DRAFT: FEDERAL PROFILE OF NISTIR 8259A: NON-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: Non-Technical Device Cybersecurity Capabilities needed to Support Federal Cybersecurity Controls

Table of Contents

1 IOT Non-Technical Security and Privacy Controls 1
2 Device Identity 2
3 Device Configuration 3
4 Data Protection 5
5 Logical Access to Interfaces 9
6 Software Update 17
7 Cybersecurity Event Awareness 20
8 Device Security 29
9 Device Acquisition and Maintenance 35

IOT Non-Technical Security and Privacy Controls

Non-technical security and privacy controls include such actions and things as:

- Administrative
  - Policies, procedures and standards for the full range of information security and privacy domains
  - Assigned responsibilities
  - Workforce security and privacy (ensuring appropriate access authorizations, separation of duties, clearance to data, onboarding practices, offboarding practices, appraisals, etc.)
  - Training
  - Risk assessments
  - Risk management activities
  - Backup, disaster recovery and contingency plans
  - Emergency mode operations
  - Systems and applications development lifecycles (including testing, revision, change controls, etc.)
  - Vendor management
- Physical
  - Facility access controls
  - Contingency operations (allowing for access to facilities, devices, etc., as part of disaster recovery and emergency mode operations)
  - Maintenance records
  - Workstation/work area use
  - Workstation/work area security and privacy
  - Computing device and digital storage device controls (privacy screens/filters, theft alarms, device physical locks, etc.)
  - Disposal
  - Media re-use
  - Accountability for hardware and software movements, use, etc.
  - Data backup storage

These types of non-technical security and privacy controls and activities should be considered for the use of IOT devices within organizational systems.

Throughout this document references to policies and procedures include the need to have them documented and maintained, even if not explicitly stated.

Device Identity

The management and operational controls to support device identity capabilities to configure and use the IoT device according to the requirements established by the organization.

Policies and procedures requiring unique identification for each IoT device.

Policies and procedures provide the details necessary to implement management and operational controls for required unique identification for each IoT device associated with the system and critical system components within which it is used. Controls that may be necessary:

Manufacturer:

- Provides capabilities within the IoT device to allow for unique identification of each IoT device.
- Provides instructions for implementing and using the unique IoT identifiers.
- Provides training videos showing how to implement unique identifiers for the IoT device.

Agency:

- Organizational IoT device policies and procedures establish the unique identification required for each IoT device associated with the system and critical system components within which it is used.

Device Configuration

The management and operational controls to support the capabilities to configure the IoT device according to the requirements established by the organization.

Policies and procedures establish the minimum requirements for IoT device configuration settings.

Policies and procedures detail the necessary management and operational controls to support configuration of the IoT device's software, to ensure the configuration can be securely changed, and to ensure such changes can be performed only by authorized entities. Controls that may be necessary:

Manufacturer:

- Provide documentation detailing the minimum configuration settings available within the IoT device, and how to change those settings, to meet their customers' needs and requirements.
- Provide a process by which customers can contact the manufacturer to ask questions or obtain help related to the minimum requirements for the IoT device configuration settings.

Agency:

- Establish the requirements for configuration settings to meet policies and procedures governing the associated IoT devices based upon their roles and functions within the associated systems.
- Assign roles and responsibilities for ensuring IoT devices are configured with the appropriate configuration settings before implementation within the system. For example, ensuring default passwords are changed before implementing the device into production.

Training is provided to workers covering the IoT device configuration requirements.

Policies and procedures establish the training necessary for individuals responsible for implementing the policies and procedures for the minimum required IoT device configuration settings. Controls that may be necessary:

Manufacturer:

- Provide documentation to the IoT device customers explaining how to configure the devices, and related actions to take with the devices.

- Provide training (e.g., in person, online webinar, video, etc.) to the IoT device customers to teach them how to configure the devices, and perform related actions.

Agency:

- Establish policies and procedures for providing training to the roles responsible for configuring IoT devices.
- Ensure the personnel responsible for configuring the IoT devices are provided with training covering how to appropriately configure the devices.

Data Protection

The management and operational controls to support securing IoT device data according to organizationally-defined requirements.

Policies and procedures for IoT device data security roles.

Policies and procedures provide the details necessary to implement management and operational controls for establishing roles and responsibilities for IoT device data security. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with documentation describing the IoT device capabilities for role-based controls, to establish different roles within the IoT device.

Agency:

- Use the manufacturer documentation to establish policies and procedures for IoT device data security and privacy organizationally-defined roles and responsibilities. Some examples: Roles to authorize IoT devices, roles to audit IoT devices, etc.
- Create and provide training to those who will be responsible for using the IoT devices to teach them how to set and change the role-based settings.

Policies and procedures for IoT device data integrity.

Policies and procedures provide the details necessary to implement management and operational controls to support IoT device and associated systems data integrity, including establishing the purpose, scope, roles, responsibilities, management commitment, and coordination of IoT devices among organizational entities, and the associated compliance activities. Controls that may be necessary:

Manufacturer:

- Provide information to the IoT device customer for the role or position within the organization that is responsible for determining the security and privacy regulatory requirements with which the IoT device capabilities must comply.

Agency:

- Implement IoT device and associated systems information integrity policies and procedures that govern establishing the purpose, scope, roles, responsibilities, management commitment, and coordination of IoT devices among organizational entities, and the associated compliance activities.

- Provide training covering the IoT device purpose, scope, roles, responsibilities, management commitment, and coordination of IoT devices among organizational entities, and the associated compliance activities.
- Perform periodic audits to ensure compliance with the policies and procedures.

Policies and procedures to establish IoT device data integrity controls.

Policies and procedures provide the details necessary to implement management and operational controls that support secure implementation of the IoT device and associated systems data integrity controls. Controls that may be necessary:

Manufacturer:

- Provide the IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them.
- If there are no data integrity controls built into the IoT device, explain to IoT device customers the ways to achieve IoT device data integrity.

Agency:

- Document the data integrity capabilities for each of the associated IoT devices, such as for validating accuracy of input data, and how to ensure data integrity if this action is not part of the device's technical capabilities.

Policies and procedures for maintaining IoT device data integrity during software modifications.

Policies and procedures provide the details necessary to implement management and operational controls for reviewing and updating the current IoT device and associated systems while preserving data integrity. Controls that may be necessary:

Manufacturer:

- Provide information to IoT device customers detailing the trigger events that result in updates to their IoT devices.
- Establish a process to consistently provide communications about updates and possible impacts to data integrity (e.g., alerting users if an update will delete data) to their IoT device.

Agency:

- Implement a policy and procedure to review and update the current IoT device and associated systems at a minimum-established organizationally-defined frequency, and following organizationally-defined trigger events while preserving data integrity.

Policies and procedures for IoT device data handling and retention.

Policies and procedures provide the details necessary to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device, in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Controls that may be necessary:

Manufacturer:

- Provide documentation to IoT device customers describing how to wipe/delete data from the IoT device.
- Provide information to IoT device customers describing how to protect device data from being accidentally modified.

Agency:

- Implement policies and procedures establishing the requirements for:
    - Securely handling IoT devices to prevent loss, theft and damage.
    - Physical access security to IoT devices.
    - Allowing for removable storage devices to be inserted into IoT devices.
    - Securely retaining IoT devices, and associated systems, after they are no longer used, along with documentation detailing the associated retention time requirements.
    - Securely retaining IoT device data within the associated information systems, and data output from the IoT device, in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
    - Appropriately marking or labeling device hardware to support distribution, handling, or dissemination of IoT devices throughout the organization.
- Implement policies and procedures for secure disposal of IoT device hardware, software and data following expiration of the established retention periods.
- Provide training to those responsible for IoT device retention and disposal.
- Perform periodic audits for the IoT device retention and disposal policies and procedures.

Policies and procedures establishing IoT data backup.

Backup and recovery policies and procedures detail how to make backups of IoT device data and software as applicable. Controls that may be necessary:

Manufacturer:

- Provide instructions describing how to backup data on the IoT device.
- Communicate and demonstrate (e.g., directly in person, in videos, in an online webinar) how to backup up the IoT device.

Agency:

- Incorporate the requirements for creating IoT device backups into the existing organizational computing and storage device backup policies.
- Incorporate the procedures for including IoT device backups into the existing set of organizational backup procedures.

Policies and procedures for removing all data from IoT devices prior to maintenance and repairs.

Policies and procedures provide the details necessary to implement management and operational controls for when and how to remove all data from IoT devices prior to removing the devices from facilities for offsite maintenance or repairs. Controls that may be necessary:

Manufacturer:

- Provide information about how to use the IoT device capabilities to remove all data from the device.
- Provide clear communications about the IoT device these capabilities and procedures to customers.

Agency:

- Implement policies and procedures governing the timeframes within which data must be removed from IoT devices prior to being removed from organizational facilities.
- Implement procedures to follow to remove all data from IoT devices

Logical Access to Interfaces

The management and operational controls to support secure IoT device interface capabilities according to the requirements established by the organization.

Policies and procedures for access control capabilities.

Policies and procedures provide the details necessary to implement management and operational controls to support the organizational access control requirements on IoT devices. Controls that may be necessary:

Manufacturer:

- Provide information to the IoT device customer describing the needs the manufacturer will have to access the IoT device interfaces for support, updates, ongoing maintenance, etc.
- Provide documentation to the IoT device customer describing any requirements for the manufacturer to collect data from the IoT device.
- Provide documentation with instructions for the IoT device customer to follow describing how to restrict interface connections that enable specific activities.
- Prior to purchase and/or implementation provide descriptions of the types of access to the IoT device the manufacturer will require on an ongoing or regular basis.
  - Some examples: medical devices, smart refrigerators, HVAC devices, IoT device maintenance data, etc.

Agency:

- Establish policies and procedures to govern the implementation of the organizational access control requirements on IoT devices.
- Establish policies and procedures for:
  - Using discovery tools to identify IoT devices implemented within the system.
  - Governing how IoT devices are reported to the agency before integration within the system is allowed.
  - Steps to follow for how the agency looks for stray and unauthorized devices that have been implemented within the network.
- Establish the organizationally-defined roles responsible for implementing authorized IoT devices within the system.
- Provide training for how to securely establish IoT device interfaces and connections to the manufacturer for any requirements from the manufacturer requiring such connections.
- Establish right-to-audit clauses within IoT device manufacturer contracts where periodic or ongoing access to IoT devices is required.

Policies and procedures for situations where identification and authentication are not needed.

Policies and procedures provide the details necessary to implement management and operational controls to support the organizational requirements for determining circumstances when identification and authentication are not needed to be used with IoT devices for specified organizationally-defined user actions. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with a description of the privacy protection capabilities built within the IoT device that do not require authentication, such as encryption, authentication, access control, data deletion, etc.
- Provide IoT device customers with a description for how to access the IoT device through the interface without authentication, as applicable to the purpose of the device. For example, when visitors need to be able to access certain IoT devices without needing to authenticate, such as when asking the IoT device for the location of a doctor's office within a health clinic.

Agency:

- Establish policies and procedures describing:
  - The organizationally-defined roles that can use the IoT device without identification and authentication.
  - Situations where the IoT device can be used by anyone, and roles do not need to be defined. -Example: A National Park IoT device where visitors are able to ask questions, and then the IoT device provides answers. The identities of persons asking questions are not collected (a privacy control), but the questions asked may be logged/recorded to determine topic interests.
- Establish policies and procedures describing situations for when certain features can be used for the IoT device without authorization by an organizationally-defined role or individual.
  - Example: using a smart coffee maker in an agency's break room.
  - Include within the policies and/or procedures a description of the compensating controls necessary in such situations, such as the need to be physically present for the use of the IoT device, the requirement to lock the door to the room where the device is located after normal business hours, etc.

Policies and procedures for managing role-based access controls.

Policies and procedures provide the details necessary to implement management and operational controls in situations where access controls are not necessary on an individual basis, but are based on the role of the IoT device user. Some examples: - Anyone within the office can use the smart coffee maker as part of a “general use” type of role, but only those within the “admin” type of role can modify the smart coffee maker settings. - A device can be configured to allow anyone with access to the device to view information in a public space, e.g., a public kiosk. However, the device has an “admin” type of role that allows only those within that role to make changes to the device.

Controls that may be necessary:

Manufacturer:

- Provide to the IoT device customer a description of the role-based access capabilities built within the IoT device, such as admin, general user, etc.
- Provide to the IoT device customer instructions for how to establish and change role-based access settings.
- Provide to the IoT device customer a description of the role-based access capabilities of the IoT device. If this capability is not available through the IoT device, document this limitation.

Agency:

- Establish policies and procedures describing:
  - The roles that can use IoT devices without using authorization.
  - Situations where IoT devices can be used by anyone, and roles do not need to be defined. For example: A National Park IoT device where visitors are able to ask questions, and then the IoT device provides answers. The identity of the person asking is not collected (a privacy control), but perhaps the question itself is logged/recorded to determine topic interests.
- Establish policies and procedures describing situations when specified features can be used for the IoT device without authorization by a role or individual.
  - For example, turning on a smart coffee maker in an agency’s break room.
  - Include within the policies and/or procedures a description of the compensating controls necessary in such situations, such as the need to be physically present for the use of the IoT device. For example, requiring a user to be physically at the coffee maker to turn the coffee maker on.

Policies and procedures for including security and privacy requirements in third party contractual agreements.

Policies and procedures provide the details necessary to implement management and operational controls for including security and privacy requirements within third party contractual agreements that involve access to, and/or use of, the IoT device by third parties. Controls that may be necessary:

Manufacturer

- Include within the IoT device customer contracts a description and listing of the third parties used by the manufacturers that will have access to the IoT device and/or the data collected, generated, accessed, processed, or shared through the device, and a description of the associated security and privacy controls established for such third parties.
- Provide the IoT device customers with documentation detailing all the cloud services used to support the use of the IoT device.
- Describe to the IoT device customers all logical interfaces to the IoT device and document the interfaces used by the manufacturer's third parties, and the purposes for such uses.
- Communicate to the IoT device customers:
  - A list of the third parties to whom the manufacturer provides the IoT device data and/or customer information, and
  - The types of data provided to the third parties directly by the device (e.g., device usage, entities using the device, device location, personal data, etc.).
- Describe to the IoT device customers other types of devices, systems, etc., that will be accessing the manufacturer's IoT device during customer use of the device, and how they will be accessing it. Some examples: Using static IP addresses, using device identifiers, etc.
- Provide to the IoT device customers documentation, in contracts, disclosures and/or similar types of documents, for the actions the manufacturer will take for requested modification of interface capabilities, and describe how device customers should make such requests.
- Describe to the IoT device customers how the IoT device customers will be notified of changes in the manufacturer's contractors and third parties that have access to the IoT devices, when the origination or locations (e.g., city, state, country) of the contractors or third parties change, and other related types of contractor and third-party changes.
- Describe to the IoT device customers the methods by which the manufacturer prevents unauthorized access to the customer's IoT device by third parties not listed on the provided documentation.
- Describe to the IoT device customers how third parties are, or can be, prohibited from accessing the IoT device and/or restricted in their access to the device.
- Provide to the IoT device customers documentation describing the expected or typical lifespan of the IoT device, and the associated support that will be provided for the device manufacturer during this time.

- Disclose to Federal agencies how the IoT device supports the Federal Risk and Authorization Management Program (FedRAMP) requirements.

Agency:

- Establish policies and procedures governing the security and privacy requirements that must be included in IoT device manufacturer's third-party contractual agreements that involve access to, and/or the use of, the IoT devices by third parties.
- Establish policies and procedures:
  - Describing the risk evaluation requirements and practices for requested IoT devices, and descriptions for how risk levels will be established for the level of risk the device brings into the system.
    - NOTE: Often the IoT devices will be used within large systems built for the government, so the interface to the IoT device within the system will need to be used based on the risk levels within the system, and for the risk the IoT device presents to the system.
  - Detailing the documentation requirements for third-party disclosure of IoT device use and data from the manufacturer, and the required types of security and privacy reviews of those disclosures and the related manufacturer documentation to collect that describe those disclosures, that must be performed by each agency.
  - Detailing the acceptable and unacceptable types of contractors (based upon related risk factors such as data use, location of the contractors, etc.), and the acceptable and unacceptable types of data sent out from the device. Some examples: personal data, intellectual property, data impacting homeland security, etc.
  - Detailing any requirements for IoT device manufacturers to ensure they are using FedRamp-approved cloud service providers for their back-end cloud service platforms.
  - Details for working with IoT device manufacturers on possible modification of IoT device interface capabilities for the agency considering use of the manufacturer's IoT device.
  - Details for implementing compensating controls for IoT devices used that do not have IoT device manufacturer support for IoT device interface software, firmware or hardware.
- Establish policies and procedures to perform a cost/benefit analysis prior to implementing the IoT device.
- Establish policies and procedures to verify the existence of disaster recovery policies and procedures within IoT device manufacturers' practices and documentation. Such disaster recovery documentation should include:
  - Descriptions of existing dependencies on third parties.
  - Restrictions obtaining documentation about third party dependencies.

- Listings of acceptable and unacceptable contractors and other types of third parties.

Policies and procedures for device interface controls.

Policies and procedures provide the details necessary to implement management and operational controls for the necessary logical and remote access IoT device controls through device interfaces for information transmission between devices and subjects, objects, systems and components within the system. Controls that may be necessary:

Manufacturer:

- Provide to IoT device customers documentation describing the IoT device logical and remote interface access controls.
- Describe to IoT device customers how to restrict access to the IoT device interface in terms of both users of the interface and data that can be transmitted through that interface, and on what basis restrictions can be defined.
- Disclose to IoT device customers the manufacturer's own policies governing how they share the data obtained from the manufacturer's IoT device.

Agency:

- Establish policies and procedures:
  - Governing risk evaluation for IoT devices, including how risk levels will be established for the risks the device brings into the system.
  - Establishing the required documentation from IoT device manufacturers for the available logical and remote interface access controls, and the required controls to allow usage of the IoT device within agency systems.
  - Describing the acceptable and unacceptable types of data that can be sent through each IoT device interface, and the controls that need to be implemented to meet the restrictions.
  - Governing how to work with manufacturers on possible modifications of interface controls for IoT devices.
  - Establishing the requirements for role-based access controls for specific types of Iot data.
  - Governing the types of compensating controls that should be use when an IoT device manufacturer will not make changes or provide support for IoT device interfaces to support necessary security controls.

Policies and procedures for required authentication techniques.

Policies and procedures establish the capabilities necessary to support required IoT control techniques, such as PIV authentication. Controls that may be necessary:

Manufacturer:

- Discloses to IoT device customers details about the IoT device interface controls, and descriptions for if and how a second factor for authentication can be implemented.

Agency:

- Policies and procedures require strong IoT device authenticators, which are documented and maintained.
- IoT device requirements will include the following, as applicable to each situation:
  - Organizationally-defined roles that require a second factor for authentication, and defining situations when a second factor must be a PIV or a PIV-derived credential.
  - Descriptions of the available logical and remote interface access controls for second factor authentication from IoT device manufacturers that must be reviewed by specified organizationally-defined agency roles.
  - Descriptions of the compensating controls to use if PIV card readers or use of a PIV-derived credential is not possible.

