Innovation Platform Agency, Japan

JST-RC-03-01-2026

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-3 Conformance Requirements for Network Devices (tentative)

June 2026

Innovation Platform Agency, Japan (IPA)

Table of Contents

1. Introduction

This document is intended for manufacturers and Evaluation Bodies and sets forth specific conformance requirements for satisfying security requirements described in "STAR-3 Security Requirements for STAR-3 Network Devices (JST-SR-03-01-2026)."

2. Concept of the Security Level to be Achieved in STAR-3 under JC-STAR

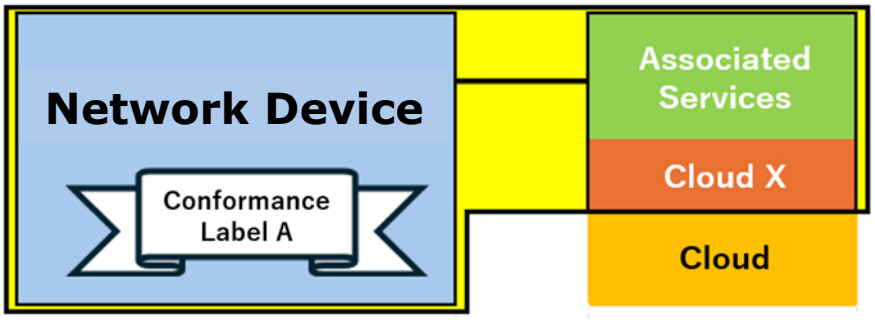
2.1 Concept of Network Devices within the Scope

For STAR-3 Network Devices under JC-STAR (hereinafter referred to as "STAR-3 Network Devices"), the scope of application is defined by referring to "2.1 Main Scope of the STAR-3 Conformance Label (Network Devices)" of the "STAR-3 Security Requirements for Network Devices."

2.2 Concept of "Associated Services"

"IoT products" under JC-STAR refer to products that serve as a unit of being sold by a supplier or being purchased by users, and include either a single "IoT device" designed to achieve its intended purpose, or a complete set consisting of "IoT devices" and "associated services." "Associated services" refer to services that "shall be used as a set" by the target "IoT device." Specifically, they are services that are provided in conjunction with the IoT device in cases [where the IoT device itself cannot provide the purpose intended by the IoT products].

For example, if a Network Device is configured to send and store logs related to communication access to a specific cloud service, the service is considered an associated service. In this case, the scope of evaluation for the conformance label includes the "Network Device," the "cloud service," and the entire communication path connecting the two. Note that the conformance label is granted to the "Network Device."



(Note) Cloud X: The cloud storage space directly utilized by the service

Figure 1: Relationship between IoT devices and associated services

There are no restrictions on the form of the provision of associated services other than the condition that they shall be "provided as a set with the opposing IoT device." For example, associated services may include digital services such as mobile applications, cloud computing/storage, and third-party application programming interfaces (APIs).

Note, however, that if the opposing services to the IoT devices cannot be identified, the services are

considered "external systems" which do not fall under "associated services."

In this document, the distinguishing factor between associated services and external systems is whether the services provided on the system are provided under the control of the IoT device manufacturer. In other words, if services are provided under the manufacturers' control, they are referred to as "associated services"; if they are used under the control of users rather than the manufacturers, they are referred to as "external systems."

2.3 Concept of Security to be Achieved for STAR-3 Network Devices

STAR-3 targets the Network Devices procured and used in critical systems by government agencies, critical infrastructure operators, local governments, and large corporations, with the objective of countering attack methods selected through risk analysis. Therefore, it is assumed that IoT products in operation will be capable of withstanding attacks carried out using generally available tools and specialized expertise (attacks by attackers possessing the attack capabilities defined under the "Enhanced Basic" level of the CEM[1] under the Information Security Evaluation and Certification Scheme).

In light of this objective, the STAR-3 Network Devices covered by these conformance requirements shall implement countermeasures against the following attack methods:

(1) Countermeasures against unintended external access attacks caused by the use of vulnerable passwords

(2) Countermeasures against attacks, including those leading to information leaks, tampering, functional anomalies, or malware infections and attacks using the device as a jump host/jump server, resulting from unpatched vulnerabilities left unaddressed

(3) Countermeasures against attacks, including those leading to information leaks, tampering, functional anomalies, or malware infections and attacks using the device as a jump host/jump server, resulting from unintended external access via unintended interfaces

(4) Countermeasures against attacks involving eavesdropping on sensitive communication information[2]

(5) Countermeasures against attacks in which securely stored information[2] is stolen from discarded or

[1] https://www.enisa.europa.eu/sites/default/files/publications/ENISA_candidate%20scheme_EUCC.pdf
(BACKGROUND INFORMATION, Table B.2, Table B.3)
https://www.ipa.go.jp/security/jisec/about/cdk3vs000000240h-att/CEMV3.1R5-J1.0.pdf
(B.4.2.3 Calculation of Attack Capability)

[2] "Sensitive communication information" and "securely stored information."
For these terms, refer to "2.4 Types of Information Assets to be Protected in STAR-3 Network Devices."

resold devices

(6) Countermeasures against attacks such as network disconnections or power outages that cause anomalies in security functions

(7) Recording of logs, such as audit logs and telemetry data

(8) Countermeasures against attacks on stored secure information

(9) Countermeasures against denial-of-service attacks

(10) Countermeasures against physical attacks

(11) Countermeasures against attacks involving unintended inputs or data

(12) Countermeasures against attacks that launch unintended software

(13) Countermeasures against supply chain attacks

Based on countermeasures against the above attack methods, this document examines the information assets, attack surfaces, threats, and countermeasures primarily assumed for Network Devices, and establishes the "STAR-3 Security Requirements for Network Devices."

