DRAFT: FEDERAL PROFILE OF NISTIR 8259A: TECHNICAL DEVICE CYBERSECURITY CAPABILITIES NEEDED TO SUPPORT FEDERAL CYBERSECURITY CONTROLS

June 30, 2020

This publication is available free of charge from:
https://pages.nist.gov/FederalProfile-8259A/

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way.

National Institute of
Standards and Technology
U.S. Department of Commerce

Next Steps for the Cybersecurity for IoT Program in the Development of a Federal Profile of NISTIR 8259A

Introduction

IoT devices may create new pathways in and out of the network systems within which they are used. These issues make controlling the secure use of IoT devices within networking systems a new and challenging task. It is also challenging when trying to identify and mitigate the cybersecurity risks and then effectively protect the associated IoT data, interfaces and linked systems. This newest effort aims to help manufacturers and Federal government agencies better understand what kinds of device cybersecurity capabilities and supporting non-technical manufacturer capabilities may be needed from or around IoT devices used by Federal government agencies.

NIST Guidance

NIST has developed extensive guidance over the years for cybersecurity, which also supports implementation of the Federal Information Security Modernization Act (FISMA) of 2014. The guidance developed to support FISMA implementation is designed to be technology neutral so it can be applied to any type of system, from the risk management framework (NIST SP 800-37, Revision 2) methodology to manage risk to the security and privacy controls (NIST SP 800-53) that identify the countermeasures and outcomes to protect information, systems, and the privacy of individuals. However, there is the opportunity to provide additional guidance to assist federal organizations in understanding the specific risks that IoT devices introduce into federal systems and organizations.

NISTIR 8259 provides manufacturers with guidance for identifying an initial core baseline of device cybersecurity capabilities and foundational activities to consider throughout the product development process. The core baseline and foundational activities are intended to help IoT device manufacturers make their IoT devices securable, giving IoT device customers the cybersecurity capabilities to meet their security goals.

IoT Device Cybersecurity Capabilities

With the release of NISTIR 8259 and NISTIR 8259A, NIST is now establishing a catalog of IoT device cybersecurity capabilities and supporting non-technical manufacturer capabilities and associated IoT device customer controls that are shown within this GitHub page. Manufacturers can engineer the technical capabilities and provide non-technical capabilities to IoT device customers, who can then use those capabilities to ensure their systems meet an established level of management, operational and technical security control requirements. The capabilities needed for each IoT device will depend upon the risks that the device brings to the system within which it is implemented.

This initial catalog of IoT device cybersecurity technical capabilities and non-technical capabilities will be referred to as the "Federal Profile" from this point forward. The Federal Profile identifies technical and non-technical capabilities necessary applicable for any type of IoT device used within a Federal environment. The Federal profile may also be useful to non-Federal organizations, or they may choose to create their own baseline profiles by choosing a different set of capabilities and elements from the catalog.

Ultimately, the 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 aims to help manufacturers looking at federal customers and use cases go beyond identifying the types of cybersecurity capabilities listed in NISTIR 8259A to considering additionally needed technical and non-technical cybersecurity capabilities.

We Need Your Feedback

NIST has developed this initial catalog of IoT device cybersecurity technical and non-technical capabilities based primarily on the guidance used by Federal agencies in NIST SP 800-53. Device cybersecurity capabilities and non-technical manufacturer capabilities are the focus of the catalog on GitHub which aim to support security controls that agencies must implement from NIST SP 800-53. A Federal Profile of the IoT device cybersecurity capability core baseline can help manufacturers and agencies more readily understand how an IoT device can support security.

The catalog has two parts - one part listing possible device technical cybersecurity capabilities and elements; the other part listing possible supporting non-technical capabilities. This initial catalog builds on the structure of NISTIR 8259A by expanding the depth of definitions for technical capabilities through new sub-levels of detail known as "sub-capabilities". The sub-capabilities are composed of elements that appear as individual bullets. This same structure is also represented in the catalog of non-technical capabilities.

We ask for your feedback on the material we have created. Please answer the following questions: 1. 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? 2. Are there any common IoT device technical cybersecurity capabilities or sub-capabilities that we have not included? Please describe. 3. 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. 4. Are there any common IoT device non-technical manufacturer capabilities that we have not included? Please describe. 5. Do you have any suggested updates or additions to the non-technical capabilities? Please describe. 6. Do you find it useful to have the technical capabilities catalog separate from the non-technical capabilities? Why or why not? 7. Is this structure (i.e., capability->sub-capability->element) useful for defining device cybersecurity capabilities? 8. Would mapping the catalog elements to NISTIR 8259A, NIST SP 800-53 (rev 4 or rev 5) and/or the Cybersecurity Framework be helpful?

June 30, 2020

Draft: Federal Profile of NISTIR 8259A: Technical Device Cybersecurity Capabilities needed to Support Federal Cybersecurity Controls

Table of Contents

Device Identity

Asset Identifier Support

Ability for device identification. Capabilities that may be necessary:

- Ability to uniquely identify the IoT device physically.
- Ability to uniquely identify the IoT device logically.
- Ability to uniquely identify a remote IoT device.
- Ability for the IoT device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device).

Actions Based on Device Identity

Actions that can occur based on or using the identity of the device. Capabilities that may be necessary:

- Ability to configure IoT device access control policies using IoT device identity.
  - Ability to hide IoT device identity from non-authorized entities.
  - Ability for the IoT device to differentiate between authorized and unauthorized remote users.
  - Ability for the IoT device to differentiate between authorized and authorized physical device users.
- Ability to monitor specific actions based on IoT device identity.
- Ability to identify software loaded on the IoT device based on IoT device identity.

Device Authentication Support

Actions to support local or interfaced device authentication. Capabilities that may be necessary:

- Ability for the IoT device to identify itself as an authorized entity to other devices.
- Ability to verify the identity of an IoT device.

Device Configuration

The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements.

Logical Access Privilege Configuration

Ability for only authorized entities to apply logical access privilege settings within the IoT device and configure logical access privilege as described in Logical Access to Interfaces.

Authentication and Authorization Configuration

Ability for only authorized entities to configure IoT device authentication policies and limitations as described in Logical Access to Interfaces.

Interface Configuration

Ability for only authorized entities to configure aspects related to the device's interfaces as described in Logical Access to Interfaces.

Display Configuration

Ability to configure content to be shown within a device display as described in Logical Access to Interfaces.

Adaptable Configuration

Ability to change configurations on the IoT device based on operational events as described in Device Security and Cybersecurity Event Awareness.

Data Protection

Cryptography Capabilities and Support

Ability for the IoT device to use cryptography for data protection. Capabilities that may be necessary:

- Ability to utilize sufficient resources to employ cryptographic mechanisms.
- Ability to obtain and validate certificates.
- Ability to verify digital signatures.
- Ability to run hashing algorithms.
- Ability to compute and compare hashes.
- Ability to change keys securely.
- Ability to manage cryptographic keys securely.
  - Ability to generate key pairs.
  - Ability to store encryption keys securely.
  - Ability to change keys securely.

Secure Storage

Ability for the IoT device, or tools used through the IoT device interface, to enable secure device storage. Capabilities that may be necessary:

- Ability to support encryption of data at rest.
  - Ability to cryptographically store passwords at rest, as well as other authentication data.
  - Ability to support data encryption and signing to prevent data from being altered in device storage.
- Ability to secure data in device storage.
  - Ability to secure data stored locally on the device.
  - Ability to secure data stored in remote storage areas (e.g., cloud, server, etc.).
  - Ability to utilize separate storage partitions for system and user data.
- Ability to “sanitize” or “purge” specific or all data within the device.

Secure Transmission

Ability to secure data transmissions sent to and from the IoT device. Capabilities that may be necessary:

- Ability to configure the cryptographic algorithm to protect data in transit.
  - Ability to support trusted data exchange with a specified minimum strength cryptography algorithm.
  - Ability to support data encryption and signing to prevent data from being altered in transit.
- Ability to utilize one or more capabilities to protect the data it transmits from unauthorized access and modification.
- Ability to use cryptographic means to validate the integrity of data transmitted.