Policies and procedures for implementing only products in the NIST-approved products list.

Policies and procedures provide the details necessary to implement management and operational controls to allow the use of only IoT devices within the organizational system that are on the Federal Information Processing Standards (FIPS) 201 approved products list for Personal Identity Verification (PIV) capability, as applicable to the use and purpose for each IoT device, unless allowed by the organizational security policy or appropriate management approval. Controls that may be necessary:

Manufacturer:

- Provides documentation describing how the IoT device can technically support PIV card implementation, accessibility and interfaces.
- If the IoT device cannot support PIV cards, they provide information with suggested ways in which customers can implement compensating controls around the IoT device.
- Provides training videos showing how to configure the IoT device to technically support PIV implementation, accessibility and interfaces.
- Provides instructions for how to integrate the IoT device with a PIV system. Or, provides some type of attestation that their IoT device can be used in compliance with Federal agency requirements, with associated descriptions for how the agency can accomplish this.

Agency:

- Policies and procedures provide the requirements for how to use IoT devices
  - That have PIV card support provided by the manufacturer.
  - That do not have PIV card support by the manufacturer.
- Training provides the information to roles responsible for implementing IoT devices that need to support PIV capabilities.
- Establish processes to communicate with IoT device manufacturer about any problems or to ask any questions about IoT devices and related support of PIV cards.

Software Update

The management and operational controls to support secure IoT device software updates.

Policies and procedures to identify, report, and correct IoT device system flaws.

Policies and procedures provide the details necessary to implement management and operational controls for how to identify, report, and correct IoT device system flaws. Controls that may be necessary:

Manufacturer:

- Communicate and provide to IoT device customers instructions for sending the manufacturer flaw reports.
- Communicate and provide to IoT device customers a description of the procedures followed for processing the flaw reports, determining which flaws need to be fixed, and for correcting identified flaws.
- Communicate device remediation efforts with stakeholders and IoT device customers.

Agency:

- Implement policies and procedures for identifying and reporting IoT device flaws to the manufacturer.
- Follow documented procedures to receive IoT device remediation reports from manufacturers.

Policies and procedures for incorporating IoT device flaw remediation into the configuration management process.

Policies and procedures provide the details necessary to implement management and operational controls for incorporating IoT device flaw remediation into the organizationally-defined configuration management process. Controls that may be necessary:

Manufacturer:

- Communicate to the IoT device customers the processes that will be followed to communicate the IoT device remediation efforts with stakeholders (IoT device customers, users, etc.).

Agency:

- Implement policies and procedures for receiving and responding to IoT device remediation reports from manufacturers.
- Implement policies and procedures for incorporating flaw remediation reports from IoT device manufacturers into the organizationally-defined configuration management processes.

Policies and procedures for software updates for flaw remediation.

Policies and procedures provide the details necessary to implement management and operational controls for how to establish the types of tests necessary for IoT device and related system software updates related to flaw remediation, for effectiveness and potential side effects before installation. Controls that may be necessary:

Manufacturer:

- Communicate to IoT device customers and other stakeholders the types of security and privacy tests necessary for the IoT device and software before installation.

Agency:

- Implement policies and procedures for receiving IoT device and software test information from manufacturers.
- Implement policies and procedures for testing IoT devices following updates for effectiveness and determining potential side effects.
- Incorporate IoT device manufacturer-recommended tests into organizationally-defined configuration and/or change management processes.

Policies and procedures for security-relevant software updates.

Policies and procedures provide the details necessary to implement management and operational controls for the installation of IoT devices and associated systems security-relevant software updates within an organizationaly-defined time period from the vendor release of the updates. Controls that may be necessary:

Manufacturer:

- Provide information to IoT device customers and stakeholders regarding the criticality of IoT device software and hardware updates, and the recommended time period within which the update should be installed.
- Communicate to IoT device customers and other stakeholders IoT device system environment dependencies or potential impacts for the updates.

Agency:

- Implement policies and procedures governing the time period within which IoT device manufacturer-supplied updates should be installed.
- Incorporate the IoT device update procedures within organizationally-defined configuration and/or change management procedures.
- Implement policies and procedures for testing IoT devices following software updates for effectiveness and determining potential side effects.

Cybersecurity Event Awareness

The management and operational controls to support reporting the IoT device cybersecurity state and associated security events within the system where the IoT device is used. Controls that may be necessary:

Policies and procedures govern malicious code protection.

Policies and procedures provide the details necessary to implement management and operational controls for malicious code protection in the IoT device and associated systems, as well as within related systems entry and exit points, to detect and eradicate malicious code. Controls that may be necessary:

Manufacturer:

- Provide information to the IoT device clients/customers that describe the vulnerabilities to malware for the associated IoT devices, and advice for the best types of anti-malware to use. If no anti-malware is needed for the IoT device, explain why.
- Provide information about the IoT device resource restraints related to malicious code protection and possible compensating controls that IoT device customers can use for such restraints.

Agency:

- Implement policies and procedures requiring IoT devices, and associated systems, to have malicious code protection mechanisms integrated into IoT devices and related systems entry and exit points that can detect and eradicate malicious code.
- Follow procedures to use IoT device anti–malware tools based upon the types of malware possible to be loaded onto each associated IoT device.
- Establish, or assign to existing, roles within the organization responsibilities for ensuring anti-malware is implemented appropriately within IoT devices used within the organizational systems.

Policies and procedures govern malicious code protection updates.

Policies and procedures provide the details necessary to implement management and operational controls for how to update IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures. Controls that may be necessary:

Manufacturer:

Provide information to the IoT device clients/customers that describe newly identified vulnerabilities for malware for the associated IoT devices.

Agency:

- Implement policies and procedures to govern how to update IoT device and related systems malicious code protection mechanisms whenever new releases are available, in accordance with organizational configuration management policy and procedures.
- Require the appropriate roles to subscribe to available notifications for anti-malware updates from the manufacturer or the software provider, as appropriate.

Policies and procedures govern malicious code protection configurations.

