PUBLICATION

The New IoT Cybersecurity Improvement Act Becomes Federal Law

December 21, 2020

Recognizing the importance of Internet of Thing (IoT) devices to the federal government, the President signed the IoT Cybersecurity Improvement Act (the Act) into law on December 4, 2020. Manufacturers who build IoT devices for the federal government and government contractors (and their subcontractors) whose services involve IoT devices should pay special attention to the requirements of the Act, as it establishes minimum security requirements for IoT devices owned or controlled by the federal government and mandates that contractors (and their subcontractors) have IoT device vulnerability disclosure policies and procedures in place.

Security Standards and Guidelines

The Act requires the National Institute of Standards and Technology (NIST) to develop standards and guidelines for use of IoT devices by federal agencies. No later than 90 days from the date of the Act, NIST must create and publish standards and guidelines for the use of IoT devices owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices. Within five years of the date NIST publishes its standards and guidelines, and every five years thereafter, NIST must review and update its standards and guidelines as appropriate.

Within 180 days of the publishing of NIST standards and guidelines, the Office of Management and Budget (OMB), working with the Department of Homeland Security (DHS), must review agencies' existing information security policies and issue policies and procedures to ensure such information security policies are consistent with NIST standards and guidelines.

Guidelines on Vulnerability Reporting and Disclosure

Within 180 days from the date of the Act, NIST must work with private industry, cybersecurity researchers and DHS and develop guidelines for reporting security vulnerabilities of IoT devices and resolving such vulnerabilities. DHS, working with OMB, must provide assistance to (i) agencies on reporting and receiving information about security vulnerabilities of such IoT devices consistent with NIST's standards and guidelines and (ii) contractors and subcontractors on receiving and disseminating information relating to vulnerabilities, and resolution of those vulnerabilities.

Prohibition on Use of Non-Compliant IoT Devices

Subject to limited exceptions, a federal agency will not be able to procure or use an IoT device unless the device complies NIST standards and guidelines.

NIST's Draft Standards and Guidelines

On December 15, 2020, NIST released four new draft publications to begin providing guidance as mandated by the Act − NIST Special Publication 800-213 and NIST Interagency Reports 8259B, 8259C and 8259D. NIST Special Publication 800-213 provides overall guidance to federal agencies on what cybersecurity requirements

they need to look for when they acquire IoT devices, including recommendations to help federal agencies consider what security capabilities an IoT device needs to provide. The NIST Interagency Reports provide guidance for manufacturers who are building IoT devices for the federal government, to help them implement NIST's guidance from Special Publication 800-213. The public comment period on these documents extends through February 12, 2021.

Key Takeaways

Given that the Act contains provisions that prevent federal agencies from procuring, using or renewing a contract to procure or use an IoT device if the agency determines that use of the IoT device will prevent compliance with the NIST standards and guidelines, we know that:

- Any IoT device purchased by the federal government will have to comply with NIST's standards and guidelines, including Special Publication 800-213.
- Manufacturers providing IoT devices to the federal government will have to comply with NIST standards and guidelines, including NIST Interagency Reports 8259B, 8259C and 8259D when developing their products.
- Government contractors (and their subcontractors) whose services involve IoT devices will have to adopt vulnerability disclosure policies and procedures to report any vulnerability that may be discovered related to an IoT device.

Considering the timelines for compliance and the wide scope of the Act, manufacturers need to review NIST's new guidance and start building a plan on how to integrate this guidance into their manufacturing processes. Also, government contractors can begin creating or updating their IoT vulnerability management programs, with the knowledge that DHS's guidance will be in line with NIST's new standards and guidelines. While the guidance is still open to public comment, we recommend organizations begin to address the issues as soon as possible, as we do not foresee material modifications and the timeline will be very tight for most organizations.

If you would like to learn more about compliance with the Act, NIST"s guidelines, any related laws, or any aspect of your data privacy and cybersecurity practices, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.