Calendar No. 215

116TH CONGRESS *1st Session*	SENATE	REPORT 116–112

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 734

TO LEVERAGE FEDERAL GOVERNMENT PROCUREMENT POWER TO ENCOURAGE INCREASED CYBERSECURITY FOR INTERNET OF THINGS DEVICES, AND FOR OTHER PURPOSES

SEPTEMBER 23, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
MICHAEL J.R. FLYNN, *Senior Counsel*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
MICHELLE M. BENECKE, *Minority Senior Counsel*
JEFFREY D. ROTHBLUM, *Minority Fellow*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 215

116TH CONGRESS *1st Session* | SENATE | REPORT 116–112

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT

SEPTEMBER 23, 2019.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 734]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 734) 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 (in the nature of a substitute) and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of S. 734, the Internet of Things Cybersecurity Improvement Act of 2019, is to proactively mitigate the risks posed by inadequately-secured Internet of Things (IoT) devices through the establishment of minimum security standards for IoT devices purchased by the Federal Government. The bill codifies the ongoing work of the National Institute of Standards and Technology (NIST)

to develop standards and guidelines, including minimum-security requirements, for the use of IoT devices by Federal agencies. The bill also directs the Office of Management and Budget (OMB), in consultation with the Department of Homeland Security (DHS), to issue the necessary policies and principles to implement the NIST standards and guidelines on IoT security and management.

Additionally, the bill requires NIST, in consultation with cybersecurity researchers and industry experts, to publish guidelines for the reporting, coordinating, publishing, and receiving of information about Federal agencies' security vulnerabilities and the coordinate resolutions of the reported vulnerabilities. OMB will provide the policies and principles and DHS will develop and issue the procedures necessary to implement NIST's guidelines on coordinated vulnerability disclosure for Federal agencies. The bill includes a provision allowing Federal agency heads to waive the IoT use and management requirements issued by OMB for national security, functionality, alternative means, or economic reasons.

II. BACKGROUND AND THE NEED FOR LEGISLATION

More than eight billion IoT devices—devices that wirelessly connect to the internet and transmit data—are connected to our information systems and networks.[1] According to industry reports, the number of IoT devices will be as high as 50 billion by 2025.[2] This exponential increase of IoT devices introduces an unparalleled attack surface for hackers to exploit. According to industry experts, by 2020 approximately 25 percent of cyberattacks will target these devices.[3] This is because many IoT devices lack necessary safeguards, leaving the systems and networks they are connected to vulnerable to cyberattacks.[4] Peter Winston, Chief Executive Officer and Founder of Integrated Computer Solutions, commented on the need to ensure the security of IoT devices:

> Ultimately, security needs to be baked into every device at the operating system level. It shouldn't be up to an individual vendor at the application level. And the level of device security should match the audience. If you're selling your connected device to the [Central Intelligence Agency (CIA)]—if it has to work in a highly secure building, a place where a breach could be catastrophic—there's a different expectation than if you're selling a toy. Yes, they both require you to lock the doors and windows. But for the CIA, you also need to seal every crack and add multiple deadlocks to reinforced doors.[5]

The Committee recognizes the challenges Federal agencies face in leveraging limited resources and navigating a cumbersome Federal procurement process to acquire and securely modernize infor-

---

[1] Matt Toomey, *IoT Device Security Seriously-Neglected*, Aberdeen (Feb. 15, 2018), https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/.

[2] Mckinsey Global Institute, https://www.mckinsey.com/~/media/McKinsey/Business%20 Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20 value%20o%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

[3] Matt Toomey, *supra* note 1.

[4] *Id.*

[5] *Id.*

mation technologies.[6] Building upon recent Federal reports, the work of the Government Accountability Office (GAO), and congressional hearings, this legislation will ensure federal agencies are operating under policies and practices for IoT devices before they become prolific on federal networks.

The traditional challenges facing Federal information technology are exacerbated by the lack of widely adopted information security standards and best practices for IoT technologies.[7] In April 2018, the Committee held a hearing entitled, *Mitigating America's Cybersecurity Risks*, to discuss a range of Federal cybersecurity challenges, including the exponential growth of IoT devices in use on Federal networks.[8] Co-Director of the Harvard University Belfer Center for Science and International Affairs, Eric Rosenbach testified on the importance of "establish[ing] baseline security standards for the manufacturers and distributors of [IoT] devices."[9] While cautioning against a regulatory approach, Mr. Rosenbach supported the idea of using government procurement reform as a "good place to start" in advancing the secure procurement and use of IoT devices.[10]

