116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 116–501
Part 1

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2019

SEPTEMBER 14, 2020.—Committed to the Committee of the Whole House on the State of the Union and Ordered to be printed

Mrs. CAROLYN B. MALONEY, of New York, from the Committee on Oversight and Reform, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 1668]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Reform, to whom was referred the bill (H.R. 1668) to leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

99–006

The amendment is as follows:

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) COVERED DEVICE.—The term "covered device" means a physical object that—

(A) is capable of being in regular connection with—

(i) the Internet; or

(ii) a network that is connected to the Internet on a recurring basis;

(B) has computer processing capabilities of collecting, sending, or receiving data; and

(C) is not a—

(i) general-purpose computing device;

(ii) personal computing system;

(iii) smart mobile communications device;

(iv) programmable logic controller with an industrial control system specifically not designed for connection to the internet;

(v) mainframe computing system; or

(vi) subcomponent of a device.

(3) DIRECTOR OF OMB.—The term "Director of OMB" means the Director of the Office of Management and Budget.

(4) DIRECTOR OF THE INSTITUTE.—The term "Director of the Institute" means the Director of the National Institute of Standards and Technology.

(5) SECURITY VULNERABILITY.—The term "security vulnerability" has the meaning given that term under section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)).

SEC. 3. COMPLETION OF ONGOING EFFORTS RELATING TO CONSIDERATIONS FOR MANAGING INTERNET OF THINGS CYBERSECURITY RISKS.

Not later than December 31, 2019, the Director of the National Institute of Standards and Technology shall complete the efforts of the Institute in effect on the date of the enactment of this Act regarding considerations for managing the security vulnerabilities of Internet of Things devices and examples of possible cybersecurity capabilities of such devices by publishing a report that includes, at a minimum, the following considerations for covered devices:

(1) Secure development.

(2) Identity management.

(3) Patching.

(4) Configuration management.

SEC. 4. SECURITY STANDARDS FOR USE OF COVERED DEVICES BY THE FEDERAL GOVERNMENT.

(a) GUIDELINES REQUIRED.—

(1) GUIDELINES.—Not later than 6 months after the date on which the report under section 3 is completed, the Director of the Institute shall develop under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), and submit to the Director of OMB, guidelines on—

(A) the appropriate use and management by the agencies of covered devices owned or controlled by the agencies; and

(B) minimum information security requirements for managing security vulnerabilities associated with such devices.

(2) DEVELOPMENT OF GUIDELINES.—In developing the guidelines submitted under paragraph (1), the Director of the Institute shall—

(A) consider relevant standards and best practices developed by the private sector, agencies, and public-private partnerships; and

(B) ensure that such guidelines are consistent with the considerations published in the report described under section 3.

(b) PROMULGATION OF STANDARDS.—

(1) STANDARDS.—Not later than 180 days after the date on which the Director of the Institute completes the development of the guidelines required under sub-

section (a), the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall—

(A) promulgate standards on the basis of the guidelines submitted under subsection (a) pertaining to covered devices owned or controlled by agencies, except those considered national security systems as defined by section 3552(b)(6) of title 44, United States Code; and

(B) ensure such standards are consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code.

(2) QUINQUENNIAL REVIEW AND REVISION.—Not later than 5 years after the date on which the Director of OMB promulgates the standards under paragraph (1), and not less frequently than once every 5 years thereafter, the Director of OMB, in consultation with and the Director of the Institute and the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall—

(A) review such standards; and

(B) revise such standards as appropriate.

(c) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised to implement any standard promulgated under subsection (b).

SEC. 5. PETITION TO EXCLUDE CERTAIN DEVICES.

(a) PETITION.—The Director of OMB shall establish a process by which an interested party may petition the Director of OMB for a device described in section 2(2) to not be considered a covered device for the purpose of standards promulgated under section 4(b).

(b) GRANTS OF PETITION.—The Director of OMB shall grant a petition under subsection (a)—

(1) on a limited basis;

(2) in a timely manner; and

(3) only if the interested party demonstrates that—

(A) the procurement of such a covered device with limited data processing and software functionality would be unfeasible; or

(B) the procurement of a covered device that does not meet the standards promulgated by the Director of OMB under this Act is necessary for national security or for research purposes.

