wiley

NEWSLETTER

NIST Continues Its Influential Work on IoT Cybersecurity and Privacy

July 2019

Privacy in Focus®

In late June, the National Institute of Standards and Technology (NIST), within the Department of Commerce, released a revised report (NISTIR 8228) on security in the Internet of Things (IoT). This report, "Considerations for Managing [IoT] Cybersecurity and Privacy Risks," sheds light on the direction of federal thinking about IoT risks and identifies risk-mitigation goals that innovators and users of IoT devices should be aware of. The stated goal of NISTIR 8228 is "to help organizations better understand and manage the cybersecurity and privacy risks associated with individual [IoT] devices throughout the devices' lifecycles." NIST has several workstreams on IoT security, and has been taking input from stakeholders, including the tech sector, consumer advocates, and other government agencies.

This document comes amidst a flurry of interest in IoT security both in the United States and abroad, and by demonstrating IoT security governance, it may help the United States maintain a seat at the table as international expectations shift toward certification requirements and regulation.

The document consists of four basic sections.

First, NISTIR 8228 provides a non-comprehensive list of device capabilities that present different cybersecurity and privacy risks than conventional IT devices. These include capabilities such as interacting with the physical world as well as other devices, as shown in the following graphic reproduced from the document.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Second, NISTIR 8228 identifies three cybersecurity and privacy risk considerations with the potential to affect risk management for IoT devices. These risk considerations are:

- "Device Interactions with the Physical World." NIST noted that IoT devices may be particularly impacted by this consideration because "[m]any IoT devices interact with the physical world in ways conventional IT devices usually do not."
- "Device Access, Management, and Monitoring Features." NIST explained that "[m]any IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can."
- "Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness." NIST noted that "[t]he availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional devices."

Third, NIST identifies three high-level risk mitigation goals for managing cybersecurity and privacy risks for IoT devices. The goals are: (1) protect device security; (2) protect data security; and (3) protect individuals' privacy. NIST then highlighted what it perceived to be challenges for achieving these goals, based on common characteristics of IoT devices and their associated risk considerations. For example, NISTIR 8228 notes that some IoT devices "may not be capable of having [their] software patched or upgraded," which is related to the latter two risk considerations above and could preclude an organization from removing known vulnerabilities. The mapping of mitigation goals to challenges and risk considerations comprises most of the document.

Fourth, NIST provides "recommendations for addressing the cybersecurity and privacy risk mitigation challenges for IoT devices." As seen in the graphic from NISTIR 8228 below, the recommendations are interrelated and structured as (1) understanding risks; (2) implementing policies and processes to address those risks; and (3) updating those policies and processes as necessary.

While NISTIR 8228 covered a lot of ground, it is only "the first in a planned series of documents NIST is developing to help IoT users protect themselves, their data and their networks."

Specifically, NIST will host a workshop on August 13 to gather feedback as the agency develops an "IoT Security Baseline." (In fact, this baseline stems from a list of IoT device capabilities that NIST initially included—but then removed—in the NISTIR 8228 draft.) NIST circulated a discussion draft for the baseline a few months ago, explaining that it identified a "critical gap area" in "baselines focused on the pre-market cybersecurity capabilities that could be built into the products, as opposed to the cybersecurity controls that consumers could apply post-market." NIST is also making moves to address privacy in its parallel proceeding to develop a privacy framework, which Wiley Rein is involved in.

NIST is likely to continue devoting considerable resources to IoT privacy and cybersecurity for the foreseeable future.