wiley

NEWSLETTER

2021 Preview: How the Private Sector Will be Impacted by IoT Cybersecurity Work at NIST

January 2021

Privacy In Focus®

The National Institute of Standards and Technology (NIST) has been an active driver of Internet of Things (IoT) cybersecurity efforts for several years, convening stakeholders from the federal government and the private sector to develop IoT risk management guidance. To date, NIST's Cybersecurity for IoT Program has collaborated across the wide IoT ecosystem to develop seminal voluntary guidance, including an IoT Device Cybersecurity Capability Core Baseline, which defines a set of device cybersecurity capabilities for organizations to consider when managing IoT risk.

NIST's important work in the IoT security space will continue in 2021. Recent developments – including the passage of the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (the IoT Cybersecurity Improvement Act) and a newly released slate of draft guidance documents – promise a busy year ahead for NIST, as well as multiple opportunities for continued industry engagement.

The IoT Cybersecurity Improvement Act Requires NIST to Develop Minimum Security Standards and Guidelines for the Federal Government That Will Form the Basis for New Procurement Restrictions.

On December 4, 2020, the bipartisan IoT Cybersecurity Improvement Act was signed into law. The new law requires baseline security standards and guidelines for IoT devices owned or controlled by federal government agencies. Specifically, the law requires NIST to develop and publish standards and guidelines for the federal government on the appropriate use and management of IoT devices

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

by agencies, including minimum security requirements. Based on these standards and guidelines, the Office of Management and Budget (OMB), in consultation with NIST and the U.S. Department of Homeland Security (DHS), must review federal agencies' IoT information security policies and principles – and issue policies and principles as needed – to ensure consistency with NIST's standards and guidelines. In addition to the provisions related to minimum IoT device security, the IoT Cybersecurity Improvement Act charges NIST with developing – in coordination with DHS, researchers, and the private sector – vulnerability disclosure policy guidelines for the "reporting, coordinating, publishing and receiving" reports about vulnerabilities in federal agency systems, including IoT devices, and systems offered by contractors to federal agencies. Additionally, the IoT Cybersecurity Improvement Act requires revision of the Federal Acquisition Regulation, as necessary, and prohibits federal agencies from procuring or using IoT devices where use of such a device would prevent compliance with the minimum security and vulnerability disclosure guidelines discussed above.

NIST must act quickly under the new law. For example, it is required to develop its security standards and guidelines by March 4, 2021. The subsequent OMB, NIST, and DHS review of federal agency policies and principles must be completed 180 days later, and the law requires review and revision, as appropriate, of the guidelines and accompanying policies and principles every five years.

Each of these provisions could have significant impacts on companies doing business, or looking to do business, with the federal government. Further, these baseline IoT security standards will have both direct and indirect cascading impacts throughout industry and critical infrastructure sectors. NIST publications regularly become doctrinal standards that feed into the international standards-setting community, which standards are invariably adopted by the private sector.

NIST Is Adding to Its IoT Risk Management Guidance Four New Documents, Including Guidance Specific to the Federal Government and a New Baseline Document for the Broader IoT Ecosystem.

Close on the heels of the IoT Cybersecurity Improvement Act, on December 15, 2020, NIST released four new draft IoT cybersecurity documents, as well as an updated IoT capabilities catalog. NIST explains that the new documents "will help address challenges raised in [the Act] and begin to provide the guidance that law mandates."

The new draft documents provide guidance for federal agencies and device manufacturers and are "intended to help ensure the government and IoT device designers are on the same page with regard to cybersecurity for IoT devices used by federal agencies." Some of the documents have a broader reach, beyond the federal government IoT use case. Specifically, the new draft documents are:

- Draft NIST SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.*
- Draft NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*
- Draft NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*
- Draft NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

Additionally, NIST has updated its IoT Device Cybersecurity Requirement Catalogs as supplemental content that may be used to support NIST-800-53 controls.

Draft SP 800-213 provides guidance to 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." 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" and lists several key questions agencies should consider.

The three 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 and 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 working application of NISTIR 8259C to develop a profile for the federal government customer use case.

Together, these documents will have significant impacts across the IoT ecosystem. NIST explains: "As is the case with all NIST publications, the guidance itself is **not regulatory**. … Because 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**." (emphasis added)

The four drafts are open for public comment through **February 12, 2021**.

NIST Is Beginning to Evaluate IoT Security Confidence Mechanisms, Including Labels and Self-Certifications.

Finally, on January 7, 2021, NIST published a summary of a recent IoT workshop that focused on building a Federal Profile for IoT device security. In the summary, NIST revealed that it will begin evaluating approaches for establishing confidence in IoT device security. It explains that "Workshop participants indicated a desire for greater specificity regarding the use of conformance assessments and other confidence mechanisms such as labels and self-certification," and noted that "these confidence mechanisms can be an important component of the IoT cybersecurity solution space."

Labeling and certification are fraught topics, as cybersecurity is highly technical, complex, and context-dependent. Additionally, cybersecurity is not a static concept, as technology and the threat landscape constantly evolve. NIST plans to collaborate closely with interested stakeholders as it begins to evaluate these approaches. Given the complexities involved, it is critical that industry engage closely with NIST to ensure the shared goals of establishing trust and confidence in IoT devices and continuing to improve IoT security.

***

2021 will be an active year as federal and state policymakers tackle cybersecurity and privacy issues related to emerging technologies, including but not limited to IoT. NIST's IoT efforts will be happening in parallel with a host of other important efforts – including those launched by the 2021 NDAA. In this environment, it is important for IoT stakeholders to remain active and engaged, as NIST's IoT security standards and guidance, as well as its work to evaluate mechanisms such as labeling, will have long-lasting effects across the burgeoning IoT ecosystem.