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter for each of the following four years, the Director of OMB shall submit to the appropriate congressional committees a report on the process established by the Director of OMB for granting or denying waivers under this section.

(2) ASSESSMENT OF IMPLEMENTATION.—The reports required under paragraph (1) shall include, at a minimum, the following:

(A) An assessment of the waiver evaluation process.

(B) A description of the methods established to carry out such assessment.

(C) A classified appendix listing the types and number of devices for each agency granted a waiver and the reasons for such waiver.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term "appropriate congressional committees" means the Committees on Oversight and Reform and Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

SEC. 6. COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO COVERED DEVICES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Institute, in consultation with the Director of Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall develop under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and submit to the Director of OMB, guidelines—

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

(A) a security vulnerability relating to a covered device owned or controlled by an agency; and

(B) the resolution of such security vulnerability;

(2) for contractors providing a covered device to the Federal Government, and any subcontractor thereof at any tier providing such device to such contractors on—

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

(B) disseminating information about the resolution of a security vulnerability relating to the covered device; and

(3) on the type of information about security vulnerabilities that should be reported to the Federal Government, including examples thereof.

(b) DEVELOPMENT OF GUIDELINES.—In developing the guidelines under subsection (a), the Director of the Institute shall—

(1) consult with such cybersecurity researchers and private sector industry experts as the Director considers appropriate;

(2) to the maximum extent practicable, align such guidelines with Standards 29147 and 30111 of the International Standards Organization, or any successor standards thereof; and

(3) ensure such guidelines are consistent with the policies and procedures developed under section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

(c) PROMULGATION OF STANDARDS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the guidelines under subsection (a) are submitted, the Director of OMB, in consultation with the Administrator of General Services and the Secretary of Homeland Security, shall promulgate standards on the basis of such guidelines.

(2) CONTRACT REQUIREMENT FOR SUBCONTRACTS.—The standards promulgated under paragraph (1) shall include a requirement for any contract related to a covered device to include a clause that requires each contractor that provides a covered device under the contract to an agency to ensure that any covered device obtained through a subcontract, at any tier, complies with the standards and regulations promulgated under this section with respect to such covered device.

(3) CONSISTENCY WITH THE STRENGTHENING AND ENHANCING CYBER-CAPABILITIES BY UTILIZING RISK EXPOSURE TECHNOLOGY ACT.—The Director of OMB shall ensure that the standards promulgated under paragraph (1) are consistent with section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (6 U.S.C. 663 note; Public Law 115–390).

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised to implement the standards promulgated under subsection (c).

SEC. 7. CONTRACTOR COMPLIANCE WITH STANDARDS AND REGULATIONS.

(a) IN GENERAL.—

(1) DETERMINATION.—

(A) COMPLIANCE REQUIRED.—Before awarding a contract to an offeror for the procurement of a covered device, or renewing a contract to procure or obtain a covered device from a contractor, the agency Chief Information Officer shall determine if such offeror or contractor has complied with each standard promulgated under section 6(c) with respect to such covered device.

(B) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under subparagraph (A) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

(2) PROHIBITION ON USE OR PROCUREMENT.—The head of an agency may not procure or obtain, or renew a contract to procure or obtain, a covered device if the agency Chief Information Officer determines under paragraph (1)(A) that such offeror or contractor has not complied with a standard promulgated under section 6(c) with respect to such covered device.

(b) WAIVER.—The head of an agency may waive the prohibition under subsection (a)(2) if the procurement of such covered device is necessary for national security or for research purposes.

(c) EFFECTIVE DATE.—The prohibition under subsection (a) shall take effect one year after the date of the enactment of this Act.

SEC. 8. 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 1 year after the date of the enactment of this Act, the Director of the Institute shall publish a report on the increasing convergence, including considerations for managing potential security vulnerabilities associated with such con-

vergence, of traditional information technology devices, networks, and systems with—

(1) covered devices, networks and systems; and

(2) operational technology devices, networks and systems.

SUMMARY AND PURPOSE OF LEGISLATION

The Internet of Things Cybersecurity Improvement Act of 2019 would require enhanced levels of cybersecurity for federally procured Internet of Things devices.

