The Heritage Foundation

ISSUE BRIEF

No. 4762 | SEPTEMBER 13, 2017

Greater Oversight Needed for the Federal Government's Use of the "Internet of Things"

Riley Walters

The interconnection of devices, known as the Internet of Things (IoT), promises greater efficiency in analysis, communication, and data between activities in the cyber and physical worlds. Up to 20 billion devices or "things" could be online by 2020.[1]

As consumers of technologies in the IoT, state, local, and the federal governments will benefit from the IoT's expansion and efficiency, just as it did with the introduction of other technologies such as the Internet itself or mobile phones. For example, IoT can make federal buildings more secure, allow public-sector works to more easily prepare for an approaching natural disaster, or aid public utilities to monitor the structure and integrity of pipes and cables.

The private sector is the leading creator of IoT technologies. As a consumer of IoT, the government should be allowed to demand from its vendors increased security and services for its devices. Increased demand in security by government purchasers may also increase the security standards for IoT devices purchased by private individuals. However, the two markets should not be confused: Separate markets for expensive, secure devices and for cheaper, less-secure devices will continue to coexist.

The IoT Cybersecurity Improvement Act of 2017

The U.S. government is a consumer of IoT like any other private individual or organization, purchasing goods from producers and suppliers in the IoT market. The U.S. government has an obligation to maintain its own information resiliency in the face of emerging cybersecurity threats. While utilizing IoT can be beneficial, the interconnecting of devices can allow bad actors to spread throughout networked systems further and faster.

The IoT Cybersecurity Improvement Act of 2017 (S. 1691), recently introduced by Senator Mark Warner (D-VA), demands higher security standards for IoT goods purchased by federal agencies.[2] IoT vendors would be required to provide certification for the following:

- Devices are free of any known vulnerabilities;
- Security updates can be provided to the devices throughout their service;
- Devices exclude any remote accessibility; and
- Devices use up-to-date industry standards for functions such as encryption, communications, and interconnection with other devices.

S. 1691 requires the Director of the Office of Management and Budget (OMB) to coordinate the efforts of the Secretary of Defense, Administrator of General Services, Secretary of Commerce, Secretary of Homeland Security, and other intelligence or national security agencies, and issue IoT purchas-

This paper, in its entirety, can be found at
http://report.heritage.org/ib4762

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

ing guidelines of each agency. However, agencies may be able to request a waiver to these higher-standard IoT devices from the Director of the OMB if such purchases are considered "unfeasible or economically impractical."[3] While agencies may demand increased security, the increase in costs may not be feasible for their limited budgets. Agencies may then be required to pursue alternative means for device security.[4]

Some exemptions may exist for vendors, along with the requirements for increased standards in devices purchased by federal agencies. Vendors can be granted a waiver if they are able to identify and justify a security flaw as well as prescribe mitigation actions. Vendors may also be able to use third-party security standards if they can demonstrate that those standards provide an equivalent or greater level of security than those prescribed in S. 1691.

S. 1691 also includes an amendment to the Computer Fraud and Abuse Act (CFAA) and Digital Millennium Copyright Act to limit criminal penalties against white hat researchers who, "in good faith," are testing the cybersecurity of the device being sold to the government.[5] Vendors would be required to notify agencies if these third-party researchers ever find security flaws.

However, clarification may be needed on what constitutes a "device." S. 1691 broadly defines IoT devices as Internet-connected devices that would include not just wearable or portable devices but desktop and laptop computers—potentially affecting an exponential number of vendors.[6]

IoT Risks at the Department of Defense

In July 2017, the Government Accountability Office (GAO) released a report highlighting the risks IoT can pose for the Department of Defense (DOD).[7] The GAO found that risks exist not just within the IoT devices themselves but also in how the IoT devices are used. To illustrate, the GAO gives an example of a smart television located in an unsecure area that is still able to pick up on conversations which may contain relatively sensitive information.

Furthermore, a 2016 GAO report highlighted that there is a lack of security standards that address unique IoT needs as well as a lack of incentives for vendors to develop more secure devices. The GAO determined that IoT securities vulnerabilities could potentially affect DOD hospitals and fuel systems. The DOD has previously identified similar security risks from IoT devices to include supply chain threats, upgrade deficiencies, risks from an increased number of Internet-connected devices, and risk of unauthorized communication with IoT devices. The DOD also has made progress by assessing IoT risks to critical infrastructure and establishing research programs aimed to mitigate IoT risks.

The GAO's July 2017 report highlights that the DOD's policies and guidance regarding IoT neither addresses clearly some IoT risks nor offers guidance to mitigate those risks. The DOD itself would have to modify existing and future contracts with vendors to include higher security standards for IoT devices, as well as include in their core security policies clear guidance on IoT and IoT devices.

Emerging Threats

High-profile IoT cyber incidents occurring over the past year have further highlighted the risk that IoT can pose for the U.S.[8] To facilitate the federal government's awareness of IoT risk and having the tools to manage it, lawmakers should:

[1] News release, "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent from 2016," Gartner Newsroom, February 7, 2017, http://www.gartner.com/newsroom/id/3598917 (accessed September 12, 2017).

[2] Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S.1691, 115th Cong., 1st Sess., https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?q=%7B"search"%3A%5B"iot"%5D%7D&r=1 (accessed September 12, 2017).

[3] Ibid.

[4] Additional security may include network segmentations, system-level security controls, multi-factor authentication, or intelligent network solutions.

[5] Internet of Things (IoT) Cybersecurity Improvement Act of 2017.

[6] There are two leading definitions of what is considered part of the Internet of Things: (1) "things" that are connected and transmit data, such as a wearable device like a Fitbit; (2) devices that are connected to the "Internet" via an Internet Protocol (IP) address.

[7] U.S. Government Accountability Office, *INTERNET OF THINGS: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, July 2017, http://www.gao.gov/assets/690/686296.pdf (accessed September 12, 2017).

[8] Riley Walters, "The U.S. Continues to Face Cyber Threats in 2016," Heritage Foundation *Issue Brief* No. 4641, December 19, 2016, http://www.heritage.org/defense/report/the-us-continues-face-cyber-threats-2016.

- **Establish a government-wide definition for IoT devices.** To bridge the gap between policymakers, agencies, and other intergovernmental bodies, a common definition of what constitutes as IoT is needed. Lawmakers could consider the Defense Intelligence Agencies' definition of a portable electronic device, S. 1691's definition of an Internet-connected device, the DOD and the Institute of Electrical and Electronics Engineer's definition of (semi)autonomous devices that can connect to the Internet, or the Department of Homeland Security's definition of systems and devices with mostly physical purposes connecting with information networks.[9]

- **Require higher standards in federal purchases of IoT devices.** The federal government should maintain high standards when it comes to IoT purchases, lest it increase the risk of cybersecurity or espionage incidents. High standards may incentivize increase in IoT security standards for devices sold to the general public, thereby increasing overall IoT security. But legislative action may not be required. Either through executive order or by the Director of OMB, OMB can require that IoT devices purchased by federal agencies meet higher security standards.

- **Enhance third-party security tests.** The CFAA should be updated to allow for private security defenders to test networked systems.[10] S. 1691 would only scratch the surface of what is needed to enable responsible active cyber defense.

- **Recognize dual markets.** Different markets for IoT devices will always exist. This includes more expensive devices with higher security standards or less expensive devices with lower security standards. Consumers may be willing to exchange security for savings. The government should acknowledge and accept consumer choice.

The Right Balance of Risk and Demand

The Internet of Things and other emerging technologies will be beneficial for American consumers, even as they give rise to presently unforeseeable threats. Even as the government encourages and embraces new technologies, it also needs a holistic understanding of the IoT. The government should be a smart consumer and buy products that meet its security needs, while also allowing private individuals to take a greater role in securing their own devices.

*—**Riley Walters** is a Research Associate in the Asian Studies Center, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

[9] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)," November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (accessed September 12, 2017).

[10] Paul Rosenzweig, Steven Bucci, and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense," Heritage Foundation *Backgrounder* No. 3188, May 5, 2017, http://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense.