Updates
December 09, 2020

New Internet of Things Cybersecurity Law Enacted

Internet of Things (IoT) devices have the potential to transform our home and work environment by integrating a growing range of "smart" wirelessly connected sensors into our daily lives. Recognizing the growing importance of IoT consumer and enterprise devices as well as their potential vulnerability to cyber attacks, both houses of Congress passed H.R. 1668, the IoT Cybersecurity Improvement Act of 2020 (the Act), which President Trump signed into law on December 4, 2020.

The Act mandates the creation of cybersecurity minimum requirements for IoT devices used by the federal government. Although intended to ensure the security of government information systems, these IoT minimum security requirements update existing National Institute of Standards and Technology (NIST) guidance regarding IoT cybersecurity. Because the federal government is such a large purchaser, as a practical matter the legislative standards could become the benchmark for reasonable security measures for IoT devices for both the enterprise and consumer IoT markets.

New Requirements for IoT Devices

Under the Act, the NIST must issue security guidelines within 90 days of the law's enactment on the use and management of IoT devices owned or controlled by the federal government. These security guidelines must, at a minimum, address secure development, identity management, patching, and configuration management for IoT devices.

The Act further requires the Office of Management and Budget (OMB) to conform agency guidelines to the NIST recommendations, including through revisions to the Federal Acquisition Regulation to implement the new security standards for IoT devices. Through OMB guidance to federal agencies and revisions to the Federal Acquisition Regulations, the law ensures that any IoT device purchased by the federal government complies with the NIST cybersecurity recommendations.

Although we will not know the contours of the NIST cybersecurity requirements until approximately three months from now, the requirements will build upon prior nonbinding guidance by NIST for private industry on improving cybersecurity for IoT devices through consideration of customer needs, goals, and use cases and communication about the proper use of IoT devices and the security risks they entail.

The existing NIST recommendations that will be updated by this Act are known as the "Foundational Cybersecurity Activities for IoT Device Manufacturers," which currently suggest identifying expected customers, users, and use cases, and determining how to address IoT device cybersecurity consistent with customer needs and goals. Based on the Act, new federal IoT cybersecurity recommendations should address the following issues:

- Cybersecurity risk-related assumptions that the manufacturer must make when designing and developing the device
- Mandatory software updates, including when, how, and by whom software updates will be distributed, and how customers can verify source and content of a software update as well as recommended device composition and capabilities, such as information about the device's software, hardware, services,

functions, and data types
- Minimum support and device lifespan, such as the expected term of support, what process will guide end of life, will any functions of the device remain after its end of life, and how customers may be able to maintain securability after support ends and at end of life

Following publication of the NIST recommendations, the law requires the director of OMB to review the NIST recommendations in consultation with the director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security. Within 180 days of publication of the NIST recommendations, OMB will promulgate policies applicable to federal agencies entailing minimum cybersecurity requirements for IoT devices.

The Act also directs NIST to publish guidelines on vulnerability disclosure and remediation for federal information systems, requiring contractors and vendors providing information systems to the U.S. government to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that can be effectively shared with a vendor for remediation. This effectively supplements the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 20-01, requiring federal agencies to develop and publish vulnerability disclosure policies.

Takeaways

IoT device manufacturers and entities that sell IoT devices to or manage devices for the U.S. government should take careful note of the NIST IoT cybersecurity guidelines when they are published pursuant to the new law. Because the federal government is a large purchaser of commercial-off-the-shelf (COTS) technology, even manufacturers that do not directly target federal government sales will have an incentive to comply. In addition, the NIST guidelines will likely become adopted broadly as best practices by manufacturers.

For example, Section 5 of the FTC Act requires manufacturers to ensure that their products contain reasonable security measures. The FTC has previously stated that compliance with prior NIST guidance on cybersecurity could provide evidence that an entity is implementing reasonable data security practices. Compliance with the new NIST guidelines may also be useful in defense of class action and other commercial litigation cases to refute allegations of negligent or improper data security practices or breach of contract. Additionally, commercial agreements involving data transfers and cybersecurity often contain representations and warranties of compliance with industry standard security practices pegged to NIST security guidelines. Accordingly, the IoT Cybersecurity Act, and the new NIST guidelines and OMB policies that will follow from it, are important for all IoT manufacturers even if one is not intending to produce products for federal government use.

Authors

Marc S. Martin

Partner
MMartin@perkinscoie.com 202.654.6351

Explore more in

Technology Transactions & Privacy Law Privacy & Security Communications

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers