wiley

NEWSLETTER

Draft IoT Legislation Increases Obligations on Contractors and Promotes Vulnerability Disclosure

September 2017

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, introduced August 1, 2017, by U.S. Senators Mark Warner (D-VA), Cory Gardner (R-CO), Ron Wyden (D-OR), and Steve Daines (R-MT), seeks to improve the security of IoT devices by establishing requirements for IoT devices procured by the federal government. Several third-parties contributed to it, including think tanks and security vendors. It does not appear that the private-sector suppliers of IoT devices or network operators were involved in the drafting.

If enacted, the law would have significant impacts. Among other things, it would require companies selling connected products to the government to make commitments about security and expand support. Certifications about security could open the door to additional liability for contractors under the False Claims Act. And the law would encourage more research and "hacking" of products provided to the government, increasing burdens on the private sector when dealing with the federal government and depriving them of choice in whether and how to manage vulnerability disclosure.

The law would create new contractor responsibilities with respect to Internet-connected device security. The legislation directs the Office of Management and Budget (OMB) to create guidance to federal agencies to include contract provisions for the acquisition of Internet-connected devices. All contracts for the acquisition of Internet-connected devices (devices) will include a clause requiring the contractor to certify that the devices do not contain, at the time of proposal, any known "security vulnerabilities" in any hardware, software, or firmware component. The clause will also require the

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Internet of Things
Privacy, Cyber & Data Governance

contractor to certify that the device relies on components capable of accepting properly authenticated and trusted updates from the vendor, and uses only "non-deprecated industry-standard protocols and technologies" for functions such as communications, encryption, and interconnection with other devices or peripherals. Finally, the clause requires the contractor to certify that the device does not include any fixed or hard-coded credentials or passwords used for remote administration, delivery of updates, or communication.

All contracts for IoT devices will also include clauses requiring the contractor to: (1) notify the purchasing agency of any known security vulnerabilities or defects subsequently disclosed to it or otherwise learned, for the duration of the contract; (2) update or replace any software or firmware; (3) timely repair any new security vulnerability, or replace, if an update does not remedy the issue; (4) provide the purchasing agency with general information on the device to be updated, relating to the anticipated support and manner in which the device receives updates.

The law would create guidelines for each agency to impose coordinated disclosure requirements on contractors providing Internet-connected devices. The U.S. Department of Homeland Security is to issue guidelines for coordinated vulnerability disclosure requirements for federal contractors supplying IoT devices to the government. These guidelines include policies and procedures for conducting research on the cybersecurity and potential vulnerability of a device. The law would also amend the Computer Fraud and Abuse Act (CFAA) and Digital Millennium Copyright Act (DMCA) to limit liability for those in "good faith" engaging in researching the cybersecurity of a type of device provided by a contractor to the government, and acting in compliance with the National Protection and Programs Directorate's promulgated guidelines. To facilitate this research and disclosure, the law would require OMB to establish, maintain, and update a public database of devices and manufacturers (1) for which limitations of liability exist under the Act, and (2) about which the government has received formal notification of security support ending.

As we have noted elsewhere, vulnerability disclosure programs can be complex and require careful consideration and resources to properly execute. *See* Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel, *CircleID* (Feb. 10, 2017). There, Megan Brown and Matthew Gardner explain that not every company can handle one. It should be a company's choice whether to have one and whether to waive their rights under the CFAA and DMCA. Finally, it is not necessarily the best approach to address vulnerabilities in devices used by the federal government.