

AMENDMENT NO. _____ Calendar No. _____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—116th Cong., 1st Sess.

S. 734

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

Referred to the Committee on _____ and
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended
to be proposed by _____

Viz:

1 Strike all after the enacting clause and insert the fol-
2 lowing:

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”.

7 **SEC. 2. DEFINITIONS.**

8 In this Act:

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

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

4 (3) INFORMATION SYSTEM.—The term “infor-
5 mation system” has the meaning given the term in
6 section 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 “se-
10 curity vulnerability” has the meaning given the term
11 in section 102 of the Cybersecurity Information
12 Sharing 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 FED-
20 ERAL GOVERNMENT.—

21 (1) IN GENERAL.—Not later than March 31,
22 2020, the Director shall develop standards and
23 guidelines for the Federal Government on the appro-
24 priate use and management by the Federal Govern-
25 ment of Internet of Things devices owned or con-

1 trolled by the Federal Government, including min-
2 imum information security requirements for man-
3 aging cybersecurity risks associated with such de-
4 vices.

5 (2) CONSISTENCY WITH ONGOING EFFORTS.—

6 The Director shall ensure that the standards and
7 guidelines developed under paragraph (1) are con-
8 sistent with the efforts of the National Institute of
9 Standards and Technology in effect on the date of
10 the enactment of this Act regarding considerations
11 for managing Internet of Things cybersecurity risks,
12 especially regarding examples of possible cybersecu-
13 rity capabilities of Internet of Things devices, and in
14 particular with respect to the following consider-
15 ations for Internet of Things devices:

16 (A) Secure Development.

17 (B) Identity management.

18 (C) Patching.

19 (D) Configuration management.

20 (b) INSTITUTE REPORT ON CYBERSECURITY CONSID-
21 ERATIONS STEMMING FROM THE CONVERGENCE OF IN-
22 FORMATION TECHNOLOGY, INTERNET OF THINGS, AND
23 OPERATIONAL TECHNOLOGY DEVICES, NETWORKS AND
24 SYSTEMS.—Not later than 180 days after the date of en-
25 actment of this Act, the Director shall brief the appro-

1 p r i a t e c o m m i t t e e s o f C o n g r e s s o n t h e i n c r e a s i n g c o n v e r -
2 g e n c e o f t r a d i t i o n a l i n f o r m a t i o n t e c h n o l o g y d e v i c e s , n e t -
3 w o r k s , a n d s y s t e m s w i t h I n t e r n e t o f T h i n g s d e v i c e s , n e t -
4 w o r k s , a n d s y s t e m s a n d o p e r a t i o n a l t e c h n o l o g y d e v i c e s ,
5 n e t w o r k s , a n d s y s t e m s , i n c l u d i n g c o n s i d e r a t i o n s f o r m a n -
6 a g i n g c y b e r s e c u r i t y r i s k s a n d s e c u r i t y v u l n e r a b i l i t i e s a s s o -
7 c i a t e d w i t h s u c h t r e n d s .

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

11 (a) **IN GENERAL.**—Not later than 180 days after the
12 date on which the Director completes the development of
13 the standards and guidelines required under section 3(a),
14 the Director of the Office of Management and Budget, in
15 consultation with the Secretary, shall issue policies and
16 principles for each agency that are consistent with such
17 standards and guidelines.

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

1 (c) REVIEWS AND REVISIONS.—The Director of the
2 Office of Management and Budget, in consultation with
3 the Secretary, shall—

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

6 (2) revise such policies, principles, standards,
7 and guidelines.

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

12 (a) IN GENERAL.—Not later than 1 year after the
13 date of the enactment of this Act, the Director, in con-
14 sultation with such cybersecurity researchers and private-
15 sector industry experts as the Director considers appro-
16 priate, and in consultation with the Secretary, shall pub-
17 lish guidelines for the reporting, coordinating, publishing,
18 and receiving of information about—

19 (1) a security vulnerability relating to agency
20 information systems, including Internet of Things
21 devices; and

22 (2) the resolution of such security vulnerability.

23 (b) ELEMENTS.—The guidelines published under
24 subsection (a) shall—

1 (1) to the maximum extent practicable, be
2 aligned with industry best practices and Standards
3 29147 and 30111 of the International Standards
4 Organization, or any successor standards; and

5 (2) incorporate guidelines on—

6 (A) receiving information about a potential
7 security or personal information vulnerability
8 relating to agency information systems, and
9 when relevant, Internet of Things devices; and

10 (B) disseminating information about the
11 resolution of a security or personal information
12 vulnerability relating to agency information sys-
13 tems, and when relevant, Internet of Things de-
14 vices.

15 (c) INFORMATION ITEMS.—The guidelines published
16 under subsection (a) shall include guidelines, including ex-
17 ample content, on the information items that should be
18 produced through the implementation of the security vul-
19 nerability disclosure process of a contractor or vendor pro-
20 viding Internet of Things devices to the Federal Govern-
21 ment.

22 (d) OVERSIGHT.—The Director of the Office of Man-
23 agement and Budget shall oversee the implementation of
24 the guidelines published under subsection (a).

1 (e) OPERATIONAL AND TECHNICAL ASSISTANCE.—
2 The Secretary shall provide operational and technical as-
3 sistance in implementing the guidelines published under
4 subsection (a).

5 **SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE**
6 **OF SECURITY VULNERABILITIES RELATING**
7 **TO AGENCY INFORMATION SYSTEMS, IN-**
8 **CLUDING INTERNET OF THINGS DEVICES.**

9 (a) AGENCY GUIDELINES REQUIRED.—Not later
10 than 180 days after the date on which the Director pub-
11 lishes guidelines under section 5(a), the Director of the
12 Office of Management and Budget shall issue policies and
13 principles on security vulnerabilities of information sys-
14 tems, including Internet of Things devices.

15 (b) PROCEDURES.—The Secretary, in consultation
16 with the Director of the Office of Management and Budg-
17 et, shall develop and issue procedures for each agency on
18 reporting, coordinating, publishing, and receiving informa-
19 tion about security vulnerabilities of information systems,
20 including Internet of Things devices.

21 (c) CONTRACTOR AND VENDOR COMPLIANCE WITH
22 POLICIES AND PROCEDURES.—The procedures required
23 under subsection (b) shall include a limitation that pro-
24 hibits an agency from acquiring or using any Internet of
25 Things device from a contractor or vendor if the con-

1 tractor or vendor fails to comply with the guidelines pub-
2 lished under section 5(a).

3 (d) CONSISTENCY WITH GUIDELINES FROM NA-
4 TIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—
5 The Secretary shall ensure that the procedures required
6 under subsection (b) are consistent with applicable stand-
7 ards and publications established by the National Institute
8 of Standards and Technology.

9 **SEC. 7. WAIVER.**

10 The head of an agency may use an Internet of Things
11 device without regard to any policies, principles, stand-
12 ards, or guidelines issued under this Act if the use of the
13 Internet of Things device is—

14 (1) necessary for national security or for re-
15 search purposes;

16 (2) appropriate to the function of the covered
17 device;

18 (3) secured using alternative and effective
19 methods; or

20 (4) of substantially higher quality or afford-
21 ability than a product that meets such policies, prin-
22 ciples, standards, or guidelines.