# NIST Special Publication 800-213A IoT Device Cybersecurity Guidance for the Federal Government: *IoT Device Cybersecurity Requirement Catalog*

# Executive Order on Improving the Nation’s Cybersecurity

Issued May 12, 2021 by President Biden

One Area Covered by this Executive Order: Enhancing Software Supply Chain Security

- Includes the requirement that NIST shall initiate pilot programs to educate the public on the security capabilities of software development practices and Internet of Things (IoT) devices
- As part of NIST published two guidance documents relating to IoT devices in November:
  - Guidance relating to Establishing IoT Device Cybersecurity Requirements (NIST Special Publication (SP) 800-213) and
  - A revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A).

The publications are targeted to information security professionals, system administrators, and others in organizations tasked with assessing, applying, and maintaining security on a system

# NIST SP800-213A IoT Device Cybersecurity Requirement Catalog

- Help Federal Organizations determine device cybersecurity requirements for IoT devices they seek to use with federal information systems and other systems operated by the federal government.
- IoT devices in-scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for interfacing with the digital world.
- IoT devices in-scope for this publication can function on their own, although they may be dependent on specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality
- Shall be used with the guidance in Special Publication (SP) 800-213, *IoT Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* [NIST SP 800-213]
- Federal organizations can use this catalog of device cybersecurity requirements to determine those appropriate to support the security controls implemented on their system and in their organization

Note: Device cybersecurity requirements are device cybersecurity capabilities and non-technical supporting capabilities needed to integrate an IoT device into a system. Device cybersecurity capabilities are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software)

# NIST SP800-213A IoT Device Cybersecurity Requirement Catalog

## Device Cybersecurity Capabilities

- **Device Identification:** The capability to identify the IoT device for multiple purposes and in multiple ways to meet organizational requirements
- **Device Configuration:** The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements
- **Data Protection:** The capability to protect IoT device data to meet organizational requirements
- **Logical Access To Interfaces:** Ability to require authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements
- **Software Update:** Ability to update IoT device software, and to have support mechanisms for such updates
- **Cybersecurity State Awareness:** The capability to generate data indicating different types of events related to the use of the device to meet organizational requirements
- **Device Security** - The capability to secure the IoT device to meet organizational requirements

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Identification Subcapabilities

- **Identifier Management Support** - Ability for device identification Requirements that may be necessary
- **Device Authentication Support** - Ability to support local or interfaced device authentication
- **Actions Based on Device Identity** - Ability to perform actions that can occur based on or using the identity of the device
- **Physical Identifiers** - Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Identification

- **Identifier Management Support**

  Requirements that may be necessary:

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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Identification

- **Device Authentication Support**

  Requirements 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 unauthorized physical device users (e.g., using a method of authentication to verify the identity of physical device users)
  - Ability to monitor specific actions based on the IoT device identity
  - Ability to identify software loaded on the IoT device based on IoT device identity
  - Ability for the device identifier to be used to discover the IoT device for the purpose
    of network asset identification and management

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Identification

- **Actions Based on Device Identity**

  Requirements 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 other devices

- **Physical Identifiers**

  Requirements that may be necessary: None Specified

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Configuration Subcapabilities

- **Logical Access Privilege Configuration** - Ability for only authorized entities (e.g., organization personnel, other system elements, enabling systems) 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 displayed on a device

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Configuration

- **Logical Access Privilege Configuration**

  Requirements that may be necessary: None Specified

- **Authentication and Authorization Configuration**

  Requirements that may be necessary: None Specified

- **Interface Configuration**

  Requirements that may be necessary: None Specified

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Configuration

- **Display Configuration**

  Requirements that may be necessary:

  - Ability for authorized entities to change the device's software configuration settings
  - Ability for authorized entities to restore the device to a secure configuration defined by an authorized entity
  - Ability to maintain control over device configuration during service and repair
  - Configuration settings for use with the Device Configuration capability including, but not limited to:
    - Ability for authorized entities to configure the cryptography use itself, such as choosing a key length
    - Ability for authorized entities to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations
    - Ability for authorized entities to enable or disable notification when an update is available and specify who or what is to be notified
    - d. Ability for authorized entities to configure authentication mechanisms (e.g., minimum password length or complexity, force change of passwords on first use)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Data Protection Subcapabilities

