

Calendar No. 215116TH CONGRESS
1ST SESSION**S. 734****[Report No. 116–112]**

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

IN THE SENATE OF THE UNITED STATES

MARCH 11, 2019

Mr. WARNER (for himself, Mr. GARDNER, Ms. HASSAN, Mr. DAINES, Ms. CORTEZ MASTO, and Mr. ROUNDS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

SEPTEMBER 23, 2019

Reported by Mr. JOHNSON, with an amendment

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Internet of Things Cy-
3 bersecurity Improvement Act of 2019” or the “IoT Cyber-
4 security Improvement Act of 2019”.

5 **SEC. 2. DEFINITIONS.**

6 In this Act:

7 (1) **AGENCY.**—The term “agency” has the
8 meaning given such term in section 3502 of title 44,
9 United States Code.

10 (2) **COVERED DEVICE.**—

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

13 (i) is capable of connecting to and is
14 in regular connection with the Internet;

15 (ii) has computer processing capabili-
16 ties that can collect, send, or receive data;
17 and

18 (iii) is not a general-purpose com-
19 puting device, including personal com-
20 puting systems, smart mobile communica-
21 tions devices, programmable logic controls,
22 and mainframe computing systems.

23 (B) **MODIFICATION OF DEFINITION.**—The
24 Director of the Office of Management and
25 Budget shall establish a process by which—

1 (i) interested parties may petition for
 2 a device that is not described in subpara-
 3 graph (A) to be considered a device that is
 4 not a covered device; and

5 (ii) the Director acts upon any peti-
 6 tion submitted under clause (i) in a timely
 7 manner.

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

15 **SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
 16 **NOLOGY CONSIDERATIONS AND REC-**
 17 **COMMENDATIONS REGARDING MANAGING**
 18 **INTERNET OF THINGS CYBERSECURITY**
 19 **RISKS.**

20 (a) COMPLETION OF ONGOING EFFORTS RELATING
 21 TO CONSIDERATIONS FOR MANAGING INTERNET OF
 22 THINGS CYBERSECURITY RISKS.—

23 (1) IN GENERAL.—The Director of the National
 24 Institute of Standards and Technology shall ensure
 25 that the efforts of the Institute in effect on the date

1 of the enactment of this Act regarding consider-
2 ations for managing Internet of Things cybersecurity
3 risks, especially regarding examples of possible cy-
4 bersecurity capabilities of Internet of Things devices,
5 are completed no later than September 30, 2019.

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

11 (A) Secure Development.

12 (B) Identity management.

13 (C) Patching.

14 (D) Configuration management.

15 (b) DEVELOPMENT OF RECOMMENDED STANDARDS
16 FOR USE OF INTERNET OF THINGS DEVICES BY FED-
17 ERAL GOVERNMENT.—

18 (1) IN GENERAL.—Not later than March 31,
19 2020, the Director of the Institute shall develop rec-
20 ommendations for the Federal Government on the
21 appropriate use and management by the Federal
22 Government of Internet of Things devices owned or
23 controlled by the Federal Government, including
24 minimum information security requirements for

1 managing cybersecurity risks associated with such
2 devices.

3 ~~(2) CONSISTENCY WITH ONGOING EFFORTS.—~~

4 The Director of the Institute shall ensure that the
5 recommendations and standards developed under
6 paragraph ~~(1)~~ are consistent with the efforts re-
7 ferred to in subsection ~~(a)~~, especially with respect to
8 the examples of possible cybersecurity capabilities re-
9 ferred to in such subsection.

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

1 **SEC. 4. POLICIES FOR FEDERAL AGENCIES ON USE AND**
2 **MANAGEMENT OF INTERNET OF THINGS DE-**
3 **VICES.**

4 (a) **REVISIONS TO THE FEDERAL ACQUISITION REG-**
5 **ULATION.**—Not later than 180 days after the date on
6 which the Director of the National Institute of Standards
7 and Technology completes the development of the rec-
8 ommendations required under section 3(b), the Director
9 of the Office of Management and Budget shall issue guide-
10 lines for each agency that are consistent with such rec-
11 ommendations.

12 (b) **REQUIREMENT.**—In issuing the guidelines re-
13 quired under subsection (a), the Director of the Office of
14 Management and Budget shall ensure that the guidelines
15 are consistent with the information security requirements
16 in subchapter II of chapter 35 of title 44, United States
17 Code.

