Internet of Things
Cybersecurity Improvement Act of 2017

Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines

FACT SHEET:

While 'Internet of Things' (IoT) devices and the data they transmit present enormous benefits to consumers, the relative insecurity of many devices presents enormous challenges. Thus far, there has been a significant market failure in the security of these devices.

Sometimes shipped with factory-set, hard-coded passwords and oftentimes unable to be updated or patched, IoT devices can represent a weak point in a network's security, leaving the rest of the network vulnerable to attack. Additionally, the sheer number of IoT devices – expected to exceed 20 billion devices by 2020 – has enabled bad actors to launch devastating Distributed Denial of Service (DDoS) attacks. **This legislation is aimed at addressing the market failure by establishing minimum security requirements for federal procurements of connected devices.**

The legislation requires vendor commitments:

- That their IoT devices are patchable.
- That the devices don't contain known vulnerabilities.
  - If a vendor identifies vulnerabilities, it must disclose them to an agency, with an explanation of why the device can be considered secure notwithstanding the vulnerability and a description of any compensating controls employed to limit the exploitability/impact of the vulnerability.
  - Based on this information, an agency CIO could issue a waiver to purchase the device.
- That the devices rely on standard protocols.
  - Outside experts emphasize the importance of having the vendor disclose what network protocols are in use, for instance to assist Department of Homeland Security (DHS)'s Einstein program.
- That the devices don't contain hard-coded passwords.

Recognizing that it may be infeasible for certain devices to meet those requirements, and in consideration of network-based technologies that can help manage risks from insecure devices:

- Agencies may ask the Office of Management and Budget (OMB) for permission to purchase non-compliant devices if they can demonstrate that certain compensating controls have been employed.
- The legislation empowers OMB, working with National Institute of Standards and Technology (NIST) and industry, to specify particular measures (such as network segmentation, use of gateways, utilization of operating system containers and micro-services) for agencies to employ.

While the legislation establishes modest new device security requirements, it offers flexibility to agencies to waive these requirements in the event that:

- Agencies employ their own equivalent, or more rigorous, device security requirements; or
- Industry develops third-party device certification standards that provide equivalent, or more rigorous, device security requirements (as determined by NIST).

The legislation directs the DHS National Protection and Programs Directorate (NPPD) to:

- Work with industry to develop coordinated disclosure guidelines for vendors selling IoT to the US government, which vendors would then adopt, allowing researchers to uncover vulnerabilities in those products and responsibly share them with the vendor, without fear of liability under the Digital Millennium Copyright Act (DMCA) or Computer Fraud and Abuse Act (CFAA).
  - Vulnerabilities found and reported to vendors must be patched (or devices must be replaced) in a timely manner.

The legislation requires that agencies maintain an inventory of IoT devices in use.

- Requires OMB to submit a report to Congress after 5 years on effectiveness of guidelines and any recommendations for updates.

The legislation allows OMB to waive, in whole or in part, any of the requirements after 5 years.

WHAT THE EXPERTS ARE SAYING:

Jonathan Zittrain, Co-Founder of Harvard University's Berkman Klein Center for Internet & Society

"Internet-aware devices raise deep and novel security issues, with problems that could arise months or years after purchase, or spill over to people who aren't the purchasers. This bill deftly uses the power of the Federal procurement market, rather than direct regulation, to encourage Internet-aware device makers to employ some basic security measures in their products. This will help everyone in the marketplace, including non-governmental purchasers and the vendors themselves, since they'll be encouraged together to take steps to secure their products."

Denelle Dixon, Chief Business and Legal Officer, Mozilla

"This bill makes important strides in refocusing attention on how to secure the government's systems and networks. Not only would reforms like these help safeguard the vast amounts of personal and sensitive information that the government holds, but would also help to secure the products that people use every day, and protect the researchers working to help secure those products."

Bruce Schneier, Fellow and Lecturer at Harvard Kennedy School of Government

"The proliferation of insecure Internet-connected devices presents an enormous security challenge. The risks are no longer solely about data; they affect flesh and steel. The market is not going to provide security on its own, because there is no incentive for buyers or sellers to act in anything but their self-interests. I applaud Senator Warner and his cosponsors for nudging the market in the right direction by establishing thorough, yet flexible, security requirements for connected devices purchased by the government. Additionally, I appreciate Senator Warner's recognition of the critical role played by security researchers and the exemptions included in this legislation for good-faith security research."

Jeff Greene, Senior Director of Global Government Affairs and Policy, Symantec

"The Mirai botnet was a wake-up call, a stark demonstration of the risk created by unsecured IoT devices. It does not have to be this way – IoT devices can be secured. We applaud Senators Warner and Gardner for taking action to address this threat and to improve the Federal government's IoT security. We look forward to working with them as their legislation moves forward."

Michelle Richardson, Deputy Director of the Freedom, Security and Technology Project, Center for Democracy and Technology

"We urgently need to start securing the Internet of Things, and starting with the government's own devices is an important first step. This legislation will push government devices to meet modern security standards, and ensure that researchers who act in good faith can independently verify the security of those devices. We hope that Congress will consider this proposal soon, and look forward to a discussion about the security of government systems, where the market for Internet of Things devices is headed, and how independent research can contribute."

Austin Carson, Executive Director of TechFreedom

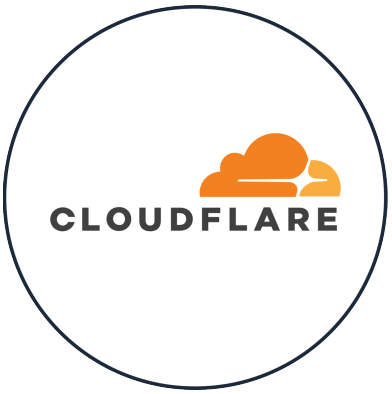
"The IoT Cybersecurity Improvement Act presents a reasonable mechanism to help prevent catastrophic attacks involving federal connected devices and encourage better security throughout the ecosystem. The bill recognizes the need to let the broader market continue to evolve while establishing a baseline for federal devices to avoid known threats. It also wisely pursues a mature framework for independent research and disclosure. I applaud Senators Gardner and Warner on an astute, good-faith effort and look forward to working with them to refine it as the bill moves through the process."

Ray O'Farrell, Executive Vice President and Chief Technology Officer, VMware

"VMware commends the bipartisan leadership of Senator Mark Warner and Senator Cory Gardner in introducing IoT security legislation. The bill includes reasonable security recommendations for the federal government to consider when purchasing IoT-related and edge computing devices. This legislation is an important, bipartisan step forward in promoting a secure federal IoT ecosystem."

Rodney Joffe, Senior Vice President and National Security Executive, Neustar

"Neustar commends Senator Warner for his continued leadership in cybersecurity. The bill he is introducing today correctly identifies the need to secure IoT devices which are not only being increasingly used to provide critical functionality for people and infrastructure but are also being used by criminals in major cyberattacks. Senator Warner's bill provides an important first step in addressing a very real and growing cyber threat. "



Doug Kramer, General Counsel, Cloudflare Inc.

"Cloudflare applauds Senator Warner for his efforts to encourage security research and to use the government procurement process to make the U.S. Government a leader in addressing the risks posed by improperly secured IoT devices. The worldwide internet outages caused last year by devices infected with the Mirai malware highlighted the need for more robust discussions about securing IoT devices. This bill should open an important dialogue on those issues, and Cloudflare looks forward to continuing to work with Senator Warner as the bill moves forward."

Josh Corman, Director of Cyber Statecraft Initiative, Atlantic Council and Founder of I Am The Cavalry

"Our dependence on connected technology is growing faster than our ability to secure it. Mirai showed us that low cost, low hygiene IoT can collectively do significant damage to the Internet and commerce. WannaCry and other attacks are now affecting patient care, industrial systems, and critical infrastructure. Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security. Poor cyber hygiene represents a public health issue - and even threat to human life. It is encouraging to see what the federal government can do to raise the bar (both for their use and the marketplace). We know other countries and private sectors initiatives are waking up to the need to preserve the promise and benefits of the technologies upon which we're increasingly dependent."

Ryan Hagemann, Director of Technology Policy, Niskanen Center

Although still in its infant stages, the emerging Internet of Things is an industry that is starting to make big economic splashes. Unfortunately, there is a great deal of public skepticism associated with IoT device security. That needs to change, and the IoT Cybersecurity Improvement Act of 2017 is an important step forward in helping to remedy those concerns. By establishing clear guidelines for contractors and vendors, the government can become a leader in showcasing the many benefits these technologies have to offer. Additionally, the Niskanen Center is heartened to see Sens. Gardner and Warner have taken steps to limit liability for researchers engaged in good faith systems penetration testing of IoT devices. By ensuring the provisions of the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act do not unduly burden those individuals seeking to make devices more secure, this bill sets the foundation for future innovations that will help build stronger, more secure IoT systems. We applaud the effort that has gone into this bill, and believe it should move forward with all due haste."