This document defines the "STAR-3 Conformance Requirements for Network Devices," which serve as the conditions for satisfying "STAR-3 Security Requirements for Network Devices." Additionally, refer to the "STAR-3 Evaluation Guide for Network Devices" for the evaluation procedures to determine whether these conformance requirements are satisfied.

2.4 Types of Information Assets to be Protected in STAR-3 Network Devices

"Protecting information" has two meanings. The first means "taking measures to prevent security issues, such as unauthorized access or data leaks, from occurring when information that should be protected is leaked to unauthorized parties due to improper disclosure or exposure"; that is, "protecting the confidentiality of information." The other means "taking measures to ensure that information is not relied upon or used despite the fact that its reliability or integrity has been compromised by tampering or forgery, thereby creating a dangerous situation"; that is, "protecting the integrity of information.

Therefore, information that requires protection of either "confidentiality" or "integrity" is referred to as "information assets to be protected." Taking into account the use cases and implementation environments for Network Devices, Table 1 defines the "information assets to be protected" for STAR-3 Network Devices. For these assets, protection of either "confidentiality" or "integrity" is required as necessary for each specific information asset.

Furthermore, "information assets that require confidentiality protection when transmitted via the network" are referred to as "sensitive communication information," and communication via a

communication protocol that employs appropriate encryption is required. The information assets subject to this requirement are specified in Table 1 (1).

"Information assets to be protected that are stored on IoT devices" are referred to as "securely stored information," and appropriate protection of either "confidentiality" or "integrity" is required. The information assets subject to this requirement are specified in Table 1 (2).

Note that Table 1 lists the minimum types of "information assets to be protected" for which secure management is required for all STAR-3 Network Devices; this does not preclude treating other information assets not included in this list as "information assets to be protected" on their own.

Table 1: Types of Information Assets to be Protected in Network Devices

(1) Sensitive communication information, (2) Securely stored information

Legend: ○ indicates included; – indicates excluded

Information assets held by STAR-3 Network Devices	**Information to be protected**	**(1)**	**(2)**
CSP (Critical Security Parameter)	Confidential security-related information whose exposure or tampering could compromise the security of a security module. Examples: secret encryption keys, passwords and other authentication values, PINs, private elements of certificates	○	○
PSP (Public Security Parameter)	Publicly available security-related information which, if tampered with, could compromise the security of security modules. Example 1: Public keys used to verify the authenticity and integrity of software updates. Example 2: Public elements of certificates.	–	○
Configuration information related to communication functions (*1)	Information that shall be configured in advance to prepare for communication. Example: Communication settings: IP address, subnet mask, default gateway, DNS server, domain name, etc. Router configuration function: Routing, QoS, DHCP (server/relay agent), etc. Function settings: HTTP port configuration (HTTP/HTTPS), IEEE 802.1X network access control settings.	○	○

Configuration information related to security functions (*1)	Information that shall be configured in advance to prepare for enabling security functions. Example: Router configuration settings: firewall, VPN, logs, statistics management, etc. Firewall configuration settings: filtering, networks permitted for administrator access, application control, etc. Function-related configuration settings: authentication information (user authentication/host authentication), digital certificates, user privilege settings.	○	○
Alert Information	Signals indicating anomalies in Network Devices, specific details of the anomalies, alert information triggered when detecting security-related anomalies.	○	–
Program code	Software	–	○
Logs (telemetry data, audit logs)	Telemetry data generated while the Network Devices are in operation. (e.g., metrics)	–	○
	Audit logs (including communication logs, event logs, etc.) generated while the Network Devices are in operation (*2).	○	○

(*1): This assumes that communication is required as a prerequisite for enabling the function.

(*2): It is assumed that audit logs on Network Devices refer to communication logs, event logs, etc. Since these audit logs may contain personal information, they are subject to "sensitive information" to be protected.

2.5 Concepts of Secure Storage (Protection Methods)

To ensure the secure storage of the "information assets to be protected" mentioned in the previous section, protection of either "confidentiality" or "integrity," or both are required.

- Protection of "Confidentiality": Protecting information assets to prevent unauthorized disclosure to external parties.
- Protection of "Integrity": Protecting information assets so that they are not forged or tampered with.

For STAR-3 Network Devices, taking into account the operational phase of the Network Devices' lifecycle, one of the following methods is required as a secure means of storing information assets to be protected.

(1) Countermeasures utilizing cryptography. Encryption is required for "sensitive information protection," while digital signatures or message authentication are required for "integrity protection." Note that the cryptography used for protection shall be those specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in

the procurement for the e-Government system (CRYPTREC Ciphers List)" and shall use key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)"

(2) Storage in a sandbox provided by the OS or in the secure area of a security chip.

(3) Storage in an area where direct access to the data is not possible, within a storage area that cannot be easily removed.

2.6 Concept of Secure Communications

For STAR-3 Network Devices, "sensitive communication information" transmitted over a network requires protection of both "confidentiality" and "integrity" as countermeasures against eavesdropping, forgery, and tampering. Furthermore, verification of "authenticity" is required to confirm the validity of the communication destination.