Security baselines for IoT devices are necessary as designers and manufactures are not producing IoT devices with basic cybersecurity measures baked into their products. In May 2017, GAO published a technology assessment of IoT. The assessment found, among other things, "[widespread] concerns have been raised about the lack of security controls in many IoT devices, which is in part because many vehicles, equipment, and other increasingly IoT-enabled devices were built without anticipating threats associated with Internet connectivity or the requisite security controls." [11] The implications of these findings were illustrated by the 2016 Mirai botnet attack, which exploited basic vulnerabilities in IoT technology to compromise an estimated 493,000 devices.[12]

In May, 2019 the Secretaries of Commerce and Homeland Security published a report entitled, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*.[13] Among the findings of this report are that IoT devices need to be secure during all stages of the technology lifecycle and that market incentives are not aligned with the cybersecurity best practices.[14] In 2018, DHS Assistant Secretary for Cybersecurity and Communications, Janette Manfra, echoed this idea during testimony before the Committee by stating that the Federal Government needs a "higher level framework" led

---

[6] *Mitigating America's Cybersecurity Risks: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2018) (testimony of Jeanette Manfra, Assistant Secretary, Department of Homeland Security), *available at* https://www.hsgac.senate.gov/imo/media/doc/.

[7] *Id.; see also* U.S. Gov't Accountability Office, GAO–17–75, Technology Assessment: Internet of Things, Status and Implications of An Increasingly Connected World (May 2017), *available at* https://www.gao.gov/assets/690/684590.pdf.

[8] *Mitigating America's Cybersecurity Risks, supra* note 6.

[9] *Id.* (Testimony of Eric Rosenbach).

[10] *Id.*

[11] GAO–17–75 at 28, *supra* note 7.

[12] Joshua Abramson, *DDoS Attacks: Bigger, Stronger, Scarier*, SYMANTEC CORP. (Apr. 19, 2016), https://www.symantec.com/connect/blogs/ddos-attacks-bigger-stronger-scarier.

[13] Sec. of Commerce, Sec. of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. (May 22, 2018) *available at* https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[14] *Id.* at 8.

by OMB to manage cybersecurity risk related to IoT devices that includes basic authentication measures.[15]

As a result, IoT device security does not end with the design, manufacture, and procurement of the device; rather ongoing efforts are necessary to discover and remediate vulnerabilities that create the potential for exploitation by bad actors. The Federal Cybersecurity Risk Determination Report and Action Plan, published by OMB, found that "[a]n agency's ability to mitigate security vulnerabilities is a direct function of its ability to identify those vulnerabilities across the enterprise."[16] To affectively secure IoT devices in use on Federal networks, a comprehensive vulnerability disclosure program is an important step in identifying vulnerable IoT on a network.

The success of the "Hack the Pentagon" program led to the establishment of a formal Vulnerability Disclosure Policy (VDP),[17] as well as legislation codifying DHS authority to create a process to easily report and mitigate vulnerabilities.[18] Standards, policies, and practices for VDP of information technology, including IoT, consistent with the authorities and responsibilities established in the Federal Information Security Modernization Act of 2014 (FISMA14),[19] is a fundamental aspect of securing networked technologies over the course of their life-cycle.

Federal agencies can better ensure the security of their networks with IoT devices that have basic cybersecurity requirements engineered into the devices, and with IT systems that are maintained throughout their life-cycle in a secure fashion. S. 734 codifies the ongoing work of NIST, OMB, and DHS to improve the resilience of IoT devices and Federal networks through enterprise-wide policies and procedures to manage this rapidly expanding emerging technology. The legislation ensures that the technical guidance developed by NIST on the security of IoT devices, from procurement to use, is implemented in policy and practice across the Federal enterprise. NIST has already begun to develop standards and guidelines necessary to help "federal agencies and other organizations better understand and manage the cybersecurity and privacy risk associated with their IoT devices throughout the devices lifecycle."[20] Due to NIST's ongoing efforts to develop the information security standards and best practices for IoT management and use, this legislation did not further define the categories, computer functions, or types of devices covered under the term IoT to ensure NIST's work is not delayed.

III. LEGISLATIVE HISTORY

Senator Mark R. Warner (D–VA) introduced S. 734 on June 19, 2019, with Senator Cory Gardner (R–CO), Senator Margaret Wood Hassan (D–NH), and Senator Steve Daines (R–MT).

---

[15] *Mitigating America's Cybersecurity Risks, supra* note 6 (Testimony of Janette Manfra).

[16] Office of Management and Budget, Executive Office of the President, *Federal Cybersecurity Risk Determination Report and Action Plan*, 12 (2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

[17] *Id.*

[18] Pub. L. No. 115–390, Title I § 101, (H.R. 7327, the "SECURE" Technology Act).