Logical Access to Interfaces

Authentication and Identity Management

Ability to require, or not require, authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements. Capabilities that may be necessary:

- Ability for the IoT device to support and require appropriate authentication.
  - Ability for the IoT device to require authentication prior to connecting to the device.
  - Ability for the IoT device to support a second, or more, authentication method(s) through an out of band path such as:
    - Temporary passwords or other one-use logon credentials
    - Third-party credential checks
    - Biometrics
    - Text messages
    - Hard Tokens
    - Manufacturer proprietary method
  - Ability for the IoT device to hide or mask authentication information during authentication process.
- Ability to set and change authentication configurations, policies and limitations settings for the IoT device.
  - Ability to set the time period for how long the device will remain locked after an established configurable limit of unsuccessful login attempts has been met.
  - Ability to disable or lock access to the device after an established pre-defined or user-configurable number of unsuccessful login authentication attempts.
  - Ability to display and/or report the previous date and time of the last successful login following successful login authentication.
  - Ability to automatically disable accounts for the IoT device after an establish period of inactivity.
    - Ability to support automatic logout of inactive accounts for the IoT device after a configurable established time period.
    - Ability to support automatic removal of temporary, emergency and other special use accounts from the IoT device after an established time period.
- Ability to display to IoT device users an organizationally-defined system use notification message or banner prior to successful IoT device authentication. (e.g., the message or banner would provide privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance).
  - Ability to create an organizationally-defined system use notification message or banner to be displayed on the IoT device.

        - ∗ Ability to edit an existing IoT device display.
        - ∗ Ability to establish the maximum size (in characters, bytes, etc.) of the available device display.
    - – Ability to keep the notification message or banner on the device screen until the device user actively acknowledges and agrees to the usage conditions.
- Ability to restrict all unauthorized interactions.
    - Ability to identify authorized users and processes.
    - Ability to differentiate between authorized and unauthorized users (physical and remote).
- Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication.

Role Support and Management

Ability to establish unique, privileged, organization-wide, and other types of IoT device user accounts. Capabilities that may be necessary:

- Ability to create unique IoT device user accounts.
- Ability to assign roles to IoT device user accounts.
- Ability to identify unique IoT device user accounts.
- Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary, etc.).
    - Ability to establish user accounts to support role-based logical access privileges.
    - Ability to administer user accounts to support role-based logical access privileges.
    - Ability to use organizationally-defined roles to define each user account's access and permitted device actions.
    - Ability to support multiple levels of user/process account functionality and roles for the IoT device.
- Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).
    - Ability to create additional processes, roles (e.g., admin, emergency, temporary, etc.) and accounts as necessary to achieve least privilege.
    - Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).
    - Ability to limit access to privileged device settings that are used to establish and administer authorization requirements.

  - Ability for authorized users to access privileged settings.
- Ability to support organizationally-defined actions for the IoT device.
  - Ability to create organizationally-defined accounts that support privileged roles with automated expiration conditions.
  - Ability to establish organizationally-defined user actions for accessing the IoT device and/or device interface.
  - Ability to enable automation and reporting of account management activities.
    - Ability to assign access to IoT device audit controls to specific roles or organizationally-defined personnel.
    - Ability to control access to IoT device audit data.
    - Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access).
  - Ability to establish conditions for shared/group accounts on the IoT device.
  - Ability to administer conditions for shared/group accounts on the IoT device.
  - Ability to restrict the use of shared/group accounts on the IoT device according to organizationally-defined conditions.
- Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:
  - run-time access control decisions facilitated by dynamic privilege management.
  - organizationally-defined actions to access/use device.
- Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information.
- Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.

Limitations on Device Usage

Ability to establish restrictions for how the device can be used. Capabilities that may be necessary:

- Ability to establish pre-defined restrictions for information searches within the device.
- Ability to establish limits on authorized concurrent device sessions for:
  - User accounts
  - Roles
  - Groups
  - Dates

  - Times
  - Locations
  - Manufacturer established parameters

External Connections

Ability to support external connections. Capabilities that may be necessary:

- Ability to securely interact with authorized external, third-party systems.
- Ability to allow for the user/organization to establish the circumstances for when information sharing from the device and/or through the device interface will be allowed and prohibited.
- Ability to establish automated information sharing to approved identified parties/entities.
- Ability to identify when the external user's system meets the required security requirements for a connection.