Therefore, the following countermeasures are mandatory for the network in use:

- Countermeasures to verify the validity of the communication destination, or access control functions that allow connections only to valid destinations (e.g., whitelist-based connections).
- Countermeasures to protect "confidentiality" and "integrity" against eavesdropping, forgery, and tampering of sensitive communication information. Note that for this countermeasure, the use of cryptography for end-to-end communication with the destination is mandatory.
- From a "Secure by Default" perspective, the above protection functions shall be enabled by default.

The cryptography and communication protocols used for end-to-end cryptography with the communication destination shall be the cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) and shall use key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

In addition, for STAR-3 Network Devices, if an application is included as one of the associated services and "sensitive communication information" is transmitted from that application, the aforementioned protective measures are also required for that application.

Furthermore, in accordance with the government’s unified standards, wireless LANs are required to encrypt wireless communications and perform device authentication using 802.1x.

2.7 Concept of Handling of Personal Information

Since Network Devices collect audit logs, etc., such information may constitute "personal information" under the Act on the Protection of Personal Information, depending on the purpose of use. Therefore, it is a mandatory requirement for STAR-3 Network Devices to possess functions for security management measures for "personal information."

Specifically, the protection of confidentiality is required for audit logs, etc., both during transmission and storage. In addition, it is required that when storage is no longer necessary, the data shall be deleted using the erasure function at the erasure level required for STAR-3 Network Devices. For details on erasure levels, refer to "Concept of Data Erasure."

2.8 Concept of Data Erasure

For STAR-3 Network Devices, in consideration of information leaks during the "disposal" phase of the lifecycle, a function is required that allows for the deletion of data and configuration information generated during operation before the Network Device is disposed of. According to NIST SP 800-88 Rev.2[3], there are three levels of "deletion," that is "Clear," "Purge," and "Destroy," classified based on the recoverability of the deleted data, but for STAR-3 Network Devices, data shall be deleted at the "Clear" level, which provides a security level capable of protecting against simple, non-invasive data recovery techniques (such as salvage using commercially available data recovery software).

Note that if the device is equipped with an appropriate encrypted erasure function that is enabled by default, data erasure via encrypted erasure shall be treated as equivalent to the "Purge" level.

2.9 Concept of SBOMs

For STAR-3 Network Devices, with the aim of addressing supply chain risks and managing vulnerabilities in third-party components, machine-readable and human-readable SBOM (Software Bill of Materials) shall be created, and a vulnerability management process utilizing the SBOM shall be established.

In these conformance requirements, the scope of SBOM application is defined as "all components used in Network Devices, including third-party components" and "associated services." However, since there are currently no global best-practice standards for creating SBOM, these conformance requirements do not specify the level of detail the SBOM shall cover; manufacturers may determine this on a case-by-case basis within the scope appropriate for managing vulnerabilities as normally assumed (it is possible that a specific level of detail may be defined in the future depending on SBOM trends).

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf

Furthermore, regarding the created SBOM, manufacturers are required not only to create it initially but also to establish a management process to periodically or sequentially verify the presence of vulnerabilities (including licensing issues) at a frequency they deem sufficient for secure SBOM management, and to implement necessary vulnerability countermeasures and SBOM updates.

2.10 Penetration Tests in Conformance Testing for STAR-3 Network Devices

In the conformance evaluation for STAR-3 Network Devices, penetration tests are conducted by the Evaluation Body.

In these conformance requirements, assuming attacks by an attacker possessing the attack capabilities explained in Section 2.3, at least all of the following penetration test items shall be performed:

- Detection of known vulnerabilities in open ports using network diagnostic tools.
- Detection of known vulnerabilities using web application diagnostic tools.
- Detection of unauthorized communications from IoT devices to external sources using packet capture tools.
- Detection of vulnerabilities in dynamic web application content using a proxy tool.
- Verification of whether debugging is possible using a tool that connects to debug ports.

If security issues are reported during the penetration tests conducted by the Evaluation Body, the manufacturer shall correct those issues and resolve all security issues.

2.11 Obligation to Provide Support

During the validity period of the conformance label, manufacturers are obligated to provide support in the form of security patches/update files to address product defects and vulnerabilities (including alternative measures such as product replacement if security patches/update files cannot be provided). The obligation to provide support during the validity period of the conformance label is imposed to prevent situations where, despite the discovery of defects or vulnerabilities in IoT products, security patches/update files are not properly provided, and those defects or vulnerabilities remain unaddressed and are left unresolved.

Therefore, since it is necessary to ensure that security patches and update files are provided equally to all users of the IoT products, one of the following methods of providing support is mandated:

(1) Support shall be provided free of charge to all users during the support period.

(2) Paid support is permitted only in cases where procurement (including rentals and leases) is performed exclusively for procurers who have entered into a separate contract, such as a maintenance or sales agreement, subject to the terms of that contract.

The validity period of the conformance label may be extended by submitting an extension application; however, if the end of support date falls before the maximum possible extended validity period, the validity period shall be limited to the end of support date. Furthermore, if support is discontinued during the validity period, the conformance label shall expire on the date support is discontinued (the validity period extends only until the date support is provided).

On the other hand, even if the conformance label expires because the product is discontinued and no extension is requested, it will be treated as "Expired—Free Support Continuing" as long as the free support period is still in effect. Furthermore, if paid support continues after the free support period ends, the conformance label shall be marked as "Expired—Validity Period Expired," but information indicating that "paid support is continuing" may be included in the "Support Information" and "Update Information" fields.

3. Conformance Requirements for STAR-3 Network Devices

[Structure of STAR-3 Conformance Requirements]

Each security requirement is linked to the conformance requirements required for IoT products, and it is described in the following structure.