- **Cryptography Capabilities and Support** - Ability for the IoT device to use cryptography for data protection
- **Cryptographic Key Management** - Ability to manage cryptographic keys securely
- **Secure Storage** - Ability for the IoT device, or tools used through the IoT device interface, to enable secure device storage
- **Secure Transmission** - Ability to secure data transmissions sent to and from the IoT device

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Data Protection

- **Cryptography Capabilities and Support**

  Requirements that may be necessary:

  - Ability to execute cryptographic mechanisms of appropriate strength and performance
  - Ability to obtain and validate certificates
  - Ability to verify digital signatures
  - Ability to run hashing algorithms (i.e., compute and compare hashes)
  - Ability to perform authenticated encryption algorithms

- **Cryptographic Key Management**

  Requirements that may be necessary:

  - Ability to manage cryptographic keys securely:
    - Ability to generate key pairs
    - Ability to store encryption keys securely
    - Ability to change keys securely
    - Ability to maintain exclusive control of cryptographic keys when used by external systems

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Data Protection

- **Secure Storage**

  Requirements that may be necessary:

  - Ability to support encryption of data at rest
    - Ability to cryptographically store passwords at rest, as well as device identity and 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 securely back-up the data on the IoT device
  - Ability to "sanitize" or "purge" specific or all data in the device

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Data Protection

- **Secure Transmission**

  Requirements 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
  - Ability to use organization-internal normalized formats to protect the data it transmits

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces Subcapabilities

- **Authentication Support** - Ability to support authentication methods
- **Authentication Configuration** - 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
- **System Use Notification Support** - Ability to support system use notifications
- **Authorization Support** - Ability to restrict all unauthorized interactions
- **Authentication & Identity Management** - Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication
- **Role Support & Management** - Ability to establish unique, privileged, organization-wide, and other types of IoT device user accounts
- **Limitations on Device Usage** - Ability to establish restrictions for how the device can be used
- **External Connections** - Ability to support external connections
- **Interface Control** - Ability to establish controls for the connections made to the IoT device

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Authentication Support**

  Requirements that may be necessary:

  - Ability for the IoT device to require authentication prior to connecting to the device, including using remote access
  - Ability for the IoT device to support and require appropriate authentication
  - 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
    - Other methods
  - Ability for the IoT device to hide or mask authentication information during authentication process

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Authentication Configuration**

  Requirements that may be necessary:

  - 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 number of unsuccessful login attempts
    - Ability to display and/or report the previous date and time of the last successful login authentication
    - Ability to automatically disable accounts for the IoT device after an established period of inactivity
      - Ability to support automatic logout of inactive accounts after a configurable established time period
      - Ability to support automatic removal of temporary, emergency and other special use accounts after an established time period
    - Ability to report or log failed login attempts
  - Ability to authenticate external users and systems
  - Ability to revoke the access of accounts and/or external users and systems

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **System Use Notification Support**

  Requirements that may be necessary:

  - 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

## Logical Access To Interfaces

- **Authorization Support**

  Requirements that may be necessary:

  - Ability to identify authorized users and processes (e.g., applications)
  - Ability to differentiate between authorized and unauthorized users (physical and remote)

- **Authentication & Identity Management**

  Requirements that may be necessary: None Specified

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Role Support & Management**

  Requirements 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Role Support & Management**

  Requirements that may be necessary (cont'd):

  - 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 or applications 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Role Support & Management**

  Requirements that may be necessary (cont'd):

  - 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

## Logical Access To Interfaces

- **Role Support & Management**

  Requirements that may be necessary (cont'd):

  - 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

## Logical Access To Interfaces

- **Limitations on Device Usage**

  Requirements 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **External Connections**

  Requirements 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 system meets the required security requirements for a connection
  - Ability to establish secure communications with internal systems when the device is operating on external networks

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Interface Control**

  Requirements 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, microphones, video).
  - Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device
  - Ability to restrict updating actions to authorized entities
  - Ability to restrict access to the cybersecurity state indicator to authorized entities
  - Ability to restrict use of IoT device services
  - Ability to enforce the established local and remote access requirements