[19] Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, 44 U.S.C. § 3553(a)(1).

[20] National Institute of Standards and Technology, NIST IR 8228, Considerations for Managing IoT Cybersecurity and Privacy Risks (June 2019).

The Committee considered S. 734 at a business meeting on June 19, 2019. During the business meeting, Chairman Ron Johnson offered a substitute amendment as modified that removed the definition of IoT and clarified DHS's role in the development of OMB's guidelines for IoT devices, and in leading the VDP. S. 734 was ordered reported favorably as amended by the Johnson Substitute Amendment as modified by voice vote *en bloc*. The Senators present for the voice vote were Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Sinema and Rosen.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section established that the bill may be cited as the "Internet of Things Cybersecurity Improvement Act of 2019" or the "IoT Cybersecurity Improvement Act of 2019."

Section 2. Definitions

This section includes definitions of the terms "Agency," "Director," "Information System," "Secretary," and "Security Vulnerability."

Section 3. National Institute of Standards and Technology considerations and recommendations regarding managing Internet of Things cybersecurity risks

Subsection (a) requires the Director of the NIST to develop, consistent with ongoing efforts, standards and guidelines for the Federal government on the appropriate use and management of Internet of things devices, including cybersecurity risks.

Subsection (b) requires the Director of NIST to brief appropriate committees of Congress on the increasing convergence of traditional information technology devices, networks, and systems.

Section 4. Policies and principles for Federal agencies on use and management of Internet of Things devices

Subsection (a) requires the Director of OMB, in consultation with the Secretary of Homeland Security, to issue policies and principles consistent on the use of IoT devices based on the standards and guidelines developed under section 3(a).

Subsection (b) requires that the policies and guidelines developed by OMB for IoT devices is consistent with the Federal Information Security Management Act, as found in subchapter II of chapter 35 of title 44, of United States Code.

Subsection (c) requires the Director of OMB and Secretary of Homeland Security to regularly review the policies and principles for the use and management of IoT devices.

Section 5. Guidelines on coordinated disclosure of security vulnerabilities relating to information systems, including Internet of Things devices

Subsection (a) requires the Director of NIST, in consultation with cybersecurity researchers and private-sector industry experts, to establish guidelines for reporting, coordinating, publishing, and re-

ceiving of information about and the resolution of security vulnerabilities related to agency information systems.

Subsection (b) lays out the elements of the coordinated vulnerability disclosure guidelines. The guidelines shall be consistent with industry best practices and Standards 29147 and 30111 of the International Standards Organization; and shall incorporate vulnerability information on IoT devices and how to disseminate information on the resolution of security or personal information vulnerabilities on agency information systems.

Subsection (c) requires the Director of OMB and Secretary of Homeland Security to regularly review the policies and principles for the use and management of IoT devices.

Subsection (d) required the Director of OMB to provide oversight and implement the guidelines laid out in section 5 subsection (a) of this bill.

Subsection (e) requires that the Secretary of DHS provide technical and operational assistance to implement section 5 subsection (a) of this bill.

Section 6. Implementation of coordinated disclosure of security vulnerabilities relating to agency information systems, including Internet of Things devices

Subsection (a) requires that, once the Director of NIST publishes guidelines required under section 5(a), within 180 days, the Director of OMB should publish policies on vulnerabilities regarding information systems and IoT devices.

Subsection (b) establishes procedures whereby the Secretary of DHS and Director of OMB develop procedures for each Federal agency to publish and receive information on vulnerabilities regarding information systems and IoT devices.

Subsection (c) creates a limitation to subsection (b) that prohibits agencies to use or acquire IoT devices from contractors if the contractors fail to comply with section 5(a).

Subsection (d) requires the Secretary of DHS to ensure that procedures outlined by subsection (b) are consistent with NIST standards.

Section 7. Waiver

This section allows the head of an agency to use an IoT device without regard to any policy under several requirements. The requirements include that the IoT device is necessary for research or national security, appropriate to the function of a device, secured, and of a greater quality or of a lesser cost than one that already meets guidelines.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform bill (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

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

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 734, 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.

S. 734, 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

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 S. 734, 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. 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 S. 734, 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 to 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 S. 734

	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 H.R. 1668, the Internet of Things Cybersecurity Improvement Act of 2019, as ordered reported by the House Committee on Oversight and Reform on June 12, 2019. S. 734 and H.R. 1668 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.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

Because this legislation would not repeal or amend any provision of current law, it would not make changes in existing law within the meaning of clauses (a) and (b) of paragraph 12 of rule XXVI of the Standing Rules of the Senate.

○