Table 2: Structure of Conformance Requirements

Category	Classification category to which the measures to STAR-3 security requirements required are applied
Security Requirement Number: S3.1-xx	Security requirement number
STAR-3 Security Requirements	Security measures and requirements that shall be satisfied for STAR-3 level IoT products
Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirements	Conditions for being Not Applicable (NA) from STAR-3 Security Requirements and Supplementary Explanation of STAR-3 Security Requirements. When claiming that it falls under "Not Applicable (NA)," the documentation demonstrating that the "Conditions for being Not Applicable (NA)" as described in this item are satisfied shall be provided to the Evaluation Body.

STAR-3 Conformance Requirements	
1. Conformance Requirements	STAR-3 Security Requirements: These requirements specify the functions that a STAR-3 IoT product shall possess and the measures that manufacturers shall implement in response to the countermeasures and requirements listed in the STAR-3 Security Requirements; they are requirements that shall be satisfied.
2. Supplementary Explanation	
2.1 Supplementary Explanation of Conformance Requirements	This document summarizes supplementary explanations regarding these conformance requirements, as well as the approach to interpreting supplementary explanations and requirements for a conformance decision.
2.2 Term	Explanations of terms used in these conformance requirements.

Category 1: Not Using Vulnerable Authentication Mechanisms (e.g., Universal Default Passwords, Weak Passwords)

Security Requirement Number: S3.1-01

STAR-3 Security Requirements

Access control based on appropriate authentication shall be implemented for access from other IoT devices or users to the IoT products.

In addition, for operations such as important setting changes, the above authentication methods shall be re-enforced.

Conditions for being Not Applicable (NA)

There is no mechanism for access. (The rationales for why there is no external access shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

For access from other IoT devices or users, all of the following Requirements 1 through 7 shall be satisfied as access control based on appropriate authentication to satisfy STAR-3 Security Requirements.

Requirement 1:

For communications necessary for the intended use of the IoT product (excluding the "exceptional protocols (*1)" listed below), both of the following Requirements (1) and (2) shall be satisfied regarding access from other IoT devices or users.

(1) Access control based on appropriate authentication shall be implemented, and access to the IoT products is permitted only to other IoT devices or users that have been granted access.

(2) The authentication method used shall be an implementation equivalent to or exceeding any of the following:

A) An implementation of user authentication using a password that complies with S3.1-02

B) An implementation of multi-factor authentication using multiple authentication factors

C) An implementation of an authentication function using digital certificates or public keys

D) An implementation of an authentication function using an external authentication service based on standard authentication methods such as OpenID Connect or FIDO

(*1): Exceptional protocols

Example 1: ARP, ICMP (because they are protocols at layers lower than TCP/UDP)

Example 2: DHCP, DNS, NTP (because they are protocols that do not support authentication)

Requirement 2

When changing settings for SSP (Sensitive Security Parameter) or security-related configuration

information, special authentication shall be required separately.

Requirement 3:

When managing continuous access via sessions or similar mechanisms in an authentication mechanism, a timeout limit shall be established.

Requirement 4:

In the initialized state, accounts (*2) that are unnecessary for use shall be deleted or disabled.

(*2): Examples of unnecessary accounts: debug accounts, etc., used during product development.

Requirement 5:

An access control mechanism shall be designed and implemented in IoT products so that users can voluntarily minimize their permissions.

Requirement 6:

For user access to IoT products that does not involve a network connection, both of the following conditions (1) and (2) shall be satisfied.

(1) Access to the IoT products is permitted only to users who have been authorized based on appropriate authentication.
(2) The authentication method used shall be an implementation equivalent to or exceeding any of the following.
   A) An implementation of user authentication using a password that complies with S3.1-02
   B) An implementation of possession-based authentication
   C) An implementation of biometric authentication

Requirement 7:

A function shall be implemented that restricts communication to specific targets, such as IP addresses.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Access Control Mechanisms

The access control mechanism refers to a function that allows the configuration of roles assigned to users, software processes, or devices. (At a minimum, it shall be able to distinguish between administrators and general users.)

2.2. Term

[SSP (Sensitive Security Parameter)]

A term referring to information assets that combine CSP (Critical Security Parameter) and PSP (Public Security Parameter). Refer to Section 2.4.

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-02

STAR-3 Security Requirements

For IoT products that use passwords in the user authentication mechanism via the network for IoT products, when a default password is used at the time of installation of the IoT product, either of the following requirements (1) or (2) shall be satisfied.

(1) The default password shall be a unique value that differs for each IoT device and shall be at least 8 characters in length that cannot be easily guessed.

(2) A function that requires users to change the password at the initial startup shall be implemented, and users are required to set a password of 8 characters or more that cannot be easily guessed as a password that can be set in the function.

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication using passwords. (The rationales for why user authentication using passwords is not required to counter threats shall be described in the "Reasons for being Not Applicable (NA)."

1. STAR-3 Conformance Requirements

In the user authentication mechanism, as a measure regarding default passwords at the time of IoT product deployment that uses passwords to satisfy STAR-3 Security Requirements, the product shall satisfy either "Requirement 1" or "both Requirement 2-1 and Requirement 2-2" below.

Requirement 1:

The default password shall be unique to each IoT device, consist of at least 8 characters, and not fall under any of the following A) through D).

A) Passwords containing common character strings or simple patterns (e.g., "admin," "root," "QWERTY," etc.)

B) Passwords that use well-known proper nouns, people's names, or place names that are easy to remember (e.g., "baseball," "mustang," "michael," etc.)