Interface Control

Ability to establish controls for the connections made to the IoT device. Capabilities that may be necessary:

- Ability to establish requirements for remote access to the IoT device and/or IoT device interface including:
  - Usage restrictions
  - Configuration requirements
  - Connection requirements
  - Manufacturer established requirement
- Ability to restrict use of IoT device components (e.g., ports, functions, protocols, services, microphones, video, etc.).
- Ability to restrict use of IoT device services.
- Ability to enforce the established local and remote access requirements.
- Ability to prevent external access to the IoT device management interface.
- Ability to control the IoT device's logical interface (e.g., locally or remotely).
- Ability to change IoT device logical interface(s).
- Ability to control device responses to device input.
- Ability to control output from the device.
- Ability to support communications technologies (including but not limited to):
  - 802.11x

  - Bluetooth
  - Ethernet
  - Manufacturer defined
- Ability to establish and configure IoT device settings for communications technologies including authentication protocols (e.g., EAP/TLS, PEAP).

Software Update

Ability to update the IoT device software within the device and/or through the IoT device interface. Capabilities that may be necessary:

- Ability to update the software by authorized entities only using a secure and configurable mechanism.
- Ability to identify the current version of the organizational audit policies and procedures governing the software update.
- Ability to restrict software installations to only authorized individuals or processes.
- Ability to restrict software changes/uninstallations to only authorized individuals or processes.
- Ability to verify software updates come from valid sources using an effective method (e.g., digital signatures, checksums, certificate validation, etc).

Cybersecurity Event Awareness

Access to Event Information

Ability to access IoT device state information. Capabilities that may be necessary:

- Ability to access information about the IoT device's cybersecurity state and other necessary data (e.g., trustworthy time).
- Ability to preserve system state information.

Event Identification and Monitoring

Ability to provide event identification and monitoring capabilities and/or support event identification and monitoring tools interfacing with the device. Capabilities that may be necessary:

- Ability to identify organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.
- Ability to monitor for organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.
- Ability to support a list of events that are necessary for auditing purposes (to support the organizational auditing policy).
- Ability to identify unique users interacting with the device (to allow for user session monitoring).
- Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check).
- Ability to monitor communications traffic.
- Ability to detect remote activation attempts.
- Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera, etc.).
- Ability to detect remote activation of sensors.
- Ability to define the characteristics of unapproved content.
- Ability to scan files for unapproved content.

Event Response

The device can respond to organizationally-defined cybersecurity events in an organizationally-defined way. Capabilities that may be necessary:

- Ability to generate alerts for specific events (e.g., capacity thresholds).
- Ability to respond to alerts according to predefined responses (e.g., such as those dictated by the auditing policies of the organization).
- Ability to alert connected information systems of potential issues found during the auditing process.
- Ability to provide information to an external process that will issue auditing process alerts.
- Ability to notify users of activation of a collaborative computing device.
- Ability to provide a physical indicator of sensor use.
- Ability to respond following an auditing failure (either by the device or an external auditing process that interacts with the device).
- Ability to prevent download of unapproved content.
- Ability to delete unapproved content.
- Ability to support alternative security mechanisms when primary mechanisms (e.g., login protocol, encryption, etc.) are compromised.

Audit Support

Ability for the device, or an interfaced system, to generate, store, retain, delete, and report on specific device audit events, to run specific audit checks, and report findings in a variety of ways. Capabilities that may be necessary:

- The device can generate audit logs for defined events
  - Ability to identify and capture organizationally-defined events using a persistent method.
  - Ability to capture information related to organizationally-specified cybersecurity events (e.g., cybersecurity state, timestamp) through organizationally-defined means (e.g., logs).
  - Ability to create audit logs within the device for organizationally-defined and auditable events (e.g. account creation, modification, enabling, disabling, removal actions and notifications).
- The device can capture required information in audit logs
  - Ability to track users interacting with the device, the time they interacted with the device, the time the user logged out of the device, and to list this information in an audit log.

