crowell moring

CLIENT ALERT

NIST Floats Revised IoT Guidance as California Law Goes Into Effect

Jan.28.2020

Notable for being its first IoT guidance published since the January 1, 2020, implementation of California's law requiring all IoT devices to include "reasonable security features," the National Institute of Standards and Technology (NIST) has updated its manufacturer-facing IoT cybersecurity guidelines, NISTIR 8259, *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline*. This second draft "contains the same main concepts" as the first but revises how these concepts are presented to "clarify the concepts and address other comments from the public." The second draft describes "voluntary, recommended activities related to cybersecurity" that IoT device manufacturers can use to enhance the security profiles of IoT devices when they are ultimately deployed by consumers.

The recommended activities continue to center on designing and preparing IoT devices such that they can be properly outfitted by consumers with the firmware and software necessary to remain secure in myriad environments. NIST's aim is one of both flexibility and adaptability: through the activities, manufacturers can improve "how securable the IoT devices they make are," given what manufacturers might know about how their IoT devices will be used.

The revised NISTIR 8259 contains six broad activities and splits them into two groups: those that involve device design and configuration prior to sale, and those that involve communication with consumers after a device's sale.

In the "Pre-Market" group, NIST lists four primary activities that are focused on understanding how IoT products can meet consumer expectations regarding cybersecurity:

- Activity 1: Identify expected customers and define expected use cases.
- Activity 2: Research customer cybersecurity goals.
- Activity 3: Determine how to address customer goals.
- Activity 4: Plan for adequate support of customer goals.

By engaging in these activities, NIST expects that manufacturers will be better able to anticipate the environments in which consumers will deploy their devices and, in turn, design devices so that *consumers* can more easily secure them once in use.

The most robust of the four pre-market activities is Activity 3, for which NIST recommends a "core device cybersecurity capability baseline," described as "a set of device cybersecurity capabilities that customers are likely to need" in most IoT environments. Examples include the ability to change and update a device's firmware and software, using a secure and configurable mechanism; the ability to restrict logical access to a device's local and network interfaces, as well as the protocols and services used by those interfaces, to authorized entities only; and the ability to determine a device's cybersecurity state at any given time.

In the "Post-Market" group, NIST includes two activities:

- Activity 5: Define approaches for communicating to customers.
- Activity 6: Decide what to communicate to customers and how to communicate it.

These two activities center on providing consumers with the information necessary to secure particular IoT devices once deployed, and to maintain that security over a device's lifespan. Examples of "what to communicate to customers" include the cybersecurity "risk-related assumptions that the manufacturer made when designing and developing the device," device "support and lifespan expectations," and the "cybersecurity capabilities that a device provides."

The focus of the second draft of NISTIR 8259 continues to extend only to devices that can operate on their own, and that "have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface . . . for interfacing with the digital world."

Public comments on the second draft will be accepted through February 7, 2020. Even in draft form, however, IoT manufacturers can expect that consumers and regulators alike will consider NIST's guidance when assessing an IoT device's reasonable security.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Cheryl A. Falvey
Partner – Washington, D.C.
Phone: +1 202.624.2675
Email: cfalvey@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Kristin J. Madigan, CIPP/US
Partner – San Francisco
Phone: +1 415.365.7233
Email: kmadigan@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.

Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Paul C. Mathis
Associate – Washington, D.C.
Phone: +1 202.688.3432
Email: pmathis@crowell.com