C) Passwords based on sequential numbering (e.g., "123456," "aaaaaaaa," "1234abcd," "password1," etc.)

D) Passwords based on publicly available information, such as MAC addresses, Wi-Fi SSIDs, or the serial numbers, model numbers, or names (abbreviations) of IoT products

Requirement 2-1:

A function that requires the user to change the password at the initial startup shall be implemented, and it shall be enforced that the password set via this function be at least 8 characters long. Note that for IoT products that have a mechanism for user authentication via a network but can also be used

without using network function, it is acceptable to require users to change the password used for network-based user authentication not at the time of initial startup, but rather when the network function is used for the first time.

Requirement 2-2:

The product shall either enforce the use of a password of 8 characters or more that cannot be easily guessed or include a function that warns the user if the password is not at least 8 characters and cannot be easily guessed. The following (1) through (4) are considered to determine whether a password cannot be easily guessed or not. A method that provides an equivalent or more rigorous judgement shall be implemented.

(1) It shall be verified that the password does not match the conditions listed in A) through D) above (i.e., it is resistant to dictionary attacks).

(2) A randomness evaluation indicator shall be used.

(3) Conditions for the number of character types and password length shall be set.

(4) The use of automatically generated passwords shall be enforced.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-03

STAR-3 Security Requirements

It shall be possible to change the authentication values used for user authentication of access to IoT products through the networks from other IoT devices or users, regardless of the authentication type (password, token, fingerprint, etc.).

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication or device authentication. (The rationales for why user authentication and device authentication are not required to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

In the user authentication and device authentication mechanisms, the method for changing authentication values to satisfy STAR-3 Security Requirements shall satisfy all of the following Requirements 1 through 4.

Requirement 1:

For user authentication, regardless of the type of authentication (password, token, fingerprint, etc.), users shall be able to change the authentication value.

Requirement 2:

The procedure for changing the authentication value described in Requirement 1 shall be provided to users via a manual or other means.

Requirement 3:

When changing an authentication value, the product shall require re-authentication, even if the user is already authenticated.

Requirement 4:

If a user cannot change the authentication value described in Requirement 1 on their own, the devices shall have a mechanism to reset or initialize the authentication value either at the user's request or through administrator privileges. Additionally, the authentication value shall be resettable or initializable using a method different from that described in Requirement 1.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[authentication value]

Individual values of attributes used in authentication mechanisms for IoT products. (e.g., For the password-based authentication mechanism, the authentication value is password information. For the biometric fingerprint authentication, the authentication value is the fingerprint data of the index finger of the left hand, for example.)

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-04

STAR-3 Security Requirements

The mechanism for user authentication via the network to IoT devices shall make brute force attacks difficult.

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication. (The rationales for why user authentication is not required to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

The user authentication mechanism shall satisfy STAR-3 Security Requirements by making brute-force attacks difficult; to do so, it shall satisfy either "both Requirement 1-1 and Requirement 1-2" or "Requirement 2."

Requirement 1-1:

For user authentication, the product shall implement authentication attempt restrictions similar to those described below in response to "a certain number of times (*1)" of consecutive failed authentication attempts.

A) Prohibition of additional authentication
B) Temporary outage of authentication
C) A fixed delay in issuing the authentication response

(*1): "A certain number of times" refers to the default value for the IoT device (1 or more times) or a value assigned by the administrator within the acceptable range.

Requirement 1-2:

If a user authentication mechanism via a network is implemented, measures equivalent to or exceeding any of the following items (1) through (4) shall be implemented.

(1) Device authentication shall be accepted only from specific devices or browsers (Device Cookie).
(2) In the event of a "certain number" of consecutive failed authentication attempts from a specific IP address, authentication attempt restrictions for that IP address similar to those in Requirement 1-1 shall be addressed.
(3) Authentication shall be performed using a unique URL for each user account.
(4) CAPTCHA shall be used.

Requirement 2:

Multi-factor authentication shall be used.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-05

STAR-3 Security Requirements

Digital certificates used for authentication in IoT products shall have sufficient security strength.
Digital certificates used in IoT products shall be renewable.

Conditions for being Not Applicable (NA)

No digital certificates are used for authentication. (The fact that digital certificates are not used shall be described in the "Reasons for being Not Applicable (NA).)

1. STAR-3 Conformance Requirements

Regarding digital certificates used for authentication, to ensure the security strength required to satisfy the STAR-3 Security Requirements and to enable the secure renewal of digital certificates, all of the following Requirements 1 through 5 shall be satisfied.

Requirement 1:

The cryptography used in digital certificates shall be those specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that shall be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) " and shall use key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 2:

The digital certificates shall be renewed only after verifying its integrity and authenticity. Furthermore, if integrity or authenticity cannot be verified, the renewal shall be canceled.

Requirement 3:

The product shall have a mechanism to cause digital certificates to expire upon receiving valid instructions from an external source, or a mechanism to prevent digital certificates that have expired due to other means from being used for authentication.

Requirement 4:

The generation mechanism shall ensure that the private key corresponding to each digital certificate is unique per device.

Requirement 5:

When updating trust anchors, such as root certificates, the update shall be performed securely to ensure that no malfunctions occur in IoT devices after the update.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Digital Certificates

Digital certificates shall be certificates whose reliability is ensured. At a minimum, it shall be possible to verify that the manufacturer is legitimate. Such certificates include public certificates, root certificates managed by the manufacturer itself, or root certificates issued by a CA contracted by the manufacturer.