    - Ability to log information pertaining to:
        - The type of event that occurred
        - The time that the event occurred
        - Where the event occurred
        - The source of the event
        - The outcome of the event
        - Identity of users/processes associated with the event
    - Ability to support auditing of configuration actions.
    - Ability to provide information as to why the device captured a particular event or set of events.
    - Ability to capture organizationally-defined information to support examination of security incidents.
    - Ability to record stored data access and usage.
- Ability to maintain audit logs in accordance with organizational policy.
    - Ability to comply with organizational policy for storing persistent audit logs up to a predefined size.
    - Ability to comply with organizational policy for audit log retention period (i.e., the required time to keep the audit logs).
    - Ability to delete audit logs in accordance with organizational policy.
    - Ability to send alerts that the logs are too big for the device to continue to store (if the predefined amount of time has not yet passed to delete them).
- Ability to use timestamps to record the time an auditing event occurred.
    - Ability to support organizationally-defined granularity in device timing measurements.
    - Ability to use synchronization with a verified time source to determine the validity of a timestamp.
    - Ability to record timestamps that can be translated to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) to support a standardized representation of timing.
    - Ability to log timing measurements that stray beyond a set threshold value (e.g., enabling alerts if the device's system time is too far out of sync to be reliable).
- Ability to report on its cybersecurity state.
- Ability to support a self-audit generation process.
- Ability to run audit scans (automated or otherwise) to provide specific information (e.g., such as that requested for an external process to audit the device).
- Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting.).
- Ability to support an alternate auditing process in the event that the primary auditing process fails.

- Ability to protect the audit information through the use of:
  - Encryption
  - Digitally signing audit files
  - Securely sending audit files to another device
  - Other protections created by the device manufacturer

Device Security

Secure Execution

Ability to protect the execution of code on the device. Capabilities that may be necessary:

- Ability to enforce organizationally-defined execution policies.
    - Ability to execute code in confined virtual environments.
    - Ability to separate IoT device processes into separate execution domains.
- Ability to separate the levels of IoT device user functionality.
- Ability to authorize various levels of IoT device functionality.

Secure Communication

Ability to securely initiate and terminate communications with other devices. Capabilities that may be necessary:

- Ability to enforce traffic flow policies.
- Ability to utilize standardized protocols.
- Ability to establish network connections.
- Ability to terminate network connections (e.g., automatically based on organizationally-defined parameters).
- Ability to de-allocate TCP/IP address/port pairings.
- Ability to establish communications channels.
- Ability to secure the communications channels.
- Ability to interface with DNS/DNSSEC.
- Ability to store and process session identifiers.
- Ability to identify and track sessions with identifiers.

Secure Resource Usage

Ability to securely utilize system resources and memory. Capabilities that may be necessary:

- Ability to support shared system resources.
    - Ability to release resources back to the system.
    - Ability to separate user and process resources use.
- Ability to manage memory address space assigned to processes.
- Ability to enforce access to memory space through the kernel.

- Ability to prevent a process from accessing memory space of another process.
- Ability to enforce configured disk quotas.
- Ability to provide sufficient resources to store and run the operating environment (e.g., operating systems, firmware, applications).
- Ability to utilize file compression technologies (e.g., to provide denial of service protection).

Device Integrity

Ability to protect against unauthorized changes to hardware and software. Capabilities that may be necessary:

- Ability to perform security compliance checks on system components.
- Ability to detect unauthorized hardware and software components.
- Ability to take organizationally-defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a USB port is present).
- Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).

Secure Device Operation

Ability to operate securely and safely. Capabilities that may be necessary:

- Ability to keep an accurate internal system time.
- Ability to define various operational states.
- Ability to support various modes of IoT device operation with more restrictive operational states.
  - “travel mode” for transit.
  - “safe mode” for operation when some or all network security is unavailable.
  - Others as determined necessary based on the purpose and goals for the IoT device.
- Ability to define differing failure types.
- Ability to fail in a secure state.
- Ability to disable operations and/or functionality in the event of security violations.
- Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services, etc.) in accordance with organizationally-defined policies.
- Ability to sense the environment and securely (i.e., preserving confidentiality, integrity, and availability of the device and its data) interface with the environment, either directly or through the IoT system. Examples include:

- Emergency shutoff mechanism
- Emergency lighting mechanism
- Fire protection mechanism
- Temperature and humidity mechanism
- Water damage protection mechanism
- Manufacturer defined capability