BACKGROUND AND NEED FOR LEGISLATION

H.R. 1668 would establish cybersecurity standards for federal devices that are connected to the internet.[1] At the moment, there are no national standards to ensure the security of Internet of Things Devices (IoT).[2] As such, hackers frequently target IoT devices, "leading to problems like default passwords and vulnerabilities that can't be fixed."[3]

In 2016, internet access was denied for millions on the East Coast due to a distributed denial of service attack facilitated by "hundreds of thousands of compromised unsecured IoT devices."[4] Device vulnerability can pose a threat to the Federal Government because "these devices can serve as gateways to accessing a network and launching cyberattacks."[5]

In a 2018 Senate hearing, Director of Defense Intelligence Agency Lt. General Robert Ashley testified that "insecure IoT devices are one of the 'most important emerging cyberthreats' to US national security."[6]

The bill would require any contractor or vendor at any tier that provides IoT devices to the Federal Government to meet minimum cybersecurity standards based on guidelines by the National Institute of Standards and Technology (NIST).[7] Exceptions from this requirement could be approved be the Director of the Office of Management and Budget (OMB) if an interested party demonstrated that the covered device is required for national security or research purposes.[8]

The NIST security guidelines for managing risk would be established by September 20, 2019 and reviewed every five years. OMB would promulgate standards for agency implementation based on the NIST guidelines by March 30, 2020. The bill would also require vendors of IoT devices to disclose when devices are vulnerable to cyberattacks.

---

[1] House Committee on Oversight and Reform, Statement of Chairman Elijah E. Cummings, Business Meeting (June 12, 2019).

[2] *Congress Introduces Bill to Improve 'Internet of Things' Security*, C/Net (Mar. 11, 2019) (online at www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security/).

[3] *Id.*

[4] House Committee on Oversight and Reform, Statement of Rep. Robin Kelly, Business Meeting (June 12, 2019).

[5] *Id.*

[6] Senate Committee on Armed Services, Written Testimony of Lieutenant General Robert Ashley, Director, Defense Intelligence Agency, *Worldwide Threat Assessment*, 115th Cong. (Mar. 6, 2018) (online at www.armed-services.senate.gov/imo/media/doc/Ashley_03-06-18.pdf).

[7] *Congress Introduces Bill to Improve 'Internet of Things' Security,* C/Net (Mar. 11, 2019) (online at www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security/).

[8] House Committee on Oversight and Reform, Statement of Rep. Robin Kelly, Business Meeting (June 12, 2019).

The number of connected devices is expected to surpass 20 billion by 2020.[9] These standards may encourage IoT manufacturers to increase the level of security of their devices.[10]

SECTION-BY-SECTION ANALYSIS

Section 1. Short titles

Short titles for the bill include: "Internet of Things Cybersecurity Improvement Act of 2019" and "IoT Cybersecurity Improvement Act of 2019."

Section 2. Definitions

Section 2 provides certain definitions, including for a "covered device." A covered device refers to a physical object that can maintain regular connection with the Internet or a network connected to the internet on a recurring basis; has computer processing capabilities to collect, send, or receive data; and is not a general-purpose computing device, personal computing system, smart mobile communications device, programmable logic controller with an industrial control system not designed for connection to the internet, mainframe computing system, or subcomponent of a device.

Section 3. Completion of ongoing efforts relating to considerations for managing Internet of Things cybersecurity risks

Section 3 requires the Director of NIST to publish a report by December 31, 2019, regarding management and security vulnerabilities of IoT devices, including consideration of secure development, identity management, patching, and configuration management for covered devices.

Section 4. Security standards for use of covered devices by the Federal Government

Subsection (a)—Guidelines required

Subsection (a) requires the Director of NIST to submit to the Director of OMB guidelines on appropriate use and management of covered devices and minimum information security requirements for managing security vulnerabilities associated with connected devices not later than six months after the report required by section 3 is completed. When developing these guidelines, the Director shall consider best practices from the private sector, agencies, and public-private partnerships and ensure that guidelines are consistent with the report.

Subsection (b)—Promulgation of Standards

Subsection (b) requires the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security, to promulgate standards based on the guidelines submitted under subsection (a), except for devices considered national security systems as defined by section 3552 (b)(6) of title 44, United States Code. These standards

[9] Gartner, Inc., *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017) (online at www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016).