Policies and procedures provide the details necessary to implement management and operational controls for how to configure malicious code protection mechanisms in IoT devices and related systems. Controls that may be necessary:

Manufacturer:

- If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should provide documentation to the IoT device customers describing:
  - How to schedule automatic scanning on the IOT device.
  - How to perform real-time scanning for new files introduced through the IoT device interfaces.
  - How to block and/or quarantine malicious code to allow for inspection of that code by customer organizational roles with those responsibilities.
  - How to configure the IoT device to shut-down upon detecting malicious code, as appropriate to the purpose of the IoT device.
- Provide information to IoT device customers describing the operational impacts of the anti-malware activities on mission critical processes in the system where the IoT device is used.
  - Provide additional information on recommended responses to malware beyond just shutting down the IoT device.
  - Provide options for responding to malicious code identification within the IoT device. Some examples: shutting down, redirecting the network traffic, sending alerts, logging the events, etc.

Agency:

Implement policies and procedures to govern how to configure malicious code protection mechanisms in IoT devices and related systems to: - Perform periodic scans of the IoT devices and associated systems on an ongoing basis. - Perform real-time scans of files from external sources at IoT device interfaces, and associated systems entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policies. - Block and/or quarantine malicious code and send an alert to the organization administrator, as well as shutting down the IoT device if appropriate, in response to malicious code detection.

Policies and procedures for malicious code detection and eradication.

Policies and procedures provide the details necessary to implement management and operational controls for malicious code detection and eradication. Controls that may be necessary:

Manufacturer:

- If the IoT device manufacturer provides anti-malware tools for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should:
  - Document how the IoT device user should address false positives and report the false positives to the manufacturer.
  - Document the possible availability and functioning impacts on the associated IoT device and the system within which it is implemented.

Agency:

- Implement policies and procedures to perform periodic scans of the IoT devices and related systems, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with the organizational security policy.
- Implement policies and procedures to block malicious code; quarantine malicious code; and send alerts to admin roles.
- Implement policies and procedures governing how to identify and respond to malware false positives for IoT devices, and how to identify and resolve any potential impacts to the associated IoT device and associated systems.
- Implement policies and procedures establishing how to address the receipt of false positives during IoT device and associated systems malicious code detection and eradication, and the resulting potential impact on the availability of the IoT device and associated systems.

Policies and procedures for information system monitoring.

Policies and procedures provide the details necessary to implement management and operational controls for how to monitor IoT devices and associated systems. Controls that may be necessary:

Manufacturer:

- Provide documentation to IoT device customers:
  - Describing all the ways in which the IoT device can be monitored, and the recommended associated tools to perform monitoring.
  - Describing the indicators of attacks on the IoT device.
  - Describing how to identify local, network and remote IoT device access attempts and connections.
  - Describing expected behavior of the normal operation of the IoT device.
  - Describe IoT device behavior indicators that could occur when an attack is being launched.

Agency:

- Establish or assign to existing roles within the organization responsibilities for monitoring access to IoT devices and associated systems, identifying suspicious and malicious access, and for reacting appropriately.
- Establish policies and procedures to monitor IoT devices and associated systems to detect:
  - Attacks and indicators of potential attacks in accordance with organizationally-defined monitoring policies and objectives.
  - Unauthorized local, network, and remote IoT device, and associated systems, connections.

Policies and procedures to identify unauthorized use.

Policies and procedures provide the details necessary to implement management and operational controls for how to identify unauthorized use of IoT devices and their associated systems, in accordance with the organizationally-defined techniques and methods. Controls that may be necessary:

Manufacturer:

- Provide documentation to the IoT device customers that describes indicators of unauthorized use of the IoT device.

Agency:

- Establish or assign to existing roles within the organizational responsibilities for identifying unauthorized use of IoT devices and associated systems and for reacting appropriately.
- Implement policies and procedures to establish how to identify unauthorized use of IoT devices and their associated systems, in accordance with the organizationally-defined techniques and methods.

Policies and procedures for monitoring devices and tools.

Policies and procedures provide the details necessary to implement management and operational controls for how to deploy monitoring devices and tools for IoT devices and associated systems. Controls that may be necessary:

Manufacturer:

- Provide documentation to the IoT device customers describing how to best implement and secure the IoT device and associated systems monitoring.

Agency:

- Establish or assign to existing organizational roles responsibilities for monitoring use of IoT devices within the organization.
- Implement policies and procedures to govern how to deploy monitoring of IoT devices and associated systems to collect organizationally-defined essential information:
  - Strategically within IoT devices.
  - In information systems where IoT devices are used.
- Implement policies and procedures to govern how to deploy monitoring of IoT devices and associated systems in ad hoc locations to track specific types of transactions of interest to the organization.

Policies and procedures for protecting cybersecurity event information from unauthorized access, modification, and deletion.

Policies and procedures provide the details necessary to implement management and operational controls for protecting information obtained from IoT devices, and associated systems and intrusion-monitoring tools, from unauthorized access, modification, and deletion. Controls that may be necessary:

Manufacturer:

- Provide documentation to IoT device customers describing the types of usage and environmental systems data that can be collected from the IoT device.

Agency:

- Establish or assign to existing organizational roles responsibilities for collecting, securing and analyzing organizationally-defined data of interest from IoT devices and associated systems.
- Develop policies and procedures to establish the requirements for protecting information from unauthorized access, modification, and deletion that was obtained from IoT devices and associated systems using intrusion-monitoring tools.

Policies and procedures for security level changes.

Policies and procedures provide the details necessary to implement management and operational controls to govern when to heighten the level of security for an IoT device and associated systems. Controls that may be necessary:

Manufacturer:

- Provide documentation to IoT device customers describing the security controls and monitoring capabilities built within the IoT device, and how to configure the device to best fit the risk levels within the systems where they are used.

Agency:

- Establish policies and procedures to govern when to increase the level of security for an IoT device and associated systems, including for monitoring activity, whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Policies and procedures for ensuring legal compliance.

Policies and procedures provide the details necessary to implement management and operational controls for establishing whether the IoT device, and associated systems, monitoring activities are in compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations. Controls that may be necessary:

Manufacturer:

- Provide the legal (Federal regulations, state and local laws) requirements for security and privacy controls that the IoT device supports. Some examples: Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), EU General Data Protection Regulation(GDPR).

Agency:

- Establish policies and procedures for determining if the monitoring activities for IoT devices and associated systems are in compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

Policies and procedures for providing monitoring information to authorized personnel or roles.

Policies and procedures provide the details necessary to implement management and operational controls for how to provide organizationally-defined IoT device and associated systems monitoring information to authorized personnel or roles as needed and according to organizationally-defined frequencies. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools.

Agency:

- Establish policies and procedures to govern how to provide organizationally-defined IoT device and associated systems monitoring information to authorized personnel or roles as needed and according to organizationally-defined frequencies.

Policies and procedures for receiving external security alerts, advisories, and directives.