2.1.2. Digital Certificates Used Only during Initial Startup

To verify the reliability of digital certificates used during normal operation, digital certificates used only during the initial startup may be excluded from Requirements 2 and 3.
However, such digital certificates shall not be used during normal operation.

2.1.3. Examples of Secure Methods for Updating Trust Anchors

Example 1: Update the trust anchor and all certificates (such as code-signing certificates) whose trust is established by the trust anchor in a single batch along with the firmware

Example 2: Add a new root certificate during the validity period of the old root certificate. Adopt an update mechanism that maintains both the old and new root certificates to assure compatibility before and after the update.

2.2. Term

Not applicable

Security Requirement Number: S3.1-06

STAR-3 Security Requirements

When SSH is used for public key authentication in IoT products, the public key authentication function shall use secure cryptographic algorithms.

Conditions for being Not Applicable (NA)

SSH is not used for public key authentication. (The fact that SSH is not used for public key authentication shall be described in the "Reasons for being Not Applicable (NA)."

1. STAR-3 Conformance Requirements

When using SSH with public key authentication, to enable authentication using cryptography with a security strength that satisfies the STAR-3 Security Requirements, both Requirement 1 and Requirement 2 below shall be satisfied.

Requirement 1:

The cryptography used for SSH public key authentication shall be those described in the "e-Government Recommended Ciphers List" of "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) " and shall use key lengths that comply with the provisions of the "Standards Regarding Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 2:

The public key used for SSH public-key authentication shall be updatable.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-07

STAR-3 Security Requirements

IoT products with VPN gateway function shall satisfy all of the following requirements (1) and (2).

(1) The product shall have a function to perform multi-factor authentication for user authentication.

(2) It shall have a function to restrict the devices, etc., from which it is connected.

Conditions for being Not Applicable (NA)

IoT products do not have a VPN gateway function. (The fact that IoT products do not have a VPN gateway function shall be described in the "Reasons for being Not Applicable (NA)."

1. STAR-3 Conformance Requirements

If the product has VPN gateway function, it shall satisfy all of the following Requirements 1 through 3 as functions to perform strict user authentication and device connection restrictions to satisfy STAR-3 Security Requirements for VPN connections (*1). Furthermore, if the product has a function to perform multi-factor authentication through integration with external systems other than associated services, it shall satisfy requirement 4 in addition to requirements 1 through 3.

(*1) VPN connection:

This applies to remote access VPNs from devices used by users to the internal network. Site-to-site VPNs are excluded.

Requirement 1:

The user authentication method used shall be multi-factor authentication or a similar implementation (*2). (*2) Similar implementation:

This includes FIDO authentication and certain methods referred to as two-step authentication. Examples of such two-factor authentication include methods where a one-time password is sent to the user's mobile phone number or email address and the user is prompted to enter it, as well as authentication methods that utilize authentication requests sent to a smartphone or similar device. When using two-factor authentication, it shall be implemented after conducting an evaluation of the risks involved.

Requirement 2:

The method for restricting device connections shall be either device authentication using digital certificates or a method that involves registering information capable of uniquely identifying the device in advance (whitelist method). However, for the whitelist methods that rely solely on information that is easily spoofed or stolen—such as MAC addresses—are not permitted.

Requirement 3:

As VPN protocols, those generally recognized as secure (e.g., OpenVPN, IPsec, IKEv2, etc.) shall be used by default.

Requirement 4:

If multi-factor authentication function is provided through integration with external systems other than the associated services, all of the following requirements shall be satisfied.

A) A document specifying the conditions under which integration with reliable external systems for multi-factor authentication is possible shall be provided to users. At least one of these conditions shall be technically verifiable.

B) IoT devices shall have the function to verify that external systems integrated for multi-factor authentication satisfy the technically verifiable conditions specified in A).

C) IoT devices shall comply with S3.1-20 in communications with external systems with which they integrate to perform multi-factor authentication.

D) The functions and measures described in B) and C) are enabled by default.

E) Procedures for integrating with external systems using the function described in B) shall be disclosed in media accessible to users, such as IoT product manuals and websites.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. When using a digital certificate as one of the authentication factors for multi-factor authentication

When using a digital certificate as one of the authentication factors in multi-factor authentication, if the certificate is used to verify the destination of the connection, a conformance decision may be made with respect to Requirement 2.

2.2. Term

[VPN gateway function]

A function located at the boundary between an internal network and an external network (such as the Internet) that establishes an encrypted communication path with the user's device.

Security Requirement Number: S3.1-08

STAR-3 Security Requirements

IoT devices shall implement a function to identify connecting devices and to reject the connection of unauthorized devices.

Conditions for being Not Applicable (NA)

IoT devices do not have L2/L3 switching functions. (The fact that IoT devices do not have L2/L3 switching function shall be described in the "Reasons for being Not Applicable (NA)."

1. STAR-3 Conformance Requirements

To deny connections from unauthorized devices, the device shall uniquely identify connecting devices, for example, using IEEE 802.1X authentication, and based on the results, be able to grant or deny the connection.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Unique Device Identification

Methods that rely on information that is easily spoofed, such as MAC addresses, are not considered "methods capable of uniquely identifying devices."

2.2. Term

Not applicable

Category 2: Implementing Means to Manage Vulnerability Reporting

Security Requirement Number: S3.1-09

STAR-3 Security Requirements

Manufacturers shall publish (e.g., post on the manufacturer's website) a vulnerability disclosure policy that includes the information listed in items (1) through (3) below, and shall have the process described in (4) below.