[10] *Congress Introduces Bill to Improve 'Internet of Things' Security,* C/Net (Mar. 11, 2019) (online at www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security/).

must be consistent with information security requirements under subchapter II of chapter 35 of title 44, United States Code.

The standards shall be reviewed at least once every five years and revised as appropriate. The Federal Acquisition Regulation shall be revised to implement any standard promulgated under subsection (b).

Section 5. Petition to exclude certain devices

Subsection (a)—Petition the director

Subsection (a) would require the Director of OMB to establish a process for interested parties to petition that a covered device not be considered a covered device for the purpose of standards promulgated under section 4(b).

Subsection (b)—Grants of petition

Subsection (b) requires the Director of OMB to grant petitions under subsection (a) on a limited basis, in a timely manner, and only if the interested party demonstrates that the procurement of such a covered device with limited data processing and software functionality would be unfeasible, or the procurement of a covered device that does not meet the standards promulgated by the Director of OMB is necessary for national security or for research purposes.

Subsection (c)—Report

Subsection (c) requires the Director of OMB shall submit a report to the appropriate congressional committee detailing the process established by the Director for granting or denying waivers under this section annually for five years. The reports shall include, at a minimum, an assessment of the waiver evaluation process, a description of the methods used in the waiver evaluation process, and a classified listing in the appendix with the types and number of devices for each agency granted a waiver and the reasons for such waiver.

Section 6. Coordinated Disclosure of Security Vulnerabilities Relating to Covered Devices

Subsection (a)—In general

Subsection (a) requires the Director of NIST, in consultation with the Director of Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, to develop and submit to the Director of OMB guidelines for reporting, coordinating, publishing, and receiving information about a security vulnerability in a covered device owned or controlled by an agency and the resolution of the vulnerability within 180 days of enactment. The subsection also requires such guidelines for contractors and subcontractors providing a covered device to the Federal Government on receiving information about a potential security vulnerability relating to the covered device and disseminating information about the resolution of a security vulnerability and on the type of information about security vulnerabilities that should be reported to the Federal Government, including examples.

Subsection (b)—Development of guidelines

Subsection (b) requires the Director of NIST to consult with cybersecurity researchers and private sector industry experts as appropriate, align the guidelines a closely as possible with Standards 29147 and 30111 of the International Standards Organization, and ensure consistency of guidelines with policies and procedures under section 2209 (m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

Subsection (c)—Promulgation of standards

Subsection (c) requires the Director of OMB, in consultation with the Administrator of General Services and the Secretary of Homeland Security, to promulgate standards based on the guidelines required by subsection (a). The standards shall extend to contracts for covered devices from contractors or subcontractors at any tier and be consistent with section 101 of the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act.

Section 7. Contractor compliance with standards and regulations

Subsection (a)—In general

Subsection (a) requires agency Chief Information Officers (CIOs) to determine that offerors of covered devices are in compliance with each standard promulgated under section 6(c) with respect to covered devices before awarding a contract. This requirement would apply to contracts below the simplified acquisition threshold. Agency heads would be prohibited from purchasing covered devices if the CIO has not issued a positive determination.

Subsection (b)—Waiver

Subsection (b) would allow the head of an agency to waive the prohibition under subsection (a) if the procurement of the covered device is necessary for national security or research purposes.

Subsection (c)—Effective date

The prohibition against non-compliant devices shall take effect one year after the Act is enacted.

Section 8. Institute report on cybersecurity considerations stemming from the convergence of information technology, Internet of Things, and operational technology devices, networks, and systems

Section 8 requires the Director of NIST to publish a report on the increasing convergence, including considerations for managing potential security vulnerabilities associated with such convergence, of traditional information technology devices, networks, and systems with covered devices, networks, and systems, and operational technology devices, networks, and systems within one year of enactment of the Act.

LEGISLATIVE HISTORY

On March 11, 2019, Representative Robin Kelly (D–IL) introduced H.R. 1668, the Internet of Things Cybersecurity Improve-

ment Act of 2019. The bill was referred to the Committee as well as the Committee on Science, Space, and Technology.

On June 12, 2019, the Committee considered H.R. 1668 at a business meeting with a quorum present. The Committee ordered the bill reported favorably, as amended, by voice vote.

