ML STRATEGIES

Senate Passes IoT Cybersecurity Bill by Unanimous Consent

November 18, 2020 | | By **Christian Tamotsu Fjeld**

Last night, the Senate passed by unanimous consent **H.R. 1668, the Internet of Things (IoT) Cybersecurity Improvement Act**. The House had previously passed the bill by voice vote in September after lengthy negotiations with the Senate to resolve differences between their respective bills. The bill now heads to the President's desk for his signature.

The IoT Cybersecurity Improvement Act directs the National Institute of Standards and Technology (NIST) to develop standards and guidelines on how federal government agencies should appropriately use and manage IoT devices connected to information systems. In so doing, the bill directs NIST to develop "minimum information security requirements for managing cybersecurity risks associated with such devices" and further requires NIST to take into account current standards and best practices in the marketplace. Moreover, the bill requires NIST to develop guidelines on how federal agencies should manage and resolve cybersecurity vulnerabilities in their IoT devices, as well as how contractors and subcontractors receive and disseminate information about such vulnerabilities. The Office of Management and Budget (OMB) is tasked with implementing NIST's guidelines throughout the federal government, except for national security systems.

The scope and effect of the bill remains to be seen. The final version of the bill struck the definition of IoT devices under section 3 and instead placed guidance on that term in section 2, which is the bill's Sense of Congress. This will likely have the effect of providing NIST with greater discretion in determining the scope of the bill, *i.e.*, to which IoT devices the guidelines will apply. According to **one estimate**, the number of IoT connected devices will reach 125 billion by 2030.

Furthermore, the bill only applies to practices of the federal government and federally procured devices. While private sector practices remain nominally unaffected, NIST's guideline could spillover and serve as *de facto* standards for private sector management as well. Lastly, while the bill does not impose any standards on the functionality and security of IoT devices themselves, federal agencies are prohibited from procuring devices that do not allow for compliance with NIST's guidelines. This prohibition will likely have some effect on how manufacturers design their devices.

Congress will likely continue to deliberate on cyber and data security measures in the 117th Congress. ML Strategies will keep a close eye on implementing guidelines from this legislation, once enacted.

Authors

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.