

116TH CONGRESS
2^D SESSION

H. R. 1668

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 15, 2020

Received

AN ACT

To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, 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 2020” or the “IoT Cyber-
4 security Improvement Act of 2020”.

5 **SEC. 2. SENSE OF CONGRESS.**

6 It is the sense of Congress that—

7 (1) ensuring the highest level of cybersecurity
8 at agencies in the executive branch is the responsi-
9 bility of the President, followed by the Director of
10 the Office of Management and Budget, the Sec-
11 retary of Homeland Security, and the head of each
12 such agency;

13 (2) this responsibility is to be carried out by
14 working collaboratively within and among agencies
15 in the executive branch, industry, and academia;

16 (3) the strength of the cybersecurity of the
17 Federal Government and the positive benefits of dig-
18 ital technology transformation depend on proactively
19 addressing cybersecurity throughout the acquisition
20 and operation of Internet of Things devices by the
21 Federal Government; and

22 (4) consistent with the second draft National
23 Institute for Standards and Technology Interagency
24 or Internal Report 8259 titled “Recommendations
25 for IoT Device Manufacturers: Foundational Activi-
26 ties and Core Device Cybersecurity Capability Base-

1 line”, published in January 2020, Internet of Things
2 devices are devices that—

3 (A) have at least one transducer (sensor or
4 actuator) for interacting directly with the phys-
5 ical world, have at least one network interface,
6 and are not conventional Information Tech-
7 nology devices, such as smartphones and
8 laptops, for which the identification and imple-
9 mentation of cybersecurity features is already
10 well understood; and

11 (B) can function on their own and are not
12 only able to function when acting as a compo-
13 nent of another device, such as a processor.

14 **SEC. 3. DEFINITIONS.**

15 In this Act:

16 (1) AGENCY.—The term “agency” has the
17 meaning given that term in section 3502 of title 44,
18 United States Code.

19 (2) DIRECTOR OF OMB.—The term “Director of
20 OMB” means the Director of the Office of Manage-
21 ment and Budget.

22 (3) DIRECTOR OF THE INSTITUTE.—The term
23 “Director of the Institute” means the Director of
24 the National Institute of Standards and Technology.

1 (4) INFORMATION SYSTEM.—The term “infor-
2 mation system” has the meaning given that term in
3 section 3502 of title 44, United States Code.

4 (5) NATIONAL SECURITY SYSTEM.—The term
5 “national security system” has the meaning given
6 that term in section 3552(b)(6) of title 44, United
7 States Code.

8 (6) OPERATIONAL TECHNOLOGY.—The term
9 “operational technology” means hardware and soft-
10 ware that detects or causes a change through the di-
11 rect monitoring or control of physical devices, proc-
12 esses, and events in the enterprise.

13 (7) SECRETARY.—The term “Secretary” means
14 the Secretary of Homeland Security.

15 (8) SECURITY VULNERABILITY.—The term “se-
16 curity vulnerability” has the meaning given that
17 term in section 102(17) of the Cybersecurity Infor-
18 mation Sharing Act of 2015 (6 U.S.C. 1501(17)).

19 **SEC. 4. SECURITY STANDARDS AND GUIDELINES FOR**
20 **AGENCIES ON USE AND MANAGEMENT OF**
21 **INTERNET OF THINGS DEVICES.**

22 (a) NATIONAL INSTITUTE OF STANDARDS AND
23 TECHNOLOGY DEVELOPMENT OF STANDARDS AND
24 GUIDELINES FOR USE OF INTERNET OF THINGS DEVICES
25 BY AGENCIES.—

1 (1) IN GENERAL.—Not later than 90 days after
2 the date of the enactment of this Act, the Director
3 of the Institute shall develop and publish under sec-
4 tion 20 of the National Institute of Standards and
5 Technology Act (15 U.S.C. 278g–3) standards and
6 guidelines for the Federal Government on the appro-
7 priate use and management by agencies of Internet
8 of Things devices owned or controlled by an agency
9 and connected to information systems owned or con-
10 trolled by an agency, including minimum informa-
11 tion security requirements for managing cybersecu-
12 rity risks associated with such devices.

13 (2) CONSISTENCY WITH ONGOING EFFORTS.—
14 The Director of the Institute shall ensure that the
15 standards and guidelines developed under paragraph
16 (1) are consistent with the efforts of the National
17 Institute of Standards and Technology in effect on
18 the date of the enactment of this Act—

19 (A) regarding—

20 (i) examples of possible security
21 vulnerabilities of Internet of Things de-
22 vices; and

23 (ii) considerations for managing the
24 security vulnerabilities of Internet of
25 Things devices; and

1 (B) with respect to the following consider-
2 ations for Internet of Things devices:

3 (i) Secure Development.

4 (ii) Identity management.

5 (iii) Patching.

6 (iv) Configuration management.

7 (3) CONSIDERING RELEVANT STANDARDS.—In
8 developing the standards and guidelines under para-
9 graph (1), the Director of the Institute shall con-
10 sider relevant standards, guidelines, and best prac-
11 tices developed by the private sector, agencies, and
12 public-private partnerships.

13 (b) REVIEW OF AGENCY INFORMATION SECURITY
14 POLICIES AND PRINCIPLES.—

15 (1) REQUIREMENT.—Not later than 180 days
16 after the date on which the Director of the Institute
17 completes the development of the standards and
18 guidelines required under subsection (a), the Direc-
19 tor of OMB shall review agency information security
20 policies and principles on the basis of the standards
21 and guidelines published under subsection (a) per-
22 taining to Internet of Things devices owned or con-
23 trolled by agencies (excluding agency information se-
24 curity policies and principles pertaining to Internet
25 of Things of devices owned or controlled by agencies

1 that are or comprise a national security system) for
2 consistency with the standards and guidelines sub-
3 mitted under subsection (a) and issue such policies
4 and principles as may be necessary to ensure those
5 policies and principles are consistent with such
6 standards and guidelines.

7 (2) REVIEW.—In reviewing agency information
8 security policies and principles under paragraph (1)
9 and issuing policies and principles under such para-
10 graph, as may be necessary, the Director of OMB
11 shall—

12 (A) consult with the Director of the Cyber-
13 security and Infrastructure Security Agency of
14 the Department of Homeland Security; and

15 (B) ensure such policies and principles are
16 consistent with the information security require-
17 ments under subchapter II of chapter 35 of
18 title 44, United States Code.

19 (3) NATIONAL SECURITY SYSTEMS.—Any policy
20 or principle issued by the Director of OMB under
21 paragraph (1) shall not apply to national security
22 systems.

23 (c) QUINQUENNIAL REVIEW AND REVISION.—

24 (1) REVIEW AND REVISION OF NIST STANDARDS
25 AND GUIDELINES.—Not later than 5 years after the

1 date on which the Director of the Institute publishes
2 the standards and guidelines under subsection (a),
3 and not less frequently than once every 5 years
4 thereafter, the Director of the Institute, shall—

5 (A) review such standards and guidelines;

6 and

7 (B) revise such standards and guidelines
8 as appropriate.

9 (2) UPDATED OMB POLICIES AND PRINCIPLES
10 FOR AGENCIES.—Not later than 180 days after the
11 Director of the Institute makes a revision pursuant
12 to paragraph (1), the Director of OMB, in consulta-
13 tion with the Director of the Cybersecurity and In-
14 frastructure Security Agency of the Department of
15 Homeland Security, shall update any policy or prin-
16 ciple issued under subsection (b)(1) as necessary to
17 ensure those policies and principles are consistent
18 with the review and any revision under paragraph
19 (1) under this subsection and paragraphs (2) and
20 (3) of subsection (b).

21 (d) REVISION OF FEDERAL ACQUISITION REGULA-
22 TION.—The Federal Acquisition Regulation shall be re-
23 vised as necessary to implement any standards and guide-
24 lines promulgated in this section.

