wiley

NEWSLETTER

Congress Looks to Government Contractors to Fix IoT Cybersecurity, Raising Concerns

November 2017

Government Contracts Issue Update

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S.1691, introduced August 1, 2017, by Sens. 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. Members of the house are working on a companion bill to S. 1691. Several congressional hearings have been held about IoT security, and efforts are underway throughout the executive branch. The private sector is likewise addressing IoT security, as explained in a recent paper by the U.S. Chamber of Commerce.

The proposed law is designed to combat poor cybersecurity in IoT devices sold to the Government; however, securing surveillance cameras, traffic lights, autonomous cars, and similar remote sensors is not the end goal. Rather, drafters of the proposed law hope to prevent Distributed Denial of Service (DDoS) attacks that capitalize on the poor cybersecurity of some IoT devices and jeopardize life on the Internet.

The law, if enacted, would have significant impacts for contractors. Among other things, it would require companies selling connected products to the Government to make commitments about product security and expand support. The certifications about security could open the door to contractual and enforcement liability for noncompliance. The law would encourage more research and "hacking" of products provided to the Government, increasing burdens on those dealing with the federal government and depriving them of choice in whether and how to manage vulnerability

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contracts
Privacy, Cyber & Data Governance

disclosure.

As the Government looks at how to manage an increasingly dynamic technology landscape, those selling connected products to the Government should watch this and related developments.

Background on IoT Cybersecurity

Vulnerabilities in IoT devices are attracting increased attention as the number of IoT devices in use has expanded exponentially. The emerging consensus among security experts both in the private sector and Government is that IoT cybersecurity is often poor and presents a growing threat.

IoT devices are often built to be plugged in and forgotten about, and security is not given much (if any) attention. The security shortcomings are attributable to a number of factors unique to IoT products. IoT devices often have rudimentary operating systems, making advanced security features difficult to implement. Many devices are not protected by a firewall or router and are connected directly to the Internet. These devices are generally not patched or updated. Perhaps most alarming, many devices are shipped with default usernames and passwords built into the firmware, like “root” and “admin” or “test” and “1234.”

This combination of default passwords, direct internet connections, and limited security precautions, makes IoT devices vulnerable. Hackers are able to scan random IP addresses for open connections and attempt a brute-force login with commonly-used or known default credentials. This method of attack is easy and effective.

DDoS Attack on October 21, 2016

The proposed law is designed to help prevent the use of highly-vulnerable IoT devices to conduct large-scale DDoS attacks that are capable of shutting down portions of the Internet, like a significant and widespread DDoS attack on October 21, 2016. In general, DDoS attacks work by overwhelming a target with very high levels of traffic, causing the target to no longer respond to legitimate internet traffic. DDoS attacks are “distributed” because the attacker utilizes numerous IP addresses to launch the attack. Hackers often gain the needed computing power and diverse IP addresses needed to mount these attacks by hacking into numerous computers and forcing them to work in coordination. The hacked computers are referred to as a botnet. Because the attack comes from the large number of IP addresses that belong to the computers in the botnet, preventing a successful DDoS attack is not just a matter of denying internet traffic from a single malicious IP address.

The attack on October 21st followed this basic pattern. Unlike previous attacks, however, that DDoS attack utilized thousands of infected IoT devices, like video cameras with fixed administrator credentials, to create a massive botnet army. As a result, the attack was highly distributed and powerful, even compared to traditional DDoS attacks. The attack was focused on Dyn, a domain name server (DNS) lookup company that routes internet traffic and traditionally had very strong defenses. However, using the IoT devices, the botnet overwhelmed Dyn, which had a secondary effect of taking offline hundreds of websites, like Amazon, Etsy, and Twitter, that relied on Dyn. Security researchers fear that future DDoS attacks based on botnet armies of IoT devices could be powerful enough to constitute a significant threat to the Internet.

The Requirements Under the Proposed Law

To prevent future DDoS attacks that threaten the Internet, the proposed law aims to improve the cybersecurity of IoT devices sold to the Government, with the goal of reducing the threat of these devastating DDoS attacks. This may not come to fruition given the relatively small market share federal procurement has in the global market for connected devices. Nevertheless, putting aside efficacy of the legislation, there are some areas of practical concern as well.

For example, the proposed law would require contractors to make several certifications with respect to IoT devices, such as:

- The devices do not contain, at the time of proposal, any known "security vulnerabilities" in any hardware, software, or firmware component;
- The devices rely on components capable of accepting properly authenticated and trusted updates from the vendor;
- The devices use only "non-deprecated industry-standard protocols and technologies" for functions such as communications, encryption, and interconnection with other device or peripherals; and
- The devices do not include any fixed or hard-coded credentials or passwords used for remote administration, delivery of updates, or communication.

In addition, under the proposed law, companies that sell IoT devices to the Government will be required to create vulnerability disclosure programs. According to the proposed law, among other things, these programs will require the contractor to:

- Notify the purchasing agency of any known security vulnerabilities or defects subsequently disclosed to it or otherwise learned, for the duration of the contract;
- Update or replace any software or firmware;
- Timely repair any new security vulnerability, or replace the device, if an update does not remedy the issue; and
- 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.

Are Burdens on Contractors the Right Remedy?

The certifications under the proposed law are designed to discourage the sale or use of IoT devices that can be easily hacked and used as part of a botnet army. Certainly, some changes may be relatively easy to implement. For example, eliminating fixed passwords like "1234" from the firmware of IoT devices would be a step in the right direction.

Nonetheless, the certifications appear likely to create compliance challenges for well-meaning contractors. There is ambiguity inherent in reporting known vulnerabilities and using industry standard protocols in a field as rapidly evolving as cybersecurity. Moreover, verifying, testing, and patching vulnerabilities is not always an easy process, putting contractors in a difficult position when the answer is more complex than a simple fix. Individuals who report vulnerabilities have mixed motives, and it is difficult for a company to quickly ascertain whether they are working with a genuine "white-hat" hacker with a legitimate bug or someone with a more nefarious agenda. It may be premature for the Government to mandate the use and particular design of vulnerability disclosure programs which are relatively new and with which the Government itself has little experience.

Correctly describing these inherently ambiguous situations to the Government will take on extra importance after the Supreme Court's decision in *Universal Health Services Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016), which held that contractors may be liable under the False Claims Act for "misleading half-truths" in certain situations. A good faith judgment call on reporting an uncertain vulnerability might look different when re-contextualized in the aftermath of a cyber incident.

Moreover, the scope of the bill is limited to government contractors. Even if government contractors are fully compliant and implement robust cybersecurity for IoT devices, will that eliminate the threat from DDoS attacks? That is unlikely. For example, it appears that video cameras sold by large Chinese electronics companies were a significant part of the botnet that was used in the DDoS attack in October 2016. The proposed bill would do nothing to directly change the behavior of the many companies selling IoT devices in the commercial market. As long as IoT devices with weak cybersecurity remain on the market, the possibility remains that hackers can exploit those devices to create DDoS attacks. This is why the ecosystem is taking layered steps to mitigate risks by, for example, filtering traffic and using third party security services to respond to DDoS attacks.

Other aspects of the draft legislation deserve careful consideration. Codifying technical definitions in the United States Code can make it hard to keep up with changing technology. Obsolescence is particularly a concern where those definitions will shape contract clauses that may linger for decades before the next revision. The legislation also calls for public lists of devices for which security support may have ceased and for which researchers have immunity to conduct research. This may worsen the security posture of federal networks.

Conclusion

Companies that make IoT devices for the Government should pay careful attention to this bipartisan legislation as it advances. The legislation has been hailed as a step in the right direction, but its complexity and unintended consequences should make technology companies think twice. While the threat posed by poor cybersecurity in IoT devices is daunting, it is not obvious that the proposed law would make material progress towards a solution.