**Frequently Asked Questions (FAQs)**

**Federal Profile of NISTIR 8259A (“Federal Profile”)**

June 30, 2020

1. ***What is the Federal Profile?***

The Federal Profile is a catalog of Internet of Things (IoT) device cybersecurity capabilities and supporting non-technical manufacturer capabilities and associated IoT device customer controls designed to protect an organization’s devices, data, systems, and ecosystems.

1. ***What is the goal of the Federal Profile?***

NIST’s goal is to enable Federal agencies to securely incorporate IoT devices into their systems and meet their security requirements for Federal information and systems. The future Federal Profile should help manufacturers looking at Federal customers and use cases to go beyond identifying the types of cybersecurity capabilities listed in NISTIR 8259A to considering additionally needed technical and non-technical cybersecurity capabilities.

1. ***How can I access and provide feedback on the Federal Profile?***

Anyone can view and submit feedback on the catalog through GitHub [link to Federal Profile landing page]. Feedback can also be sent to [IoTsecurity@nist.gov](mailto:IoTsecurity@nist.gov).

1. ***Has NIST provided any guidance or direction regarding the nature of the feedback it seeks?***

Yes. NIST requests feedback on both the *technical* and *non-technical* device cybersecurity capabilities outlined in the Federal Profile and has formulated specific questions to help guide feedback submissions:

* For any given technical capability and sub-capability, have we identified the most common, or expected, device cybersecurity capability or sub-capability that should be built within an IoT device?
* Are there any common IoT device technical cybersecurity capabilities or sub-capabilities that we have not included? Please describe.
* Do you have any suggested updates or additions to elements of device cybersecurity capabilities and sub-capabilities, or suggestions for re-arranging the elements? Please describe.
* Are there any common IoT device non-technical manufacturer capabilities that we have not included? Please describe.
* Do you have any suggested updates or additions to the non-technical capabilities? Please describe.
* Do you find it useful to have the technical capabilities catalog separate from the non-technical capabilities? Why or why not?
* Is this structure (i.e., capability->sub-capability->element) useful for defining device cybersecurity capabilities?
* Would mapping the catalog elements to NISTIR 8259A, NIST SP 800-53 (rev 4 or rev 5) and/or the Cybersecurity Framework be helpful?

1. ***How did the Federal Profile come about?***

[NIST](https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program) leveraged the core baseline established in [NISTIR 8259A](https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf) and analyzed the controls found in NIST SP 800-53 to develop a catalog of key IoT device cybersecurity capabilities and supporting non-technical manufacturer capabilities to ensure that customers’ systems meet an established level of management, operational, and technical security control requirements.

This catalog is a critical building block for establishing a federal profile of NISTIR 8259A (i.e. the “Federal Profile”) to help government entities securely incorporate IoT devices into their systems and meet security requirements for federal information and systems.

1. ***What is a device cybersecurity capability?***

A device cybersecurity capability is a feature or function that a device provides through its hardware or software that customers (both organizations and individuals) need to secure the device as a key component of overall IT ecosystem security.

1. ***What is the core baseline?***

The core baseline provided in NISTIR 8259A is comprised of device capabilities generally needed to support common cybersecurity controls. It provides a vital foundation upon which industry- and market-specific baselines can be formulated.

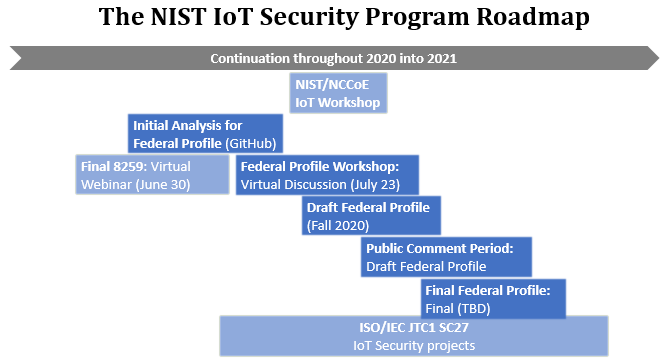
1. ***Will NIST update the Federal Profile over time?***

NIST has well-established strategies and processes for reviewing and updating all of its guidance—including the Federal Profile—to help ensure long-term value and effectiveness.

1. ***What’s Next for the Federal Profile?***

NIST seeks feedback from stakeholders on this initial analysis of the Federal Profile via GitHub and a series of events to follow as they are highlighted in the current snapshot of the NIST IoT Device Security Publication Roadmap below throughout 2020 into 2021.

**NIST IoT Device Security Publication Roadmap**



NIST also continues its active involvement and leadership role in the joint technical committee of the [International Organization for Standardization](https://www.iso.org/home.html) (ISO) and the [International Electrotechnical Commission](https://www.iec.ch/) (IEC) to develop an international baseline of IoT device cybersecurity capabilities.