Policies and procedures provide the details necessary to implement management and operational controls for how and when to receive up-to-date security and privacy information on an ongoing basis about IoT devices and associated systems, such as information system security alerts, advisories, and directives from IoT device manufacturers, information security researchers, and other sources the organization determines to be valuable. Controls that may be necessary:

Manufacturer:

- Provide documentation to the IoT device customers about related security and privacy updates, such as IoT device information system security and privacy alerts, advisories, directives, security and/or privacy research, and other information that would be valuable for IoT device customers to help ensure security and privacy of the IoT device.

Agency:

- Establish policies and procedures to govern how and when to receive up-to-date security and privacy information on an ongoing basis about IoT devices and associated systems, such as information system security alerts, advisories, and directives from IoT device vendors, information security researches, and other sources the organization determines to be valuable.

Policies and procedures for receiving internal security alerts, advisories, and directives.

Policies and procedures provide the details necessary to implement management and operational controls for when and how to generate internal security alerts, advisories, and directives about the IoT devices. Controls that may be necessary:

Manufacturer:

- Provide necessary information to customers to inform the review and update of the IoT device systems and services practices.

Agency:

- Establish policies and procedures to govern when and how to generate internal security alerts, advisories, and directives about the IoT devices, and associated systems, used within the organization as deemed necessary.

Policies and procedures for disseminating privacy and security alerts, advisories, and directives outside of the organization.

Policies and procedures provide the details necessary to implement management and operational controls to disseminate privacy and security alerts, advisories, and directives about the IoT devices, and associated systems outside of the organization. Controls that may be necessary:

Manufacturer:

- Provide necessary information to IoT device customers to inform the review and update of the IoT device systems and services practices.

Agency:

- Establish policies and procedures to disseminate privacy and security alerts, advisories, and directives about the organizational IoT devices, and associated systems to appropriate organizationally-defined personnel and roles, and to organizationally-defined external organizations.

Policies and procedures for implementing security control directives.

Policies and procedures provide the details necessary to implement management and operational controls to govern the implementation of IoT device and associated systems security directives in accordance with established time frames, and/or to notify the IoT device manufacturer and/or vendor of the degree of noncompliance. Controls that may be necessary:

Manufacturer:

- Provide directions and procedures to IoT device customers for how to submit questions and requests for information about their IoT device related to security and privacy compliance requirements. Some examples: Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), EU General Data Protection Regulation(GDPR).
- Include a timeframe within which such IoT device compliance questions and requests will be answered.

Agency:

- Establish policies and procedures to govern the implementation of IoT devices and associated systems security directives in accordance with established compliance requirements, including time frames, and/or notices to the IoT device manufacturers and/or vendors of the degree of noncompliance.

Device Security

The management and operational controls to support IoT device security.

Policies and procedures provide the details necessary to implement management and operational controls for IoT device security.

Policies and procedures govern IoT device security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, description of the information system development environment and environment in which the IoT device and associated system is intended to operate, and acceptance criteria in the acquisition contracts for every IoT device system, system component, or information system service in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with information about the IoT device security capabilities, security strength capabilities, and security assurance capabilities.

Agency:

- Implement policies and procedures governing the required security and privacy capabilities for IoT devices and their incorporation into the systems and services acquisition processes.
    - Policies and procedures providing the details necessary to implement management and operational controls for IoT device functional security requirements, security strength requirements, security assurance requirements.
    - Policies and procedures detailing the security-related documentation requirements.
    - Policies and procedures detailing the requirements for protecting security-related documentation.
    - Policies and procedures detailing the description of the information system development environment and environment in which the IoT device and associated system is intended to operate.
    - Policies and procedures detailing the acceptance criteria in the acquisition contracts for every IoT device system, system component, and information system service in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

Policies and Procedures for IoT device management within a system development life cycle.

Policies and procedures provide the details necessary to implement management and operational controls for 1) how the organization manages the IoT information system ecosystem using the organizationally-defined system development life cycle's associated information security considerations, 2) the individuals with assigned IoT device information security roles and responsibilities, and 3) integrating the organizational information security risk management process. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with the means and the documentation for implementing a hierarchy of privilege levels, that have different permissions for each privilege role responsibility within the information system, into the IoT device and/or necessary associated information systems.

Agency:

- Implement policies and procedures governing the use of a hierarchy of different roles within the IoT devices and associated information system to help ensure appropriate actions are restricted to appropriate users/roles.

Policies and procedures for IoT device vendor security requirements and documentation.

Policies and procedures provide the details necessary to implement management and operational controls for establishing the requirements for IoT device manufacturers to provide documentation for each IoT device and associated system. Controls that may be necessary:

Manufacturer:

- Provide each IoT device customer with the appropriate documentation for the IoT device that is as descriptive and straightforward as deemed necessary by the customers that will use the documentation.

Agency:

- Follow a consistent procedure to communicate with the manufacturer if the IoT device documentation is not sufficient to support integrating the devices into their risk management processes.
- Implement policies and procedures to establish the requirements for IoT device manufacturers and/or vendors to provide documentation for each IoT device and associated system that describes:

  - Secure configuration, installation, and operation of the IoT device.
  - Effective use and maintenance of IoT device security functions and mechanisms.
  - Known vulnerabilities regarding the IoT device configuration and use of administrative (i.e., privileged) functions.
  - IoT device user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
  - Methods for user interaction with the IoT device, to enable individuals to use the IoT device and any associated systems and services in a more secure manner.
  - User responsibilities in maintaining the security of the IoT device.

Policies and procedures for IoT device protections and safeguards documentation.

Policies and procedures provide the details necessary to implement management and operational controls for providing IoT device protections and safeguards documentation as required, in accordance with the organization’s risk management strategy. Controls that may be necessary:

Manufacturer:

- Provide a process to ensure that the appropriate documentation only reaches the IoT customers that purchase the devices, to prevent malicious actors from gaining in-depth knowledge of the devices, and possibly the associated information systems, from the IoT device documentation. For example, IoT device detailed documentation provided to customers should not be posted and publicly accessible on the internet.

Agency:

- Implement policies and procedures to appropriately protect IoT device documentation received from the manufacturer to ensure only employees with appropriate privileges can access and view the documentation.

Policies and procedures for IoT device manufacturers to comply with information security requirements and the organizationally-defined security controls.

