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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Internet of Things Cybersecurity Improvement Act of 2019” or the “IoT Cybersecurity Improvement Act of 2019.”
SEC. 2. DEFINITIONS.

In this Act:

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

(2) COVERED DEVICE.—

(A) IN GENERAL.—The term “covered device” means a physical object that—

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

(ii) has computer processing capabilities that can collect, send, or receive data; and

(iii) is not a general-purpose computing device, including personal computing systems, smart mobile communications devices, programmable logic controls, and mainframe computing systems.

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

(i) interested parties may petition for a device that is not described in subparagraph (A) to be considered a device that is not a covered device; and
(ii) the Director acts upon any petition submitted under clause (i) in a timely manner.

(3) Security vulnerability.—The term “security vulnerability” means any attribute of hardware, firmware, software, or combination of 2 or more of these factors that could enable the compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected.

SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CONSIDERATIONS AND RECOMMENDATIONS REGARDING MANAGING INTERNET OF THINGS CYBERSECURITY RISKS.

(a) Completion of Ongoing Efforts Relating to Considerations for Managing Internet of Things Cybersecurity Risks.—

(1) In general.—The Director of the National Institute of Standards and Technology shall ensure that the efforts of the Institute in effect on the date of the enactment of this Act regarding considerations for managing Internet of Things cybersecurity risks, especially regarding examples of possible cybersecurity capabilities of Internet of Things devices, are completed no later than September 30, 2019.
(2) MATTERS ADDRESSED.—In ensuring efforts are completed under paragraph (1), the Director shall also ensure that such efforts address, at a minimum, the following considerations for covered devices:

(A) Secure Development.

(B) Identity management.

(C) Patching.

(D) Configuration management.

(b) DEVELOPMENT OF RECOMMENDED STANDARDS FOR USE OF INTERNET OF THINGS DEVICES BY FEDERAL GOVERNMENT.—

(1) IN GENERAL.—Not later than March 31, 2020, the Director of the Institute shall develop recommendations for the Federal Government on the appropriate use and management by the Federal Government of Internet of Things devices owned or controlled by the Federal Government, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) CONSISTENCY WITH ONGOING EFFORTS.—The Director of the Institute shall ensure that the recommendations and standards developed under paragraph (1) are consistent with the efforts re-
ferred to in subsection (a), especially with respect to
the examples of possible cybersecurity capabilities re-
ferred to in such subsection.

(e) INSTITUTE REPORT ON CYBERSECURITY CONSID-
erations Stemming From the Convergence of In-
formation Technology, Internet of Things, and
Operational Technology Devices, Networks and
Systems.—Not later than 180 days following the enact-
ment of this Act, the Director of the Institute shall publish
a draft report related to the increasing convergence of tra-
ditional Information Technology devices, networks, and
systems with Internet of Things devices, networks and sys-
tems and Operational Technology devices, networks and
systems, including considerations for managing cybersecu-

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

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

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

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

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

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

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

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

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

(2) the resolution of such security vulnerability.

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

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

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

(B) disseminating information about the
resolution of a security vulnerability relating to
the covered device.
(2) Guidance, including example content, on the information items that should be produced through the implementation of the security vulnerability disclosure process of the contractor.

SEC. 6. GUIDELINES FOR FEDERAL AGENCIES ON COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO INTERNET OF THINGS DEVICES.

(a) AGENCY GUIDELINES REQUIRED.—Not later than 180 days after the date on which the guidance required under section 4 is published, the Director of the Office of Management and Budget shall, in consultation with the Administrator of the General Services Administration, issue guidelines for each agency on reporting, coordinating, publishing, and receiving information about—

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

(2) the resolution of such security vulnerability.

(b) CONTRACTOR AND VENDOR COMPLIANCE WITH NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GUIDANCE.—The guidelines required by subsection (a) shall include a limitation that prohibits an agency from acquiring or using any covered device from a contractor or vendor if the contractor or vendor fails to comply with the guidance published under section 5(a).
(c) Consistency With Guidance From National Institute of Standards and Technology.—The Director shall ensure that the guidelines issued under subsection (a) are consistent with the guidance published under section 5(a).