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Logical Access To Interfaces

- **Interface Control**

  Requirements that may be necessary (cont’d):

  - 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 wireless technologies needed by the organization (e.g., Microwave, Packet radio (UHF/VHF), Bluetooth, Manufacturer defined)
  - Ability to support communications technologies (including but not limited to):
    - IEEE 802.11
    - Bluetooth
    - Ethernet
    - Manufacturer defined
  - Ability to establish and configure IoT device settings for wireless technologies including authentication protocols (e.g., EAP/TLS, PEAP)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Software Update Subcapabilities

- **Update Capabilities** - Ability to update the IoT device software within the device and/or through the IoT device interface
- **Update Application Support** - Ability to update the device’s software through remote (e.g., network download) and/or local (e.g., removable media) means

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Software Update

- **Update Capabilities**

  Requirements 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 for authorized entities to roll back updated software to a previous version (i.e., uninstall an update)
  - Ability to restrict software installations to only authorized individuals or processes
  - Ability to restrict software changes/uninstallations and other software update actions 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.)
  - Ability to execute the software update mechanism with fault tolerance such that a failed or interrupted update (e.g., loss of communication while downloading, device power loss while installing) does not degrade the IoT device’s cybersecurity state

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Software Update

- **Update Application Support** - Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means

  Requirements that may be necessary:

  - If software updates are delivered and applied automatically:
    - Ability to verify and authenticate any update before installing it
    - Ability to enable or disable updating
  - If software updates are remote:
    - Ability to set update mechanisms functions (e.g., download, installation) to be either automatically or manually initiated
  - If notifications for software updates are delivered through the IoT device:
    - Ability to enable or disable notification when an update is available
    - Ability to specify which entities should receive notifications

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness Subcapabilities

- **Access to Event Information** - Ability to access IoT device state information
- **Event Identification & Monitoring** - Ability to provide event identification and monitoring capabilities and/or support event identification and monitoring tools interfacing with the device
- **Event Response** - Ability for the device to respond to organizationally-defined cybersecurity events in an organizationally-defined way
- **Logging Capture & Trigger 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
- **Support of Required Data Logging** - Ability for the device to capture required information in audit logs
- **Audit Log Storage & Retention** - Ability to maintain audit logs in accordance with organizational policy
- **Support for Reliable Time -** Ability to use timestamps to record the time an auditing event occurred
- **Audit Support & Protection** - Ability for the device to support and protect audit activities and associated data
- **State Awareness Support** - Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Access to Event Information**

  Requirements that may be necessary:

  - Ability to access information about the IoT device's cybersecurity state and other necessary data
  - Ability to preserve system state information

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Event Identification & Monitoring**

  Requirements 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Event Identification & Monitoring**

  Requirements that may be necessary (cont’d):

  - Ability to monitor changes to the configuration settings
  - Ability to detect remote activation attempts
  - Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera)
  - Ability to detect remote activation of sensors
  - Ability to define the characteristics of unapproved content
  - Ability to scan files for unapproved content

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Event Response**

  Requirements that may be necessary:

  - Ability to generate alerts for specific events
  - Ability to respond to alerts according to predefined responses
  - 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)
  - 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
  - Ability to configure organizationally-defined aspects of the event response

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Logging Capture & Trigger Support**

  Requirements 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 from organizationally-defined cybersecurity events (e.g., cybersecurity state, time) 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)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Support of Required Data Logging**

  Requirements that may be necessary:

  - 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Support of Required Data Logging**

  Requirements that may be necessary (cont’d):

  - Ability to support auditing of configuration actions such as:
    - Current configuration state
    - History of configuration changes
    - When changes in configuration occurred
    - Which account made the configuration change
  - 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 use an alternative audit logging mechanism in case of failure of primary mechanism

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Audit Log Storage & Retention**

  Requirements that may be necessary:

  - 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
  - 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)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Support for Reliable Time**

  Requirements that may be necessary:

  - 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 convertible to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) to support a standardized representation of timing
  - Ability to log timing measurements outside a threshold value (e.g., enabling alerts if the device's system time is not reliable)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **Audit Support & Protection**

  Requirements that may be necessary:

  - 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 manufacture
  - Ability to prevent any entities from editing audit logs unless the entity is authorized and is responsible for maintaining the audit logs

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Cybersecurity State Awareness

- **State Awareness Support**

  Requirements that may be necessary: None Stated

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security Subcapabilities

- **Secure Execution** - Ability to protect the execution of code on the device
- **Secure Communication** - Ability to securely initiate and terminate communications with other devices
- **Secure Resource Usage** - Ability to securely utilize system resources and memory
- **Device Integrity -** Ability to protect against unauthorized changes to hardware and software
- **Secure Network Onboarding Support -** Ability to use secure network onboarding technologies to connect to the network
- **Secure Device Operation -** Ability to operate securely and safely

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Execution**

  Requirements 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Communication**

  Requirements 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 Transmission Control Protocol/Internet Protocol (TCP/IP) address/port pairings
  - Ability to establish communications channels
  - Ability to secure the communications channels
  - Ability to interface with Domain Name System/Domain Name System Security Extensions (DNS/DNSSEC)
  - Ability to store and process session identifiers
  - Ability to identify and track sessions with identifiers
  - Ability to use an anti-spoofing mechanism to prevent adversaries from falsifying security attributes
  - Ability to prevent untrusted data injections

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Resource Usage**

  Requirements 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 continue operation when associated networks are unavailable (e.g., a smart smoke detector must still go off when a fire occurs even if it is not attached to the associated network)
  - 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)
  - Ability to use or enforce hardware-based, write protect to protect certain software (e.g., firmware)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Device Integrity**

  Requirements that may be necessary:

  - Ability to perform security compliance checks on system components (e.g., verify acceptable baseline configuration, perform a tamper check)
  - Ability to detect unauthorized hardware and software components and other tampering with the IoT device when used
  - Ability to detect tampering throughout the system development lifecycle
  - 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)

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Network Onboarding Support**

  Requirements that may be necessary:

  - Ability for the IoT device to provide necessary data and/or perform necessary functions participate in the device-to-network authentication
  - Ability to identify and recognize the network
  - Ability to receive, store, and/or use secure network credentials
  - Ability to restrict communications to only authorized entities, as enforced through the onboarded network

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Device Operation**

  Requirements that may be necessary:

  - Ability to keep an accurate internal system time
  - Ability to compare and synchronize internal system time with an organizationally-defined authoritative source
  - 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog
# Device Cybersecurity Capability Catalog

## Device Security

- **Secure Device Operation**

  Requirements that may be necessary (cont'd):

  - 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

# NIST SP800-213A
# IoT Device Cybersecurity Requirement Catalog

## Non-Technical Supporting Capability Catalog

Capabilities

- **Documentation:** The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, disseminate, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle
- **Information And Query Reception -** The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device
- **Information Dissemination -** The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device
- **Education and Awareness -** The ability for the manufacturer and/or supporting entity to create awareness of, and educate IoT device customers about, cybersecurity-related information, considerations, features, and other information related to reducing the risks created by the IoT device being implemented within the IoT customer's digital ecosystem

# Comparison with ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things

| Requirements Category | NIST SP 800-203A | ETSI EN 303 645 |
|---|---|---|
| Device Identification | Yes | No |
| Device Configuration | Yes | No |
| Data Protection | Yes[1] | Yes[2] |
| Logical Access to Interfaces | Yes | No |
| Software Update | Yes | Yes |
| Cybersecurity State Awareness | Yes | No |
| Device Security | Yes | No |
| Password | Yes | Yes |
| Vulnerability Management | No | Yes |
| Secure Parameter Storage[2] | Yes | Yes |
| Secure Communication[2] | Yes | Yes |
| Minimize Attack Surface | No | Yes |
| Software Integrity | No | Yes |
| Securing Personal Data | Yes[1] | Yes |
| System Resiliency (Availability) | No | Yes |
| System Telemetry Data | No | Yes |
| Data Deletion | No | Yes |
| Installation and Maintenance | Yes[3] | Yes |
| Input Data Validation | No | Yes |
| Data (Privacy) Protection | No | Yes |