Policies and procedures provide the details necessary to implement management and operational controls for IoT device and associated systems providers to comply with organizational information security requirements and the organizationally-defined security controls in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Controls that may be necessary:

Manufacturer:

- Provide the means (tools, assistance, instructions, etc.) for IoT device customers to implement necessary security controls, along with documentation that describes how to configure the devices to implement these controls.
- Provide information to IoT device customers describing how the manufacturer stays up-to-date with regulations, laws, and other legal requirements and standards that apply to IoT devices.

Agency:

- Comply with organizational risk assessment policies and procedures to support secure configuration of IoT devices when integrating them into the larger information system.
- Verify the IoT device configurations of the device and its interactions with the organizational information system before integrating the device into the information system.

Policies and procedures to distribute IoT device policies, procedures and associated documentation.

Policies and procedures provide the details necessary to implement management and operational controls for the organization to distribute IoT device policies, procedures and associated documentation to personnel with information security responsibilities and others as determined appropriate. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with documentation describing recommended device roles and responsibilities to support the ability for IoT device customers to determine to what level in their hierarchy of privileges that the documentation pertains.

Agency:

- Implement policies and procedures to assign appropriate roles to examine IoT device documentation to determine the roles to whom the documentation should be disseminated.

Policies and procedures for organizational oversight.

Policies and procedures provide the details necessary to implement management and operational controls for the organization to define oversight and user roles and responsibilities with regard to IoT devices. Controls that may be necessary:

Manufacturer:

- Provide to IoT device customers the means (tools, assistance, instructions, etc.) to have distinct roles with a hierarchy of privileges established within the IoT device. For example, the ability to assign read-only access to device data for auditors versus full access to the device for admins.

Agency:

- Implement policies and procedures that govern the different roles and responsibilities that IoT devices must be able to support.

Policies and procedures for performing periodic checks and/or audits.

Policies and procedures provide the details necessary to implement management and operational controls to perform periodic checks and/or audits to ensure IoT device security controls are functioning as intended following maintenance and repairs. Controls that may be necessary:

Manufacturer:

- Provide IoT device customers with the means (tools, assistance, instructions, etc.) for the IoT device to support audit and log maintenance and repairs operations.

Agency:

- Implement policies and procedures requiring IoT devices to be configured to properly alert the information system when maintenance and repair operations did not succeed without errors.
- The policy and procedures must include the actions to take when these operations fail, and details for how to control device interactions until these problems are resolved.

Policies and procedures for third party, contractor, and vendor IoT security oversight.

Policies and procedures provide the details necessary to implement management and operational controls for consistently using methods and techniques to monitor IoT device and associated systems security control compliance by external service providers on an ongoing basis. Controls that may be necessary:

Manufacturer:

- Provide appropriate means (tools, assistance, instructions, etc.) for the IoT device to be monitored and/or to report actions to a monitoring service. This could be included in the IoT device logging and auditing procedures.
- Establish a process to take feedback from IoT device customers about whether IoT device logging is sufficient for customers to follow security control compliance procedures required by external service providers.
- Describe how the IoT device meets legal requirements, for the activities of the organizations to whom they outsource activities to support the IoT devices and their IoT device customers through contractual requirements, remote monitoring, and other means.
- Provide auditing and monitoring requirements to the IoT device manufacturer's external service providers that outline and/or describe their responsibilities, the oversight that will be performed, and other relevant information.

Agency:

- Implement procedures to ensure the IoT device users properly implement security controls in compliance with procedures required by external service providers.
- Follow procedures to communicate with IoT device manufacturers when the IoT device is not capable of following these compliance procedures, describing the deficiencies and the actions necessary to meet compliance, along with the effect of non-compliance within the associated information system.
- Ensure proper language is within IoT device manufacturer contracts, and their external service providers, describing how they will monitor compliance, perform audits, etc., as appropriate to the IoT device and control.
- Provide a clear description of the legal compliance requirements to the IoT device manufacturer detailing the compliance needs that must be fulfilled by the IoT device manufacturer to meet all associated compliance requirements, as appropriate to the IoT device and controls.
- Follow procedures to consistently ensure appropriate security and privacy controls language is included within contracts with IoT device manufacturers and service providers.

Device Acquisition and Maintenance

The management and operational controls to support IoT device acquistion and maintenance processes.

Policies and procedures for capabilities necessary for IoT device acquisitions.

Policies and procedures provide the details necessary to implement management and operational controls for the acquisition of IoT devices, systems and services by assigned organizationally-defined personnel or roles who will ensure required device capabilities (compliance and implementation controls, etc.) exist for devices being considered for purchase. Controls that may be necessary:

Manufacturer:

- Provide documentation to potential customers that clearly indicate the IoT device security and privacy capabilities and limitations.

Agency:

- Implement policies governing IoT device, systems, and services acquisition.
- Acquisition policies should include descriptions of required device capabilities, and address the limitations that should be considered in acquisition decisions.

Policies and procedures for review and update of IoT device, systems and services acquisition practices.

Policies and procedures provide the details necessary to implement management and operational controls for the review and update of organizational IoT device, systems and services acquisition practices. Controls that may be necessary:

Manufacturer:

- Provide necessary information to inform the review and update of the IoT device systems, and services acquisition practices by agencies.

Agency:

- Implement policies and procedures to govern the review and update of organizationally-defined IoT device, systems, and services acquisition practices.

Policies and procedures for determining IoT device security requirements as part of the organizational mission/business process planning.

Policies and procedures provide the details necessary to implement management and operational controls for how management roles determine the information security requirements for the IoT device(s) as part of the organizational mission/business process planning. Followed by determining, documenting, and allocating the resources necessary to protect the associated information system to support the organization's capital planning and investment control (CPIC) process. Controls that may be necessary:

Manufacturer:

- Provide potential customers with clear documentation detailing the IoT device capabilities and limitations.
- Provide instructions and/or information describing the recommended means for protecting the IoT device hardware, software and data.

Agency:

- Determine the information security requirements of prospective IoT devices.
- Follow organizational capital planning and investment control (CPIC) processes to allocate sufficient resources to obtain, maintain, and protect the acquired IoT device.
- Update applicable existing policies and procedures as necessary to describe the requirements.

Policies and procedures for establishing a discrete line item for IoT device information security within the organizational programming and budgeting documentation.

Policies and procedures provide the details necessary to implement management and operational controls for establishing a discrete line item for IoT device information security within the organizational programming and budgeting documentation. Controls that may be necessary:

Manufacturer:

- Provide information to IoT device customers detailing all anticipated costs associated with the IoT device, including the purchase, maintenance, operations, security, and disposal costs throughout the potentional lifetime of the use of the IoT device.