1 **SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR**
2 **SECURITY VULNERABILITIES RELATING TO**
3 **INFORMATION SYSTEMS, INCLUDING INTER-**
4 **NET OF THINGS DEVICES.**

5 (a) IN GENERAL.—Not later than 180 days after the
6 date of the enactment of this Act, the Director of the In-
7 stitute, in consultation with such cybersecurity researchers
8 and private sector industry experts as the Director con-
9 siders appropriate, and in consultation with the Secretary,
10 shall develop and publish under section 20 of the National
11 Institute of Standards and Technology Act (15 U.S.C.
12 278g–3) guidelines—

13 (1) for the reporting, coordinating, publishing,
14 and receiving of information about—

15 (A) a security vulnerability relating to in-
16 formation systems owned or controlled by an
17 agency (including Internet of Things devices
18 owned or controlled by an agency); and

19 (B) the resolution of such security vulner-
20 ability; and

21 (2) for a contractor providing to an agency an
22 information system (including an Internet of Things
23 device) and any subcontractor thereof at any tier
24 providing such information system to such con-
25 tractor, on—

1 (A) receiving information about a potential
2 security vulnerability relating to the information
3 system; and

4 (B) disseminating information about the
5 resolution of a security vulnerability relating to
6 the information system.

7 (b) ELEMENTS.—The guidelines published under
8 subsection (a) shall—

9 (1) to the maximum extent practicable, be
10 aligned with industry best practices and Standards
11 29147 and 30111 of the International Standards
12 Organization (or any successor standard) or any
13 other appropriate, relevant, and widely-used stand-
14 ard;

15 (2) incorporate guidelines on—

16 (A) receiving information about a potential
17 security vulnerability relating to an information
18 system owned or controlled by an agency (in-
19 cluding an Internet of Things device); and

20 (B) disseminating information about the
21 resolution of a security vulnerability relating to
22 an information system owned or controlled by
23 an agency (including an Internet of Things de-
24 vice); and

1 (3) be consistent with the policies and proce-
2 dures produced under section 2009(m) of the Home-
3 land Security Act of 2002 (6 U.S.C. 659(m)).

4 (c) INFORMATION ITEMS.—The guidelines published
5 under subsection (a) shall include example content, on the
6 information items that should be reported, coordinated,
7 published, or received pursuant to this section by a con-
8 tractor, or any subcontractor thereof at any tier, providing
9 an information system (including Internet of Things de-
10 vice) to the Federal Government.

11 (d) OVERSIGHT.—The Director of OMB shall oversee
12 the implementation of the guidelines published under sub-
13 section (a).

14 (e) OPERATIONAL AND TECHNICAL ASSISTANCE.—
15 The Secretary, in consultation with the Director of OMB,
16 shall administer the implementation of the guidelines pub-
17 lished under subsection (a) and provide operational and
18 technical assistance in implementing such guidelines.

19 **SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE**
20 **OF SECURITY VULNERABILITIES RELATING**
21 **TO AGENCY INFORMATION SYSTEMS, IN-**
22 **CLUDING INTERNET OF THINGS DEVICES.**

23 (a) AGENCY GUIDELINES REQUIRED.—Not later
24 than 2 years after the date of the enactment of this Act,
25 the Director of OMB, in consultation with the Secretary,

1 shall develop and oversee the implementation of policies,
2 principles, standards, or guidelines as may be necessary
3 to address security vulnerabilities of information systems
4 (including Internet of Things devices).

5 (b) OPERATIONAL AND TECHNICAL ASSISTANCE.—
6 Consistent with section 3553(b) of title 44, United States
7 Code, the Secretary, in consultation with the Director of
8 OMB, shall provide operational and technical assistance
9 to agencies on reporting, coordinating, publishing, and re-
10 ceiving information about security vulnerabilities of infor-
11 mation systems (including Internet of Things devices).

12 (c) CONSISTENCY WITH GUIDELINES FROM NA-
13 TIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—
14 The Secretary shall ensure that the assistance provided
15 under subsection (b) is consistent with applicable stand-
16 ards and publications developed by the Director of the In-
17 stitute.

18 (d) REVISION OF FEDERAL ACQUISITION REGULA-
19 TION.—The Federal Acquisition Regulation shall be re-
20 vised as necessary to implement the provisions under this
21 section.

1 **SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED**
2 **DISCLOSURE OF SECURITY**
3 **VULNERABILITIES RELATING TO AGENCY**
4 **INTERNET OF THINGS DEVICES.**

5 (a) PROHIBITION ON PROCUREMENT AND USE.—

6 (1) IN GENERAL.—The head of an agency is
7 prohibited from procuring or obtaining, renewing a
8 contract to procure or obtain, or using an Internet
9 of Things device, if the Chief Information Officer of
10 that agency determines during a review required by
11 section 11319(b)(1)(C) of title 40, United States
12 Code, of a contract for such device that the use of
13 such device prevents compliance with the standards
14 and guidelines developed under section 4 or the
15 guidelines published under section 5 with respect to
16 such device.

