wiley

ALERT

New IoT Cybersecurity Drafts From NIST Will Impact the Ecosystem

December 17, 2020

On December 15, 2020, the National Institute of Standards and Technology (NIST) released four new draft Internet of Things (IoT) cybersecurity documents to provide guidance for federal agencies and device manufacturers. Additionally, NIST is updating its catalog of IoT cybersecurity capabilities.

The concurrent release of this slate of IoT cybersecurity guidance comes on the heels of the IoT Cybersecurity Improvement Act of 2020, signed into law on December 4. NIST explains that the new documents "will help address challenges raised in [the Act] and begin to provide the guidance that law mandates." As NIST acknowledges, "[b]ecause companies that do business with government agencies will need to interact with technology the government finds acceptable, the guidance is likely to have far-reaching influence."

NIST is inviting public comment through February 12, 2021. Given the broad impact of NIST's IoT cybersecurity efforts to date, and the significant ground covered in the newly released drafts, industry stakeholders—including but not limited to IoT device manufacturers—should consider engaging.

NIST's New IoT Cybersecurity Guidance Drafts

The new draft documents are:

1. Draft NIST Special Publication (SP) 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Cybersecurity

Privacy, Cyber & Data Governance

2. Draft NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*
3. Draft NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*
4. Draft NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

Additionally, NIST is updating its IoT Device Cybersecurity Requirement Catalogs (the Catalogs) as supplemental content that may be used to support NIST-800-53 controls.

Draft SP 800-213 provides guidance to federal agencies, extending NIST's risk-based cybersecurity approach to include integration of IoT devices into federal information systems and infrastructure. NIST positions this as guidance for federal agencies with respect to acquisition and implementation of IoT devices. The core substance of this document is "guidance to federal agencies in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device." (10) It emphasizes that "[a]gencies should fully understand the specific use case for an IoT device since the use case could influence device cybersecurity requirements" (11) and lists several key questions agencies should consider.

The new drafts in the 8259 series—which are aimed at manufacturers of IoT devices—build on and complement NIST's foundational cybersecurity activities for IoT device manufacturers: NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* and 8259A, *IoT Device Cybersecurity Capability Core Baseline*. The new draft NIST Interagency Reports (NISTIRs)—8259B, 8259C, and 8259D—expand the range of guidance for IoT cybersecurity, providing a roadmap for IoT device manufacturers to help organizations implement SP 800-213's guidance:

- Draft NISTIR 8259B provides baseline non-technical capabilities, which is meant to complement the device cybersecurity core baseline (NISTIR 8259A) that NIST has already finalized.
- Draft NISTIR 8259C details the process for any organization to develop a customized profile — for example, for a specific organization or industry sector — using NIST's technical and non-technical capability baselines; and
- Draft NISTIR 8259D, the federal profile, serves as a worked example of applying NISTIR 8259C and developing a profile for the federal government customer user case.

Next Steps

IoT stakeholders should review the draft documents to determine whether to provide feedback. NIST is soliciting feedback through February 12, 2021.

Manufacturers should review the new guidance — which includes a new baseline, a new profile, and updated capabilities in the Catalogs — to see how reasonably they could implement NIST's suggestions.

Any company selling a connected device to the federal government should pay particularly close attention to these documents, and the additional workstreams launched by the IoT Cybersecurity Improvement Act of 2020.

***

Wiley's Privacy, Cyber & Data Governance practice has deep experience with IoT device cybersecurity issues and advising government contractors on contractual and regulatory information security requirements. Our team of attorneys and engineers regularly helps clients navigate emerging state and federal expectations, and we have a long-history of collaboration with NIST. If you have questions about how these recent development impact your organization or would like to engage with NIST, please reach out to one of the authors.