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:

Strike all after the enacting clause and insert the following:

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) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(5) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

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

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

(1) IN GENERAL.—Not later than March 31, 2020, the Director shall develop standards and guidelines for the Federal Government on the appropriate use and management by the Federal Government of Internet of Things devices owned or con-

trolled by the Federal Government, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) CONSISTENCY WITH ONGOING EFFORTS.—The Director shall ensure that the standards and guidelines developed under paragraph (1) are consistent with the efforts of the National Institute of Standards and Technology 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, and in particular with respect to the following considerations for Internet of Things devices:

(A) Secure Development.

(B) Identity management.

(C) Patching.

(D) Configuration management.

(b) INSTITUTE REPORT ON CYBERSECURITY CONSIDERATIONS STEMMING FROM THE CONVERGENCE OF INFORMATION TECHNOLOGY, INTERNET OF THINGS, AND OPERATIONAL TECHNOLOGY DEVICES, NETWORKS AND SYSTEMS.—Not later than 180 days after the date of enactment of this Act, the Director shall brief the appro-

priate committees of Congress on the increasing convergence of traditional information technology devices, networks, and systems with Internet of Things devices, networks, and systems and operational technology devices, networks, and systems, including considerations for managing cybersecurity risks and security vulnerabilities associated with such trends.

SEC. 4. POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES FOR FEDERAL AGENCIES ON USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES.

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

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

(c) QUINQUENNIAL REVIEWS AND REVISIONS.—Not less frequently than once every 5 years, the Director of the Office of Management and Budget, in consultation with the Secretary, shall—

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

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

SEC. 5. GUIDELINES ON COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director, in consultation with such cybersecurity researchers and private-sector industry experts as the Director considers appropriate, and in consultation with the Secretary, shall publish guidelines for the reporting, coordinating, publishing, and receiving of information about—

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

(2) the resolution of such security vulnerability.

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

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

(2) incorporate guidelines on—

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

(B) disseminating information about the resolution of a security or personal information vulnerability relating to agency information systems, and when relevant, Internet of Things devices.

(c) INFORMATION ITEMS.—The guidelines published under subsection (a) shall include guidelines, including example content, on the information items that should be produced through the implementation of the security vulnerability disclosure process of a contractor or vendor providing Internet of Things devices to the Federal Government.

(d) OVERSIGHT.—The Director of the Office of Management and Budget shall oversee the implementation of the guidelines published under subsection (a).

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

SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) AGENCY GUIDELINES REQUIRED.—Not later than 180 days after the date on which the Director publishes guidelines under section 5(a), the Director of the Office of Management and Budget shall issues policies, principles, standards, or guidelines on security vulnerabilities of information systems, including Internet of Things devices.

(b) PROCEDURES.—The Secretary, in consultation with the Director of the Office of Management and Budget, shall develop and issue procedures for each agency on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems, including internet of things devices.

(c) CONTRACTOR AND VENDOR COMPLIANCE WITH POLICIES AND PROCEDURES.—The procedures required under subsection (b) shall include a limitation that prohibits an agency from acquiring or using any Internet of

Things device from a contractor or vendor if the contractor or vendor fails to comply with the guidelines published under section 5(a).

(d) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the procedures required under subsection (b) are consistent with applicable standards and publications established by the National Institute of Standards and Technology.

SEC. 7. WAIVER.

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

(1) necessary for national security or for research purposes;

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

(3) secured using alternative and effective methods; or

(4) of substantially higher quality or affordability than a product that meets such policies, principles, standards, or guidelines.