Agency:

- Establish expected information security costs for the IoT device.
- Establish separate line items for IoT device information security within the organizational programming and budgeting documentation.

Policies and procedures for maintenance.

Policies and procedures provide the details necessary to implement management and operational controls for the approval and monitoring of onsite and offsite IoT device maintenance activities. Controls that may be necessary:

Manufacturer:

- Clearly indicate to customers before the IoT device purchase the type and nature of the local and/or remote maintenance activities required once the device is purchased and deployed in the organization.
- Communicate the physical and technical capabilities required for these maintenance activities to occur.

Agency:

- Implement policies and procedures governing the approval and monitoring of both local and remote IoT device maintenance activities.
- Communicate these procedures and requirements to the device manufacturer before device purchase. For example, the manufacturer must use unique IDs/passwords for each of their clients, and for each of their workers, etc.
- Integrate these approval and monitoring procedures with the existing organizational procurement and monitoring activities.

Policies and procedures maintaining records for nonlocal IoT device maintenance and diagnostic activities.

Policies and procedures provide the details necessary to implement management and operational controls for maintaining records for nonlocal IoT device maintenance and diagnostic activities. Controls that may be necessary:

Manufacturer:

- Before IoT device purchase clearly indicate through direct communications to potential customers the type and nature of the remote maintenance and diagnostic activities required once the device is purchased and deployed in the organization.
- Communicate to IoT device customers the physical and technical capabilities required for the IoT device maintenance and diagnostic activities.

Agency:

- Implement policies and procedures for maintaining records of remote IoT device maintenance and diagnostic activities.
- Incorporate these procedures into existing organizational monitoring and auditing activities.

Policies and procedures for required maintenance personnel documentation.

Policies and procedures provide the details necessary to implement management and operational controls for IoT device maintenance personnel authorization, record-keeping of maintenance organizations and personnel. Controls that may be necessary:

Manufacturer:

- Before the IoT device purchase provide clear communications to customers describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the organization.

Agency:

- Implement policies and procedures governing IoT device maintenance personnel authorization and record keeping of maintenance.
- Communicate personnel authorization requirements, any necessary restrictions of personnel, and maintenance record keeping requirements to the manufacturer, and any contracted organizations they use, who will be performing IoT device maintenance.

Policies and procedures for IoT device maintenance assigned personnel or roles.

Policies and procedures provide the details necessary to implement management and operational controls to govern IoT device maintenance for assigned organizationally-defined personnel or roles to follow. Controls that may be necessary:

Manufacturer:

- Before the IoT device purchase clearly indicate through documented statements to customers the type and nature of the local and/or remote maintenance activities required once the device is purchased and deployed in the organization.

- Provide documented descriptions of the specific maintenance procedures for defined maintenance tasks.
- Provide training materials to IoT device customers to ensure they understand the requirements for specified maintenance procedures.

Agency:

- Implement policies governing the activities of organizationally-defined personnel who perform IoT device maintenance.
- Distribute maintenance procedures to the organizationally-defined personnel.
- Provide training, as needed, to organizationally-defined maintenance personnel.

Policies and procedures for IoT device systems review and maintenance following trigger events.

Policies and procedures provide the details necessary to implement management and operational controls for required IoT device systems review and maintenance according to organizationally-defined frequency and/or established trigger events. Controls that may be necessary:

Manufacturer:

- Before the IoT device purchase provide customers with the documentation describing suggested frequency of system review and maintenance activities for IoT devices.
- Communicate to IoT device customers the events that will trigger IoT device system review and maintenance.

Agency:

- Implement policies for required IoT device systems review and maintenance according to organizationally-defined frequencies.
- Implement policies for required IoT device systems review and maintenance according to established trigger events defined by the manufacturer.

Policies and procedures govern using only approved IoT device diagnostic tools.

Policies and procedures provide the details necessary to implement management and operational controls for using only organizationally-approved IoT device diagnostic tools. Controls that may be necessary:

Manufacturer:

- Provide IoT customers with documentation describing the tools required for IoT device diagnostics activities.

Agency:

- Implement policies requiring the use of only organizationally-approved tools for performing IoT device diagnostics.
- Implement procedures for granting approval for IoT device diagnostic tools.

Policies and procedures for access authorizations to perform IoT device maintenance activities.

Policies and procedures provide the details necessary to implement management and operational controls for the designated organizational personnel to have required access authorizations to perform unescorted maintenance activities, and for the required personnel with approved access authorizations to supervise maintenance activities of personnel without such authorizations in areas where IoT devices are in use. Controls that may be necessary:

Manufacturer:

- Before the IoT device purchase clearly indicate to customers the type and nature of the local and/or remote maintenance activities required once the device is purchased and deployed in the organization

Agency:

- Implement policies governing the access authorizations required to perform both unescorted and escorted IoT device maintenance activities.
- Develop procedures for personnel to perform both unescorted and escorted IoT device maintenance activities.

Policies and procedures requiring device manufacturers to provide documented specifications for performing IoT device maintenance and repairs.

Policies and procedures provide the details necessary to implement management and operational controls requiring IoT device manufacturers to provide documented specifications for performing IoT device maintenance and repairs for organizations to use to schedule and perform maintenance and repairs. Controls that may be necessary:

Manufacturer:

- Provide comprehensive documentation of the IoT device maintenance operations.
- If such comprehensive IoT device maintenance operations documentation does not exist, clearly communicate to IoT device customers that the user must perform these operations themselves.

Agency:

- Examine IoT device documentation to determine and understand the IoT device maintenance operations provided by the manufacturer.
- If the necessary documented actions are not provided by the manufacturer, then submit a request to the manufacturer to provide such documentations, or to determine if the agency must create a method to perform these procedures themselves.

Policies and procedures for documenting attempts to obtain IoT device components or information.

Policies and procedures provide the details necessary to implement management and operational controls for documenting attempts to obtain IoT device components, or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for employees to follow. Controls that may be necessary:

Manufacturer:

- Obtain input from IoT device customers about the breadth and depth of the technical documentation provided with the IoT device to determine if it is acceptable to support customer needs.
- Provide IoT device customers with procedures detailing how to submit questions about IoT device parts, use, and other related issues.
- Describe how to get components for the IoT device, or how to get the IoT device fixed, when necessary.

Agency:

- Establish policies and procedures that govern the actions employees must take when appropriate documentation or necessary device components are not available.
- If employees are permitted to communicate directly with the IoT device manufacturer, provide instructions for how to appropriately do so, and the documentation necessary for such communications.