17 (2) SIMPLIFIED ACQUISITION THRESHOLD.—

18 Notwithstanding section 1905 of title 41, United
19 States Code, the requirements under paragraph (1)
20 shall apply to a contract or subcontract in amounts
21 not greater than the simplified acquisition threshold.

22 (b) WAIVER.—

23 (1) AUTHORITY.—The head of an agency may
24 waive the prohibition under subsection (a)(1) with
25 respect to an Internet of Things device if the Chief

1 Information Officer of that agency determines
2 that—

3 (A) the waiver is necessary in the interest
4 of national security;

5 (B) procuring, obtaining, or using such de-
6 vice is necessary for research purposes; or

7 (C) such device is secured using alternative
8 and effective methods appropriate to the func-
9 tion of such device.

10 (2) AGENCY PROCESS.—The Director of OMB
11 shall establish a standardized process for the Chief
12 Information Officer of each agency to follow in de-
13 termining whether the waiver under paragraph (1)
14 may be granted.

15 (c) REPORTS TO CONGRESS.—

16 (1) REPORT.—Every 2 years during the 6-year
17 period beginning on the date of the enactment of
18 this Act, the Comptroller General of the United
19 States shall submit to the Committee on Oversight
20 and Reform of the House of Representatives, the
21 Committee on Homeland Security of the House of
22 Representatives, and the Committee on Homeland
23 Security and Governmental Affairs of the Senate a
24 report—

1 (A) on the effectiveness of the process es-
2 tablished under subsection (b)(2);

3 (B) that contains recommended best prac-
4 tices for the procurement of Internet of Things
5 devices; and

6 (C) that lists—

7 (i) the number and type of each Inter-
8 net of Things device for which a waiver
9 under subsection (b)(1) was granted dur-
10 ing the 2-year period prior to the submis-
11 sion of the report; and

12 (ii) the legal authority under which
13 each such waiver was granted, such as
14 whether the waiver was granted pursuant
15 to subparagraph (A), (B), or (C) of such
16 subsection.

17 (2) CLASSIFICATION OF REPORT.—Each report
18 submitted under this subsection shall be submitted
19 in unclassified form, but may include a classified
20 annex that contains the information described under
21 paragraph (1)(C).

22 (d) EFFECTIVE DATE.—The prohibition under sub-
23 section (a)(1) shall take effect 2 years after the date of
24 the enactment of this Act.

1 **SEC. 8. GOVERNMENT ACCOUNTABILITY OFFICE REPORT**
2 **ON CYBERSECURITY CONSIDERATIONS STEM-**
3 **MING FROM THE CONVERGENCE OF INFOR-**
4 **MATION TECHNOLOGY, INTERNET OF**
5 **THINGS, AND OPERATIONAL TECHNOLOGY**
6 **DEVICES, NETWORKS, AND SYSTEMS.**

7 (a) BRIEFING.—Not later than 1 year after the date
8 of the enactment of this Act, the Comptroller General of
9 the United States shall provide a briefing to the Com-
10 mittee on Oversight and Reform of the House of Rep-
11 resentatives, the Committee on Homeland Security of the
12 House of Representatives, and the Committee on Home-
13 land Security and Governmental Affairs of the Senate on
14 broader Internet of Things efforts, including projects de-
15 signed to assist in managing potential security
16 vulnerabilities associated with the use of traditional infor-
17 mation technology devices, networks, and systems with—

18 (1) Internet of Things devices, networks, and
19 systems; and

20 (2) operational technology devices, networks,
21 and systems.

22 (b) REPORT.—Not later than 2 years after the date
23 of enactment of this Act, the Comptroller General shall
24 submit a report to the Committee on Oversight and Re-
25 form of the House of Representatives, the Committee on
26 Homeland Security of the House of Representatives, and

1 the Committee on Homeland Security and Governmental
2 Affairs of the Senate on broader Internet of Things efforts
3 addressed in subsection (a).

Passed the House of Representatives September 14,
2020.

Attest: CHERYL L. JOHNSON,
Clerk.