COMMITTEE CONSIDERATION

On June 12, 2019, the Committee considered H.R. 1668 at a business meeting with a quorum present. Representative Robin Kelly (D–IL) offered an Amendment in the Nature of a Substitute (ANS), which passed by voice vote.[11]

EXPLANATION OF AMENDMENTS

During Committee consideration of the bill, Representative Robin Kelly (D–IL), offered an ANS. The Committee adopted the ANS by voice vote. The substance of the amendment is reflected in the Section-by Section analysis above.

LIST OF RELATED COMMITTEE HEARINGS

In accordance with section 103(i) of H. Res. 6, the Committee held a markup on June 12, 2019, to consider the proposals set forth in the Internet of Things Cybersecurity Act of 2019 and to examine the proposals in H.R. 1668 that were in the Committee's jurisdiction. Committee consideration extended from a hearing on the Cybersecurity of the Internet of Things before the Subcommittee on Information and Technology on October 3, 2017.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee finds that the security vulnerabilities of Internet of Things devices pose a significant threat to federal information security, such that the Committee recommends the adoption of this bill (H.R. 1668) to require vendor compliance with security standards prior to Federal Government procurement of an Internet of Things device.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goal or objective of this bill is to leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Section 102 (b)(3) of Public Law 104–1 requires a description of the application of this bill to the legislative branch when the bill relates to the terms and conditions of employment or access to public services and accommodations. This bill is to leverage Federal Government procurement power to encourage increased cybersecu-

[11] House Committee on Oversight and Reform, Business Meeting, Voice Vote on Adoption of a Substitute Amendment (June 12, 2019).

rity for Internet of Things devices, and for other purposes. As such, this bill does not relate to employment or access to public services and accommodations in the legislative branch.

DUPLICATION OF FEDERAL PROGRAMS

In accordance with clause 3(c)(5) of rule XIII, no provision of this bill establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

DISCLOSURE OF DIRECTED RULE MAKINGS

Within the meaning of section 551 of Title 5, United States Code, this bill requires the Federal Acquisition Regulation to be amended to implement the security standards and coordinated disclosure of vulnerabilities standards required by the bill.

FEDERAL ADVISORY COMMITTEE ACT STATEMENT

The legislation does not establish or authorize the establishment of an advisory committee within the definition of section 5(b) of the appendix to Title 5, United States Code.

UNFUNDED MANDATE REFORM ACT STATEMENT

Pursuant to section 423 of the Congressional Budget Act of 1974, the Committee has included a letter received from the Congressional Budget Office below.

EARMARK IDENTIFICATION

This bill does not include any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI of the House of Representatives.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(2)(B) of rule XIII of the Rules of the House of Representatives, the Committee includes below a cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974.

NEW BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the House of Representatives, the cost estimate prepared by the Congressional Budget Office and submitted pursuant to section 402 of the Congressional Budget Act of 1974 is as follows:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 13, 2019.

Hon. ELIJAH E. CUMMINGS,
Chairman, Committee on Oversight and Reform,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1668, the Internet of Things Cybersecurity Improvement Act of 2019.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is David Hughes.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 1668, Internet of Things Cybersecurity Improvement Act of 2019
As ordered reported by the House Committee on Oversight and Reform on June 12, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Deficit Effect	0	0	0
Spending Subject to Appropriation (Outlays)	0	35	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

Under H.R. 1668, the National Institute of Standards and Technology (NIST) would develop guidelines on the appropriate and secure use of Internet of things (IoT) devices by federal agencies and develop minimum information security requirements for agencies to manage security vulnerabilities for those devices.[1] In addition, the Office of Management and Budget (OMB) would promulgate standards for federal IoT devices that are consistent with NIST's standards and guidelines. OMB would review and revise those standards at least once every five years and develop waivers to exclude certain IoT devices from the new standards. OMB would report to the Congress annually from 2020 through 2025 on the effectiveness of the standards and on the types and number of excluded devices.

Under H.R. 1668, NIST also would publish standards for federal agencies, contractors, and vendors to systematically report and resolve security vulnerabilities for IoT devices. Each agency's chief information officer would be required to ensure compliance. OMB

[1] The IoT consists of devices connected one another and to a network for exchanging data without human interaction. See Suzy E. Park, *Internet of Things (IoT): An Introduction,* In Focus Report 11239 (Congressional Research Service, June 4, 2019), https://go.usa.gov/xVcdR.

would establish federal standards for that coordinated reporting process that are consistent with NIST's standards and guidelines.