18 (c) **QUINQUENNIAL REVIEWS AND REVISIONS.**—Not
19 less frequently than once every 5 years—

20 (1) the Director of the Office of Management
21 and Budget and the Director of the National Insti-
22 tute of Standards and Technology shall review the
23 policies issued under subsection (a); and

24 (2) the Director of the Office of Management
25 and Budget shall, in consultation with the Director

1 of the National Institute of Standards and Tech-
2 nology, revise such policies.

3 **SEC. 5. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
4 **NOLOGY GUIDANCE ON COORDINATED DIS-**
5 **CLOSURE OF SECURITY VULNERABILITIES**
6 **RELATING TO INTERNET OF THINGS DE-**
7 **VICES.**

8 (a) IN GENERAL.—Not later than 180 days after the
9 date of the enactment of this Act, the Director of the Na-
10 tional Institute of Standards and Technology shall, in con-
11 sultation with such cybersecurity researchers and private-
12 sector industry experts as the Director considers appro-
13 priate, publish guidance on policies and procedures for the
14 reporting, coordinating, publishing, and receiving of infor-
15 mation about—

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

18 (2) the resolution of such security vulnerability.

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

21 (1) Policies and procedures described in sub-
22 section (a) that, to the maximum extent practicable,
23 are aligned with Standards 29147 and 30111 of the
24 International Standards Organization, or any suc-
25 cessor standards. Such policies and procedures shall

1 include policies and procedures for a contractor or
2 vendor providing a covered device to the Federal
3 Government on—

4 (A) receiving information about a potential
5 security vulnerability relating to the covered de-
6 vice; and

7 (B) disseminating information about the
8 resolution of a security vulnerability relating to
9 the covered device.

10 (2) Guidance, including example content, on the
11 information items that should be produced through
12 the implementation of the security vulnerability dis-
13 closure process of the contractor.

14 **SEC. 6. GUIDELINES FOR FEDERAL AGENCIES ON COORDI-**
15 **NATED DISCLOSURE OF SECURITY**
16 **VULNERABILITIES RELATING TO INTERNET**
17 **OF THINGS DEVICES.**

18 (a) **AGENCY GUIDELINES REQUIRED.**—Not later
19 than 180 days after the date on which the guidance re-
20 quired under section 4 is published, the Director of the
21 Office of Management and Budget shall, in consultation
22 with the Administrator of the General Services Adminis-
23 tration, issue guidelines for each agency on reporting, co-
24 ordinating, publishing, and receiving information about—

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

3 (2) the resolution of such security vulnerability.

4 (b) **CONTRACTOR AND VENDOR COMPLIANCE WITH**
5 **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
6 **GUIDANCE.**—The guidelines required by subsection (a)
7 shall include a limitation that prohibits an agency from
8 acquiring or using any covered device from a contractor
9 or vendor if the contractor or vendor fails to comply with
10 the guidance published under section 5(a).

11 (c) **CONSISTENCY WITH GUIDANCE FROM NATIONAL**
12 **INSTITUTE OF STANDARDS AND TECHNOLOGY.**—The Di-
13 rector shall ensure that the guidelines issued under sub-
14 section (a) are consistent with the guidance published
15 under section 5(a).

16 **SECTION 1. SHORT TITLE.**

17 *This Act may be cited as the “Internet of Things Cy-*
18 *bersecurity Improvement Act of 2019” or the “IoT Cyberse-*
19 *curity Improvement Act of 2019”.*

20 **SEC. 2. DEFINITIONS.**

21 *In this Act:*

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

1 (2) *DIRECTOR.*—*The term “Director” means the*
 2 *Director of the National Institute of Standards and*
 3 *Technology.*

4 (3) *INFORMATION SYSTEM.*—*The term “informa-*
 5 *tion system” has the meaning given the term in sec-*
 6 *tion 3502 of title 44, United States Code.*

7 (4) *SECRETARY.*—*The term “Secretary” means*
 8 *the Secretary of Homeland Security.*

9 (5) *SECURITY VULNERABILITY.*—*The term “secu-*
 10 *urity vulnerability” has the meaning given the term in*
 11 *section 102 of the Cybersecurity Information Sharing*
 12 *Act of 2015 (6 U.S.C. 1501).*

