Client Alert: Cybersecurity Improvement Act of 2020

IoT Baby-Steps: The Feds Enact Cybersecurity Improvement Act

By:Howard G. Zaharoff
December 15, 2020

INTRODUCTION

On December 4, 2020, the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (H.R. 1668, 116th Cong.) (the "Act") was signed into law. This bipartisan bill requires the National Institute of Standards and Technology (NIST) to create minimum cybersecurity standards for IoT devices purchased or used by the federal government. Guidelines are to be developed over the next several months, so the full impact of the Act remains uncertain for now. However, the Act sets out a framework for the guidelines and provides a glimpse of what is to come for IoT device security.

BACKGROUND

An IoT device is any object with software, a sensor, or other technology that allows it to interact with the physical world by transmitting data to another device through the internet. Section 3 of the Act defines IoT devices as being able to function on their own and not solely as a component of another device, and for purposes of the Act, laptops, smartphones, and other conventional technology devices are not included. The Act focuses on IoT devices used by federal government agencies, and the guidelines are applicable not only to those agencies, but also to any contractors who provide information systems, like IoT devices, to the government.

INTERNET OF THINGS (IOT) DEVICE GUIDELINES

NIST has 90 days to develop guidelines on the appropriate use and management of IoT devices owned or controlled by government agencies. *See* H.R. 1668 § 4. The goal is to minimize the cybersecurity risks of using IoT devices, since many are connected to government information systems. These guidelines must encompass secure development, identity management, patching processes, and configuration management for IoT devices, and should include examples of potential cybersecurity vulnerabilities in IoT devices. Additionally, the guidelines must be reviewed and revised no less than every five years. *See* § 4(c).

The Act also requires that NIST develop additional guidelines within 180 days, specifically for reporting and publishing cybersecurity vulnerabilities in such IoT devices. *See* § 5(a). In creating these guidelines, NIST will consult with cybersecurity researchers and industry specialists in the private sector, as well as the Office of Management and Budget. *See* § 5(a). The Act also requires the guidelines to align with industry best practices and other appropriate standards, to the extent practicable. *See* § 5(b). The guidelines must cover relevant procedures for both receiving and disseminating information related to a security vulnerability of an IoT device and must also include examples of the types of information that should be reported.

Finally, the Act gives future notice to federal contractors who provide IoT devices by setting out the consequence for noncompliance with NIST guidelines: Starting in two years, federal agencies generally will be *prohibited* from procuring or obtaining any IoT device that does not comply, meaning that such providers will be unable to sell their devices to the government. *See* § 7. However, the Act describes situations where the general prohibition may be waived, including devices necessary for national security or research purposes and devices that can be secured

using alternative effective methods.

IMPLICATIONS

Although the scope and depth of IoT guidelines remain to be determined, the bipartisan support for the Act's passage suggests widespread concern for IoT device risk and a desire for increased security. Bill sponsor Rep. Robin Kelly characterized the Act as "a critical step towards strengthening U.S. government IT systems [that]… will help officials patch existing vulnerabilities to protect our national security and the personal information of American families. . ."

Since suppliers of government IoT devices are directly impacted by the Act, they will have to keep watch for the coming guidelines to ensure that their products are sufficiently secure. In fact, others in the industry may need to keep watch beyond these guidelines, as many experts believe this Act foreshadows future legislation for IoT devices generally.

Although this Act may signify increased security regulations for IoT devices broadly as noted above, it does provide IoT developers and vendors with some flexibility. For example, Section 7 exempts devices that are secured "effectively," seeming to allow IoT providers to secure their devices using their own methods, while still remaining compliant.

CONCLUSION

Although the specific guidelines for government IoT devices are not yet clear, it is apparent that there is a growing concern over the cybersecurity risks of such devices. Although the scope of this Act is limited to devices purchased or used by the government, IoT device providers should start to examine the security of their own devices to best prepare for the future. For more information about this topic, please contact Howard Zaharoff.

The author would like to acknowledge the contributions to this article by and give thanks to Natalie Gallego, Northeastern University School of Law (NUSL) 2021.