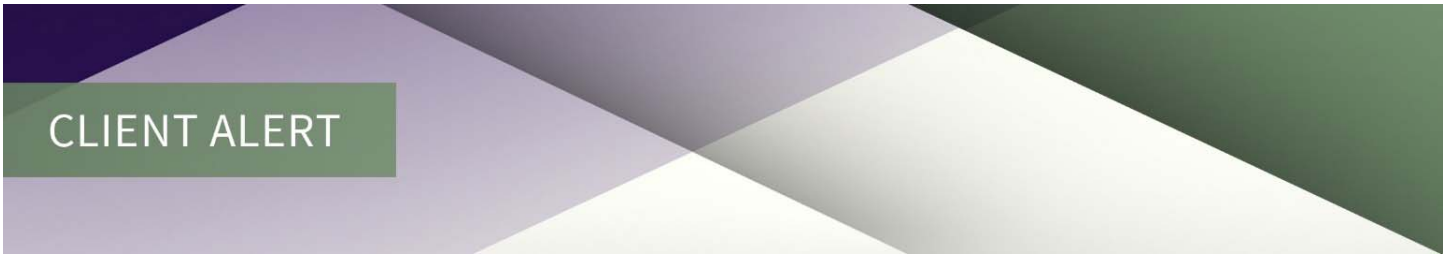
WILLKIE FARR & GALLAGHER LLP



IoT Cybersecurity Improvement Act of 2020

December 16, 2020

AUTHORS

Daniel K. Alvarez | Elizabeth Bower | Elizabeth P. Gray | Richard M. Borden
Stefan Ducich

On December 4, 2020, the bipartisan Internet of Things Cybersecurity Improvement Act of 2020 ("IoT Act") was signed into law. This statute marks an important step to standardize the assessment and treatment of vulnerabilities introduced by the use of Internet of Things ("IoT") devices by Federal government agencies. But its downstream impacts on manufacturers and service providers may be even more significant.

Background

IoT devices – physical objects with embedded sensors, software, and other technologies capable of connecting to other devices and systems over the Internet – are now ubiquitous. Along with clear benefits, these devices also introduce potential vulnerabilities into networks, operational technology, and operating systems. If exploited, these are capable of causing significant damage. Industry best practices have been ad hoc, comprised primarily of trade group guidance and recommendations directed at some combination of end users, IT departments, and manufacturers. And while California now regulates IoT manufacturers directly, state regulatory efforts have been sporadic and inconsistent. This lack of uniformity has been a significant issue for Federal agencies, too.

The IoT Act is an effort to leverage the procurement power of the Federal government by standardizing Executive Branch agencies' cybersecurity practices around IoT, particularly regarding the identification, assessment, and reporting of vulnerabilities. This represents a new approach – one which will be an important issue for vendors and service providers to the Federal government in the short term, and which has the opportunity to significantly influence private sector best practices generally in the long run.

Requirements of the IoT Act

The IoT Act calls for the development of new IoT device security guidance by the National Institute of Standards and Technology ("NIST"), new rules to be promulgated by the Office of Management and Budget ("OMB"), and amendments to the Federal Acquisition Regulations to effectuate the new minimum standards embodied in the NIST guidance and OMB rules. Ultimately, Federal agencies will be prohibited from purchasing IoT devices that do not meet the new standards adopted by NIST and OMB.

Per the IoT Act, NIST shall issue:

(i) *Standards and Guidelines for Use of IoT Devices by Agencies* – Within 90 days of enactment, NIST must issue guidance detailing the appropriate use and management by Federal agencies of IoT devices, consistent with, and building upon, current NIST recommendations relating to vulnerability management, secure development, identity management, patching, and configuration management for IoT devices; and

(ii) *Guidelines on the Disclosure Process for Security Vulnerabilities Relating to Information Systems, Including IoT Devices* – Within 180 days of enactment, in consultation with cybersecurity researchers, industry experts, and the Department of Homeland Security, NIST must publish guidelines for reporting, coordinating, publishing, and receiving information about security vulnerabilities related to IoT devices operated by, or on behalf of, a Federal agency, as well as resolving such issues and informing relevant parties about the same.

These guidelines do not apply to national security systems, and must be reviewed and revised, as necessary, at least every five years.

Following the publication of the NIST guidelines, OMB must conduct a review of agency cybersecurity policies and procedures, promulgate rules consistent with the guidelines, oversee the implementation of procedures conforming to the guidelines, and provide ongoing operational and technical assistance necessary to address security vulnerabilities affecting agencies' information systems that include IoT devices.

Takeaways

The IoT Act directly implicates Executive Branch agencies and their service/device providers, requiring new guidance from NIST and new regulations to be promulgated by OMB that could change the way these entities identify, account for, and address security risk in the IoT devices they purchase and use. However, the impact of these new standards will be felt far beyond the Federal agencies. Given the scale and breadth of products the Federal government may seek to purchase that are likely to fall within the ambit of the new regulations, the IoT Act will likely influence manufacturers and services providers to incorporate the new minimum standards into products available on the general market.

Moreover, the standards may be probative of industry best practices against which private companies may be evaluated in reasonableness of security measures, and may be used as a standard of care in IoT security. The IoT Act outlines a collaborative process whereby the NIST guidance is to be developed in consultation with public and private sector cybersecurity experts. To the greatest extent possible, the guidelines are to be aligned with industry best practices and are to be updated, at a minimum, every five years.

The IoT Act leaves many questions unanswered. It does not itself set the new minimum standards; rather, it requires NIST and OMB to do so within a relatively short time frame. This leaves open questions of the exact scope and contours of the forthcoming requirements, and how they will be implemented. However, by leveraging the Federal government's purchasing power, the new standards will likely have broader impact over time, significantly influencing standardization of IoT cybersecurity, vulnerability assessments, and remediation.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Stefan Ducich
202 303 1168
sducich@willkie.com

Copyright © 2020 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Palo Alto, San Francisco, Chicago, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.