “secu-
13 rity vulnerability” has the meaning given that term
14 under section 102(17) of the Cybersecurity Informa-
15 tion Sharing Act of 2015 (6 U.S.C. 1501(17)).

16 **SEC. 3. COMPLETION OF ONGOING EFFORTS RELATING TO**
17 **CONSIDERATIONS FOR MANAGING INTERNET**
18 **OF THINGS CYBERSECURITY RISKS.**

19 Not later than December 31, 2019, the Director of the
20 National Institute of Standards and Technology shall com-
21 plete the efforts of the Institute in effect on the date of the
22 enactment of this Act regarding considerations for man-
23 aging the security vulnerabilities of Internet of Things de-
24 vices and examples of possible cybersecurity capabilities of

1 *such devices by publishing a report that includes, at a min-*
2 *imum, the following considerations for covered devices:*

3 (1) *Secure development.*

4 (2) *Identity management.*

5 (3) *Patching.*

6 (4) *Configuration management.*

7 **SEC. 4. SECURITY STANDARDS FOR USE OF COVERED DE-**
8 **VICES BY THE FEDERAL GOVERNMENT.**

9 (a) *GUIDELINES REQUIRED.—*

10 (1) *GUIDELINES.—Not later than 6 months after*
11 *the date on which the report under section 3 is com-*
12 *pleted, the Director of the Institute shall develop*
13 *under section 20 of the National Institute of Stand-*
14 *ards and Technology Act (15 U.S.C. 278g-3), and*
15 *submit to the Director of OMB, guidelines on—*

16 (A) *the appropriate use and management*
17 *by the agencies of covered devices owned or con-*
18 *trolled by the agencies; and*

19 (B) *minimum information security require-*
20 *ments for managing security vulnerabilities asso-*
21 *ciated with such devices.*

22 (2) *DEVELOPMENT OF GUIDELINES.—In devel-*
23 *oping the guidelines submitted under paragraph (1),*
24 *the Director of the Institute shall—*

1 (A) consider relevant standards and best
2 practices developed by the private sector, agen-
3 cies, and public-private partnerships; and

4 (B) ensure that such guidelines are con-
5 sistent with the considerations published in the
6 report described under section 3.

7 (b) *PROMULGATION OF STANDARDS.*—

8 (1) *STANDARDS.*—Not later than 180 days after
9 the date on which the Director of the Institute com-
10 pletes the development of the guidelines required
11 under subsection (a), the Director of OMB, in con-
12 sultation with the Director of the Cybersecurity and
13 Infrastructure Security Agency of the Department of
14 Homeland Security, shall—

15 (A) promulgate standards on the basis of
16 the guidelines submitted under subsection (a)
17 pertaining to covered devices owned or controlled
18 by agencies, except those considered national se-
19 curity systems as defined by section 3552(b)(6)
20 of title 44, United States Code; and

21 (B) ensure such standards are consistent
22 with the information security requirements
23 under subchapter II of chapter 35 of title 44,
24 United States Code.

1 (2) *QUINQUENNIAL REVIEW AND REVISION.*—Not
2 later than 5 years after the date on which the Direc-
3 tor of OMB promulgates the standards under para-
4 graph (1), and not less frequently than once every 5
5 years thereafter, the Director of OMB, in consultation
6 with and the Director of the Institute and the Direc-
7 tor of the Cybersecurity and Infrastructure Security
8 Agency of the Department of Homeland Security,
9 shall—

10 (A) review such standards; and

11 (B) revise such standards as appropriate.

12 (c) *REVISION OF FEDERAL ACQUISITION REGULA-*
13 *TION.*—The Federal Acquisition Regulation shall be revised
14 to implement any standard promulgated under subsection
15 (b).

16 **SEC. 5. PETITION TO EXCLUDE CERTAIN DEVICES.**

17 (a) *PETITION.*—The Director of OMB shall establish
18 a process by which an interested party may petition the
19 Director of OMB for a device described in section 2(2) to
20 not be considered a covered device for the purpose of stand-
21 ards promulgated under section 4(b).

22 (b) *GRANTS OF PETITION.*—The Director of OMB shall
23 grant a petition under subsection (a)—

24 (1) on a limited basis;

25 (2) in a timely manner; and

1 (3) *only if the interested party demonstrates*
2 *that—*

3 (A) *the procurement of such a covered device*
4 *with limited data processing and software*
5 *functionality would be unfeasible; or*

6 (B) *the procurement of a covered device that*
7 *does not meet the standards promulgated by the*
8 *Director of OMB under this Act is necessary for*
9 *national security or for research purposes.*

10 (c) *REPORT.—*

11 (1) *IN GENERAL.—Not later than one year after*
12 *the date of the enactment of this Act, and annually*
13 *thereafter for each of the following four years, the Di-*
14 *rector of OMB shall submit to the appropriate con-*
15 *gressional committees a report on the process estab-*
16 *lished by the Director of OMB for granting or deny-*
17 *ing waivers under this section.*

18 (2) *ASSESSMENT OF IMPLEMENTATION.—The re-*
19 *ports required under paragraph (1) shall include, at*
20 *a minimum, the following:*

21 (A) *An assessment of the waiver evaluation*
22 *process.*

23 (B) *A description of the methods established*
24 *to carry out such assessment.*

1 (C) *A classified appendix listing the types*
2 *and number of devices for each agency granted*
3 *a waiver and the reasons for such waiver.*

4 (3) *APPROPRIATE CONGRESSIONAL COMMITTEES*
5 *DEFINED.—In this subsection, the term “appropriate*
6 *congressional committees” means the Committees on*
7 *Oversight and Reform and Homeland Security of the*
8 *House of Representatives and the Committee on*
9 *Homeland Security and Governmental Affairs of the*
10 *Senate.*

11 **SEC. 6. COORDINATED DISCLOSURE OF SECURITY**
12 **VULNERABILITIES RELATING TO COVERED**
13 **DEVICES.**

14 (a) *IN GENERAL.—Not later than 180 days after the*
15 *date of the enactment of this Act, the Director of the Insti-*
16 *tute, in consultation with the Director of Cybersecurity and*
17 *Infrastructure Security Agency of the Department of Home-*
18 *land Security, shall develop under section 20 of the Na-*
19 *tional Institute of Standards and Technology Act (15*
20 *U.S.C. 278g-3) and submit to the Director of OMB, guide-*
21 *lines—*

22 (1) *for the reporting, coordinating, publishing,*
23 *and receiving of information about—*

1 (A) a security vulnerability relating to a
2 covered device owned or controlled by an agency;
3 and

4 (B) the resolution of such security vulner-
5 ability;

6 (2) for contractors providing a covered device to
7 the Federal Government, and any subcontractor there-
8 of at any tier providing such device to such contrac-
9 tors on—

10 (A) receiving information about a potential
11 security vulnerability relating to the covered de-
12 vice; and

13 (B) disseminating information about the
14 resolution of a security vulnerability relating to
15 the covered device; and

16 (3) on the type of information about security
17 vulnerabilities that should be reported to the Federal
18 Government, including examples thereof.

19 (b) *DEVELOPMENT OF GUIDELINES.*—In developing
20 the guidelines under subsection (a), the Director of the Insti-
21 tute shall—

22 (1) consult with such cybersecurity researchers
23 and private sector industry experts as the Director
24 considers appropriate;

1 (2) *to the maximum extent practicable, align*
2 *such guidelines with Standards 29147 and 30111 of*
3 *the International Standards Organization, or any*
4 *successor standards thereof; and*

5 (3) *ensure such guidelines are consistent with the*
6 *policies and procedures developed under section*
7 *2209(m) of the Homeland Security Act of 2002 (6*
8 *U.S.C. 659(m)).*

9 *(c) PROMULGATION OF STANDARDS.—*

10 (1) *IN GENERAL.—Not later than 180 days after*
11 *the date on which the guidelines under subsection (a)*
12 *are submitted, the Director of OMB, in consultation*
13 *with the Administrator of General Services and the*
14 *Secretary of Homeland Security, shall promulgate*
15 *standards on the basis of such guidelines.*

16 (2) *CONTRACT REQUIREMENT FOR SUB-*
17 *CONTRACTS.—The standards promulgated under*
18 *paragraph (1) shall include a requirement for any*
19 *contract related to a covered device to include a clause*
20 *that requires each contractor that provides a covered*
21 *device under the contract to an agency to ensure that*
22 *any covered device obtained through a subcontract, at*
23 *any tier, complies with the standards and regulations*
24 *promulgated under this section with respect to such*
25 *covered device.*

1 (B) *SIMPLIFIED ACQUISITION THRESH-*
2 *OLD.—Notwithstanding section 1905 of title 41,*
3 *United States Code, the requirements under sub-*
4 *paragraph (A) shall apply to a contract or sub-*
5 *contract in amounts not greater than the sim-*
6 *plified acquisition threshold.*

7 (2) *PROHIBITION ON USE OR PROCUREMENT.—*
8 *The head of an agency may not procure or obtain, or*
9 *renew a contract to procure or obtain, a covered de-*
10 *vice if the agency Chief Information Officer deter-*
11 *mines under paragraph (1)(A) that such offeror or*
12 *contractor has not complied with a standard promul-*
13 *gated under section 6(c) with respect to such covered*
14 *device.*

15 (b) *WAIVER.—The head of an agency may waive the*
16 *prohibition under subsection (a)(2) if the procurement of*
17 *such covered device is necessary for national security or for*
18 *research purposes.*

19 (c) *EFFECTIVE DATE.—The prohibition under sub-*
20 *section (a) shall take effect one year after the date of the*
21 *enactment of this Act.*

1 **SEC. 8. INSTITUTE REPORT ON CYBERSECURITY CONSIDER-**
2 **ATIONS STEMMING FROM THE CONVERGENCE**
3 **OF INFORMATION TECHNOLOGY, INTERNET**
4 **OF THINGS, AND OPERATIONAL TECHNOLOGY**
5 **DEVICES, NETWORKS AND SYSTEMS.**

6 *Not later than 1 year after the date of the enactment*
7 *of this Act, the Director of the Institute shall publish a re-*
8 *port on the increasing convergence, including consider-*
9 *ations for managing potential security vulnerabilities asso-*
10 *ciated with such convergence, of traditional information*
11 *technology devices, networks, and systems with—*

- 12 *(1) covered devices, networks and systems; and*
13 *(2) operational technology devices, networks and*
14 *systems.*

Union Calendar No. 402

116TH CONGRESS
2^D SESSION

H. R. 1668

[Report No. 116-501, Part I]

A BILL

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

SEPTEMBER 14, 2020

Reported from the Committee on Oversight and Reform
with an amendment

SEPTEMBER 14, 2020

Committee on Science, Space, and Technology discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed