THE
NATIONAL LAW REVIEW

Feds Want New IoT Guidance to Address Security Vulnerabilities

Article By Elfin L. Noce
Townsend L. Bourne
Sheppard, Mullin, Richter & Hampton LLP
Eye On Privacy

Communications, Media & Internet
Administrative & Regulatory
All Federal

Thursday, May 23, 2019

“Internet of Things” devices are listening. And now the federal government is taking notice. As we reported in our Government Contracts and Investigations blog, to date, federal cybersecurity regulations for government contractors focus on implementing safeguards to protect sensitive government data. A gap has emerged where the federal government purchases IoT devices. Those devices collect and send data online, and are thus are susceptible to hacking and listening in. Proposed legislation recently introduced in both the Senate (S.734) and the House (H.R. 1668) calls for new information security standards to manage these cybersecurity risks. This legislation would affect a wide range of IoT devices. I.e., a device connect to the internet that is not a “general purpose computing device.”

This legislation calls on the National Institute of Standards and Technology to take several actions. First is to review how companies can manage IoT cybersecurity risks. The review should be done by September 30, 2019 and cover, at a minimum several key elements. These include identity management and patching. They also include secure development and configuration management. Second, the legislation calls on NIST to recommend minimum information security requirements for managing IoT cybersecurity risks. The deadline under the legislation for this is March 31, 2020. Third, the new legislation calls on NIST to publish guidance relating to sharing security vulnerabilities relating to devices used by the federal government. As part of this is sharing potential fixes to those security vulnerabilities.

While not directly related to the proposed legislation, NIST has published a preliminary draft practice guide on *Securing Small Business and Home Internet of Things Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description*. The comment period for this draft guide ends June 24, 2019.

Putting it Into Practice: While still in the early stages, if the legislation passes, agencies will eventually be prohibited from acquiring or using devices from any contractor or vendor that does not have appropriate safeguards in place. This will likely impact all companies that make IoT devices. The impact will either be direct, where an organization provides these devices to the federal government. Or, it may be indirect, where an organization may use the NIST standards as a baseline for the security of its devices.

Source URL: https://www.natlawreview.com/article/feds-want-new-iot-guidance-to-address-security-vulnerabilities