13 **SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
 14 **NOLOGY CONSIDERATIONS AND REC-**
 15 **COMMENDATIONS REGARDING MANAGING**
 16 **INTERNET OF THINGS CYBERSECURITY**
 17 **RISKS.**

18 (a) *DEVELOPMENT OF RECOMMENDED GUIDELINES*
 19 *FOR USE OF INTERNET OF THINGS DEVICES BY FEDERAL*
 20 *GOVERNMENT.*—

21 (1) *IN GENERAL.*—*Not later than March 31,*
 22 *2020, the Director shall develop standards and guide-*
 23 *lines for the Federal Government on the appropriate*
 24 *use and management by the Federal Government of*
 25 *Internet of Things devices owned or controlled by the*

1 *Federal Government, including minimum informa-*
2 *tion security requirements for managing cybersecurity*
3 *risks associated with such devices.*

4 (2) *CONSISTENCY WITH ONGOING EFFORTS.—The*
5 *Director shall ensure that the standards and guide-*
6 *lines developed under paragraph (1) are consistent*
7 *with the efforts of the National Institute of Standards*
8 *and Technology in effect on the date of enactment of*
9 *this Act regarding considerations for managing Inter-*
10 *net of Things cybersecurity risks, especially regarding*
11 *examples of possible cybersecurity capabilities of*
12 *Internet of Things devices, and in particular with re-*
13 *spect to the following considerations for Internet of*
14 *Things devices:*

15 (A) *Secure development.*

16 (B) *Identity management.*

17 (C) *Patching.*

18 (D) *Configuration management.*

19 (b) *INSTITUTE REPORT ON CYBERSECURITY CONSID-*
20 *ERATIONS STEMMING FROM THE CONVERGENCE OF INFOR-*
21 *MATION TECHNOLOGY, INTERNET OF THINGS, AND OPER-*
22 *ATIONAL TECHNOLOGY DEVICES, NETWORKS, AND SYS-*
23 *TEMS.—Not later than 180 days after the date of enactment*
24 *of this Act, the Director shall brief the appropriate commit-*
25 *tees of Congress on the increasing convergence of traditional*

1 *information technology devices, networks, and systems with*
 2 *Internet of Things devices, networks, and systems and oper-*
 3 *ational technology devices, networks, and systems, including*
 4 *considerations for managing cybersecurity risks and secu-*
 5 *rity vulnerabilities associated with such trends.*

6 **SEC. 4. POLICIES AND PRINCIPLES FOR FEDERAL AGEN-**
 7 **CIES ON USE AND MANAGEMENT OF INTER-**
 8 **NET OF THINGS DEVICES.**

9 *(a) IN GENERAL.—Not later than 180 days after the*
 10 *date on which the Director completes the development of the*
 11 *standards and guidelines required under section 3(a), the*
 12 *Director of the Office of Management and Budget, in con-*
 13 *sultation with the Secretary, shall issue policies and prin-*
 14 *ciples for each agency that are consistent with such stand-*
 15 *ards and guidelines.*

16 *(b) REQUIREMENT.—In issuing the policies, prin-*
 17 *ciples, standards, or guidelines required under subsection*
 18 *(a), the Director of the Office of Management and Budget,*
 19 *in consultation with the Secretary, shall ensure that the*
 20 *policies and principles are consistent with the information*
 21 *security requirements in subchapter II of chapter 35 of title*
 22 *44, United States Code.*

23 *(c) REVIEWS AND REVISIONS.—The Director of the Of-*
 24 *fice of Management and Budget, in consultation with the*
 25 *Secretary, shall—*

1 (1) *review any policies, principles, standards, or*
 2 *guidelines issued under subsection (a); and*

3 (2) *revise such policies, principles, standards,*
 4 *and guidelines.*

5 **SEC. 5. GUIDELINES ON COORDINATED DISCLOSURE OF SE-**
 6 **CURITY VULNERABILITIES RELATING TO IN-**
 7 **FORMATION SYSTEMS, INCLUDING INTERNET**
 8 **OF THINGS DEVICES.**

9 (a) *IN GENERAL.*—*Not later than 1 year after the date*
 10 *of enactment of this Act, the Director, in consultation with*
 11 *such cybersecurity researchers and private-sector industry*
 12 *experts as the Director considers appropriate, and in con-*
 13 *sultation with the Secretary, shall publish guidelines for the*
 14 *reporting, coordinating, publishing, and receiving of infor-*
 15 *mation about—*

16 (1) *a security vulnerability relating to agency*
 17 *information systems, including Internet of Things de-*
 18 *vices; and*

19 (2) *the resolution of such security vulnerability.*

20 (b) *ELEMENTS.*—*The guidelines published under sub-*
 21 *section (a) shall—*

22 (1) *to the maximum extent practicable, be*
 23 *aligned with industry best practices and Standards*
 24 *29147 and 30111 of the International Standards Or-*
 25 *ganization, or any successor standards; and*

1 (2) *incorporate guidelines on—*

2 (A) *receiving information about a potential*
3 *security or personal information vulnerability*
4 *relating to agency information systems, and*
5 *when relevant, Internet of Things devices; and*

6 (B) *disseminating information about the*
7 *resolution of a security or personal information*
8 *vulnerability relating to agency information sys-*
9 *tems, and when relevant, Internet of Things de-*
10 *vices.*

11 (c) *INFORMATION ITEMS.—The guidelines published*
12 *under subsection (a) shall include guidelines, including ex-*
13 *ample content, on the information items that should be pro-*
14 *duced through the implementation of the security vulner-*
15 *ability disclosure process of a contractor or vendor pro-*
16 *viding Internet of Things devices to the Federal Govern-*
17 *ment.*

18 (d) *OVERSIGHT.—The Director of the Office of Man-*
19 *agement and Budget shall oversee the implementation of the*
20 *guidelines published under subsection (a).*

21 (e) *OPERATIONAL AND TECHNICAL ASSISTANCE.—The*
22 *Secretary shall provide operational and technical assistance*
23 *in implementing the guidelines published under subsection*
24 *(a).*

1 **SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE**
2 **OF SECURITY VULNERABILITIES RELATING**
3 **TO AGENCY INFORMATION SYSTEMS, INCLUD-**
4 **ING INTERNET OF THINGS DEVICES.**

5 (a) *AGENCY GUIDELINES REQUIRED.*—Not later than
6 180 days after the date on which the Director publishes
7 guidelines under section 5(a), the Director of the Office of
8 Management and Budget shall issue policies and principles
9 on security vulnerabilities of information systems, includ-
10 ing Internet of Things devices.

11 (b) *PROCEDURES.*—The Secretary, in consultation
12 with the Director of the Office of Management and Budget,
13 shall develop and issue procedures for each agency on re-
14 porting, coordinating, publishing, and receiving informa-
15 tion about security vulnerabilities of information systems,
16 including Internet of Things devices.

17 (c) *CONTRACTOR AND VENDOR COMPLIANCE WITH*
18 *POLICIES AND PROCEDURES.*—The procedures required
19 under subsection (b) shall include a limitation that pro-
20 hibits an agency from acquiring or using any Internet of
21 Things device from a contractor or vendor if the contractor
22 or vendor fails to comply with the guidelines published
23 under section 5(a).

24 (d) *CONSISTENCY WITH GUIDELINES FROM NATIONAL*
25 *INSTITUTE OF STANDARDS AND TECHNOLOGY.*—The Sec-
26 retary shall ensure that the procedures required under sub-

1 *section (b) are consistent with applicable standards and*
2 *publications established by the National Institute of Stand-*
3 *ards and Technology.*

4 **SEC. 7. WAIVER.**

5 *The head of an agency may use an Internet of Things*
6 *device without regard to any policies, principles, standards,*
7 *or guidelines issued under this Act if the use of the Internet*
8 *of Things device is—*

9 *(1) necessary for national security or for re-*
10 *search purposes;*

11 *(2) appropriate to the function of the covered de-*
12 *vice;*

13 *(3) secured using alternative and effective meth-*
14 *ods; or*

15 *(4) of substantially higher quality or afford-*
16 *ability than a product that meets such policies, prin-*
17 *ciples, standards, or guidelines.*

Calendar No. 215

116TH CONGRESS
1ST Session

S. 734

[Report No. 116-112]

A BILL

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

SEPTEMBER 23, 2019

Reported with an amendment