wiley

NEWSLETTER

How to Protect IoT Devices: NIST Issues Key Draft Cybersecurity Guidance

August 2019

Privacy in Focus®

The National Institute of Standards and Technology (NIST) released in late July NISTIR 8259, a draft of the long awaited[1] "Core Cybersecurity Feature Baseline for Securable IoT Devices." The publication (the baseline draft) proposes a voluntary, flexible, minimum "baseline of cybersecurity features based on common cybersecurity risk management approaches as a starting point for manufacturers." (p. 1). We expect it to shape standards of care and regulatory expectations for manufacturers and sellers of all connected devices. For stakeholders, and others, NIST provided multiple opportunities for engagement. NIST held a workshop on the baseline on August 13. Comments on the baseline draft are due September 30.

NIST's baseline draft is part of NIST's longstanding and ongoing work on IoT device security. These federal efforts are increasingly important, given that states — California and Oregon thus far — have enacted legislation to require IoT device manufacturers to equip such devices with reasonable security features. Both of those laws reference, and give various levels of deference to, federal IoT requirements. All of these efforts come amidst global regulatory interest in IoT security, from the European Union's certification requirements to evolving industry best practices.

NIST's document is primarily targeted at IoT device manufacturers and secondarily at individuals and entities that purchase such 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

This article will tell you what you need to know about: (1) the scope of the draft; (2) the features included in the baseline itself; and (3) NIST's guidance about implementation.

NIST focuses on manufacturers and consumers of IoT devices

NIST defines the audience for the baseline draft as (1) "IoT device manufacturers seeking a better understanding of how to identify the appropriate cybersecurity features for their IoT devices, or wanting a common language for communicating with others regarding these features;" and (2) a "secondary audience" of "IoT device customers (i.e., individuals and organizations) that want to specify which cybersecurity features they need from IoT devices during their evaluation and acquisition process." (p. iii).

The draft covers only devices with the following characteristics: (1) at least one transducer "for interacting with the physical world;" and (2) "at least one network interface (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee); and (3) "are not conventional IT devices . . . (e.g., smartphone, laptop)." (p. 1).

Finally, the baseline is a starting point that "addresses general cybersecurity risks faced by a generic consumer." (p. ii). NIST explains that the baseline should be the "default for minimally securable devices" but recognizes that "cybersecurity features will often need to be *added* or *removed* from an IoT device's design to take into account the manufacturer's understanding of customers' likely cybersecurity risks." (p. 9). The baseline also does not say how a feature must be achieved, providing manufacturers with "considerable flexibility in implement[ation] . . ." (p. 9).

The Draft Offers Six Baseline Features and Dozens of Elements it Suggests for Security By Design

The baseline contains six features for IoT devices. However, each "feature" is comprised of multiple "key elements," with a total of 22 such elements. These "features" and "key elements" are reproduced below: Feature Key Elements Device Identification: The IoT device can be uniquely identified logically and physically.

1. A unique logical identifier
2. A unique physical identifier on it at an external or internal location authorized entities can access Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.

1. The ability to change the device's software and firmware configuration settings
2. The ability to restrict configuration changes to authorized entities only
3. The ability for authorized entities to restore the device to a secure default configuration defined by an authorized entity Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.

1. The ability to use accepted cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised

2. The ability for authorized entities to configure the cryptography use itself when applicable, such as choosing a key length
3. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data) Logical Access to Interfaces: The IoT device can limit logical access to its local and network interfaces to authorized entities only.

1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device
2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication)
3. The ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.

1. The ability to update all the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media)
2. The ability to confirm the validity of any update before installing it
3. The ability to restrict updating actions to authorized entities only
4. The ability to enable or disable updating
5. The ability to set remote update mechanisms to be either automatically or manually initiated for update downloads and installations
6. The ability to enable or disable notification when an update is available and specify who or what is to be notified Cybersecurity Event Logging: The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

1. The ability to log cybersecurity events across the device's software and firmware
2. The ability to record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened
3. The ability to restrict access to the logs so only authorized entities can view them
4. The ability to prevent any entities (authorized or unauthorized) from editing the logs
5. The ability to make the logs available to a logging service on another device, such as a log server

Each feature references "existing sources of IoT device cybersecurity guidance specifying a similar or related cybersecurity feature." (pp. 9-12). These references include publications from both private and public entities, such as CTIA's Cybersecurity Certification Test Plan for IoT Devices and the European Union Agency for Network and Information Security's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.

Lastly, each feature also contains NIST's rationale for its inclusion in the baseline. Under "data protection," for example, NIST explained that "[c]ustomers often want the confidentiality of their data protected so unauthorized entities cannot access their data and misuse it." (p. 11).

Implementation Is Voluntary But Encouraged

Implementation of the baselines is voluntary. NIST explains that "manufacturers may *voluntarily* adopt [the baseline] for IoT devices they produce." (p. ii). And the "overall objective of this publication is to provide *voluntary guidance* for IoT device manufacturers . . ." (p. iv).

As noted above, this voluntary implementation of the baseline is intended to be flexible. Nevertheless, NIST provides four general categories of guidance for implementation of both the baseline and ancillary activities (e.g., customer disclosure).

First, NIST provides a non-comprehensive list of considerations for device manufacturers regarding *provisioning cybersecurity features*. (pp. 14-15). At a high level, these include the following recommendations:

- Select or build a device with sufficient hardware, firmware, and software resources to support desired features.
- "Be forward-looking and size hardware resources for potential future use."
- "Use hardware-based cybersecurity features."
- "Do not include unneeded features . . ."
- "Do not force the use of features that may negatively impact operations."
- "[C]onsider using an established IoT platform instead of acquiring and integrating hardware, firmware, and supporting software components (e.g., operating system)."

Second, NIST encourages IoT manufacturers to consider the context in which IoT devices will be used in order to recognize opportunities for "cybersecurity feature inheritance." (pp. 15-16). As an example, NIST notes that "if an IoT device is intended for use in an environment with stringent physical security controls in place, a manufacturer might be able to omit restricting access to the device's local interfaces because the facility's physical security can take care of it." (p. 15).

Third, NIST recommends that manufacturers provide cybersecurity information to customers. It provides specific examples under the rubric of five main categories: (1) device cybersecurity features; (2) device transparency; (3) software and firmware update transparency; (4) support and lifespan expectations; and (5) decommissioning. For example, under device cybersecurity features, NIST recommends "[c]ommunicating to customers which cybersecurity features the device provides, especially using common terminology (e.g., the feature names from the core baseline) . . ." (p. 17).

Fourth, NIST provides resources to manufacturers looking for information on secure software development practices for IoT devices. (pp. 20-21). Rather than diving into specifics, NIST points manufacturers to a number of white papers that lay out these best practices.

Next Steps

NIST wants feedback! They can change the draft before it is finalized, so IoT stakeholders should review it and determine whether they want to provide feedback.

Manufacturers should have their design and engineering teams review the baselines to see how reasonably they could implement NIST's suggestions.

Any company selling a connected device to the government should pay particularly close attention to this document because of ever-increasing attention being paid to IoT by procurement officials.

Policymakers should consider NIST's extensive treatment of the complexity and variety in IoT ecosystems, recognizing that when it comes to IoT security, one size does not fit all.

---

[1] NIST had initially included a precursor to this baseline in its NISTIR 8228 draft but ultimately decided to remove it, explaining in the final draft that the baseline would be "refined and released in a separate publication." Additionally, NIST explains in the current baseline draft that the baseline is part of the larger Botnet Road Map published by the Departments of Commerce and Homeland Security in November 2018. (pp. iv-v).