Using information from NIST, CBO estimates that implementing the bill would cost $35 million over the 2019–2024 period, assuming appropriation of the necessary amounts.

The costs of the legislation (detailed in Table 1) fall within budget function 370 (commerce and housing credit).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 1668

	By fiscal year, millions of dollars—						
	2019	2020	2021	2022	2023	2024	2019–2024
Estimated Authorization	0	11	6	6	6	6	35
Estimated Outlays	0	11	6	6	6	6	35

In 2020, CBO estimates that NIST and OMB would spend a total of $11 million to develop the IoT guidelines and standards. Of that amount CBO estimates that NIST would spend a little more than $3 million to hire 11 employees and that OMB would spend about $350,000 to hire 2 employees. Those newly hired NIST staff would develop the new federal guidelines and provide technical assistance to federal agencies. In addition, CBO estimates that NIST would spend a little more than $3 million to hire contractors and convene workshops to assist with guideline development. Finally, CBO estimates that NIST would spend around $4 million to update their National Vulnerability Database (NVD) to account for the vulnerability of IoT data.

After 2020, CBO estimates that NIST and OMB would spend approximately $6 million annually to update the IoT guidelines and standards, report to Congress, and further update the NVD.

On September 13, 2019, CBO transmitted a cost estimate for S. 734, the Internet of Things Cybersecurity Improvement Act of 2019, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 19, 2019. H.R. 1668 and S. 734 are similar and CBO's cost estimates are the same for both pieces of legislation.

The CBO staff contact for this estimate is David Hughes. The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

ADDITIONAL VIEWS

Internet of Things (IoT) refers to the concept of connecting commercial products, appliances, or sensors to either the open internet or an organization's closed network information system. Generally, IoT devices have lower computing power and lack mature security architecture found in widely used general purpose computing devices and network infrastructure, such as personal laptops, tablets, and routers.

IoT adoption rapidly expands the size and complexity of networks. Network complexity leads to new cybersecurity complexities and associated vulnerabilities, which bad actors can exploit. Security limitations should be fully understood and accounted for before any IoT device is connected to an agency's network. IoT devices could pose real risks to federal systems if information security procedures are not effectively implemented and monitored.

However, H.R. 1668 does not adequately account for the federal government's existing security framework. As such, it is potentially redundant and may add unnecessary complexity or burdens to our federal security workforce. Principally, the Federal Information Security Modernization Act (FISMA) (44 U.S.C. § 3551) established a government-wide cybersecurity management framework.[1] Under the law, the Office of Management and Budget oversees agency information security policies and the Department of Homeland Security administers associated requirements,[2] which incorporate baseline information security standards maintained by the National Institute of Standards and Technology.[3] Agencies are required to implement these security protocols, and other additional protections as necessary, in the context of their own organizational risk management and operational needs.

Additionally, this bill seeks to "leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices" beyond federal government specific applications.[4] This is not an appropriate use of the government's established contracting procedures, which are designed to ensure the integrity of the federal acquisition process.

Finally, the private sector is incentivized to meet the needs of consumers and will respond as consumer demands arise. Private industry groups are actively working to address IoT security concerns through consensus-based standards.[5] Responding to existing

---

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, 128 Stat. 3073–3088 (2014).

[2] 44. U.S.C. § 3553.

[3] *Id.* See also, 40 U.S.C. § 11331.

[4] See H.R. 1668, 116th Cong. (2019) (preamble).

[5] Gary Shapiro and Jonathan Spalter, *The C2 Consensus on IoT Device Security Baseline Capabilities*, Council to Secure the Digital Economy: The Convene the Conveners Project (Sept. 17, 2019), https://www.tiaonline.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf See also, Chris Doman, et al., *Securing Edge Devices,* Cyber Threat Alliance

Continued

market incentives, companies offering IoT products are coordinating to develop best practices and ensure the networked interoperability of consumer products. At a minimum, H.R. 1668 could duplicate these private sector efforts.

JIM JORDAN.

○

(April 2019), https://www.cyberthreatalliance.org/wp-content/uploads/2019/04/CTA-Network-Edge-Joint-Analysis_Final.pdf.