(1) Contact information for reporting to the manufacturer regarding security issues of IoT products (e.g., URL, phone number, and email address of the manufacturer's or other entity's website)

(2) Procedures to be taken by the manufacturer after receiving a report on the security of IoT products (e.g., how the report on security will be accepted, what procedures and methods will be used to communicate with the reporter afterwards, how the manufacturer will respond to the report, declaration of legal disclaimer for good faith reports, etc.), and outline of the process

(3) Procedures for updating the status of IoT products and vulnerabilities until the vulnerability is resolved (e.g., how investigations and countermeasures will be conducted until the vulnerability is resolved, how the status will be managed and announced, and what actions will be taken in response to reporters) and an outline of these procedures

(4) Declaration that the vulnerability will be reported in a timely manner to the appropriate reporting organization.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

The vulnerability disclosure policy shall be made publicly available, and to satisfy the STAR-3 Security Requirements, the disclosure shall satisfy all of the following Requirements 1 through 5:

Requirement 1:

The vulnerability disclosure policy shall include contact information (e.g., the manufacturer's website URL, phone number, email address) for reporting security issues to the manufacturer.

Requirement 2:

The vulnerability disclosure policy shall include a description of the procedures the manufacturer follows after receiving a security report and an overview of those procedures (it is not necessary to disclose detailed procedures, but an overview shall be provided—such as how security reports are accepted and what procedures, methods, and timeframes are used to address them thereafter).

Requirement 3:

The vulnerability disclosure policy shall include an overview of the procedures regarding updates on the status of the IoT products and the vulnerability until the vulnerability is resolved (it is not necessary to disclose detailed procedures, but the policy shall provide an overview—to be made public—of how investigations and countermeasures are conducted until the vulnerability is resolved, how the status is managed and disclosed, and how the reporter is handled, etc.).

Requirement 4:

The vulnerability disclosure policy shall be published on a medium accessible to the general public (such as a website). For IoT products not yet on the market, if the vulnerability disclosure policy has not been published at the time of evaluation, there shall be a plan to publish it. The publication plan shall include information on the vulnerability disclosure policy to be published and the method of publication (e.g., the planned URL or location where it will be posted).

Requirement 5:

The organization shall have a process in place to promptly report critical vulnerabilities, as well as vulnerabilities for which it is aware that an incident has occurred or is likely to occur, to IPA or a designated organization.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Significance of Publicly Disclosing the Vulnerability Disclosure Policy

The significance of publicly disclosing a vulnerability disclosure policy lies in creating an environment where external security researchers, engineers, and others can feel confident reporting potential vulnerabilities that the manufacturer itself was not aware of.

Specifically, for manufacturers, this is expected to expand the means by which they can obtain vulnerability information at an early stage, enabling them to take countermeasures against vulnerabilities promptly. On the other hand, by publicly announcing in advance how manufacturers will respond to reported vulnerabilities, vulnerability discoverers are given the assurance that the reported vulnerability information will be handled appropriately.

Taking into account these significances, JC-STAR asks for the disclosure of:

- the destination for vulnerability reports
- the procedures manufacturers follow after receiving reports regarding the security of IoT products, along with an overview of those procedures (particularly the timeframe for sending an "acknowledgment of receipt" upon receiving a report)
- the procedures and an overview regarding updates on the status of IoT products and vulnerabilities until the vulnerabilities are resolved (specifically, how frequently the status of the response will be provided or communicated, while ensuring transparency).

Reference materials for vulnerability disclosure policies include ISO/IEC 29147:2018 (under the PSTI Act[4], specifically clauses 6.2.2, 6.2.5, and 6.5), the Vulnerability Disclosure Policy Template[5], and clause 5.2-1 of ETSI EN 303 645.

Note that "publishing a vulnerability disclosure policy" and "publishing vulnerability information" have different meanings.

2.2. Term

Not applicable

[4] https://www.legislation.gov.uk/uksi/2023/1007/schedule/2/paragraph/2

[5] https://www.cisa.gov/vulnerability-disclosure-policy-template

Category 3: Keeping Software Up-to-dated

Security Requirement Number: S3.1-10

STAR-3 Security Requirements

All of the following requirements (1) through (4) shall be satisfied for the update function of firmware (software) included in IoT products.

(1) It shall be possible to update the firmware (software) package of IoT products.

(2) The firmware (software) package shall have a means to confirm that the latest firmware (software) is installed, such as being able to check the version of the firmware (software) package.

(3) The version of the firmware (software) package that has been updated shall be maintained even after the power is turned off.

(4) If online updates are available, the device shall have an automatic update function.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates. (The rationales for being able to address vulnerabilities without updates shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

Regarding the software update function, to ensure that updates satisfy STAR-3 Security Requirements can be executed, all of the following Requirements 1 through 4 shall be satisfied. Additionally, if the product has a function to perform automatic updates through integration with external systems other than associated services, Requirement 5 shall be satisfied in addition to Requirements 1 through 4.

Requirement 1:

The firmware (software) package shall have an update function.

Requirement 2:

The product shall have a means to verify that the latest firmware (software) is installed, such as by checking the firmware (software) package version. Alternatively, the product shall have a function that automatically displays a warning indicating that an update to the latest firmware (software) has not been performed.

Requirement 3:

The version of the updated firmware (software) package is retained even after the power is turned off.

Requirement 4:

When updating the firmware **(**software**)** via a network, the device shall have an automatic update function.

Requirement 5:

If the device has a function to perform automatic updates through integration with external systems other than the associated services, it shall satisfy all of the following requirements.

A) A document specifying the conditions under which integration with reliable external systems for automatic updates is possible shall be provided to the user. At least one of these conditions shall be technically verifiable.

B) The IoT device shall have a function to verify that the external system with which it interfaces to perform automatic updates satisfies the technically verifiable conditions specified in A).

C) IoT devices shall comply with S3.1-20 in communications with external systems with which they interact to perform automatic updates.

D) The functions and measures described in B) and C) are enabled by default.

E) Procedures for integrating with external systems using the function described in B) shall be disclosed in media accessible to users, such as IoT product manuals and websites.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Automatic update function being enabled by default

When an update is performed, temporary outages may occur due to the Network Devices restarting. In light of situations where it is necessary to prevent such temporary outages from occurring at inappropriate times against the user's intent, the requirement to enable the automatic update function by default is not mandated.

2.2. Term

Not applicable

Security Requirement Number: S3.1-11

STAR-3 Security Requirements

It shall be possible to perform software updates in an easy and understandable procedure when users apply updates.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates by users. (The rationales for being able to address vulnerabilities without updates by users shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

To ensure that software updates can be performed using a simple and easy-to-understand procedure that satisfies the STAR-3 Security Requirements, one of the following Requirements 1 through 4 shall be satisfied. Note that if multiple update methods are used, the applicable requirements shall be satisfied for each one.

Requirement 1:

Users shall be informed via a manual or other means that updates are performed automatically. Furthermore, users shall be informed of the steps to take if an automatic update fails.

Requirement 2:

Users performing updates shall be provided with instructions, such as in a manual, on how to perform the update using the associated services for IoT products (e.g., mobile applications).

Requirement 3:

The procedures for performing updates via the IoT products' interfaces (such as a web interface) shall be clearly communicated to users performing the updates through manuals or other means.

Requirement 4:

The procedures for users performing updates to obtain update files, such as by downloading them from the manufacturer's website, and to perform the update by installing them shall be clearly communicated to users in manuals or other documentation.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. "Easy and Clear Procedures"

The "easy and clear instructions" required by this conformance requirement refer to procedures

designed so that even users without specialized knowledge can typically successfully perform the update by following the instructions in the installer, manual, or operating procedures.

2.1.2. "Users Performing Updates"

The scope of "users performing updates" may vary depending on the IoT products. These conformance requirements apply only to "users performing updates" among all users; it is sufficient for the procedures to be made known to those specific users.

For example, for IoT products where a customer engineer performs the update, it is sufficient for the customer engineer to be familiar with the update procedure; it is not necessarily required for the product's users to be familiar with it. On the other hand, in cases of automatic updates or when users are required to perform the update, the users shall be familiar with the procedure.

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-12

STAR-3 Security Requirements

When updating software, a function that satisfies all of the following (1) through (3) shall be implemented.

(1) IoT products shall have a mechanism to confirm the integrity and authenticity of the software prior to an update.

(2) If authenticity or integrity is not satisfied, the update shall be suspended.

(3) Anti-rollback function shall be provided.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates. (The rationales for being able to address vulnerabilities without updates shall be described in the "Reasons for being Not Applicable (NA).")

1. STAR-3 Conformance Requirements

Regarding software updates, the following "mechanism equivalent to either Requirement 1 or Requirement 2, or a mechanism that goes beyond them" shall be implemented as a mechanism to securely execute updates that satisfy STAR-3 security requirements, and it shall also satisfy "Requirements 3 and 4."

Requirement 1:

Before or during an update using the updated software, message authentication is used to simultaneously verify the digital signature, integrity, and authenticity of the updated software; if the verification results in a failure, the update is aborted.

Requirement 2:

Before updating with the updated software, the digital signature attached to the updated software is used to verify the software within the relevant application on a PC, smartphone, or similar device; if the verification results in a "failure," the update is aborted.

Requirement 3:

The cryptography used for the digital signatures or message authentication in Requirements 1 and 2 shall be those specified in the "List of Cryptographic Algorithms Recommended for E-Government" within the "List of Cryptographic Algorithms to be Referenced for Procurement in E-Government (CRYPTREC Cryptographic Algorithm List)," and shall use key lengths that comply with the provisions of the "Configuration Standards Regarding Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 4:

Before updating with the updated software, the version of the updated software shall be verified; if it is confirmed to be is the same as or earlier than the current version, the update shall be canceled. Note that this requirement does not preclude the provision of a means to install previous versions of the software as needed, but by default, it shall not be possible to update using a previous version of the updated software.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Message Authentication That Simultaneously Verifies Integrity and Authenticity

This is a type of message authentication known as "key-based message authentication," in which message authentication is performed using secret information that is possessed only by the sender (in this conformance requirement, the updated software provider server) and the recipient (the IoT device). However, since this secret information shall be shared only between a unique sender and recipient, it is necessary to configure unique secret information per IoT device when using this conformance requirement. In other words, it is not possible to implement this mechanism using secret information shared across multiple IoT devices.

2.2. Term

Not applicable

Security Requirement Number: S3.1-13

STAR-3 Security Requirements

Manufacturers shall document policies and guidelines for determining priorities of security updates for the purpose of promptly updating security issues.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

Regarding the response to security issues, as a mechanism to ensure prompt updates addressing security issues in order to satisfy the STAR-3 Security Requirements, the organization shall satisfy all of the following Requirements 1 through 3.

Requirement 1:

Guidelines for determining the priority of security updates, based on factors such as the severity and criticality of vulnerabilities, as well as the type of vulnerabilities (e.g., firmware, hardware, software, etc.) shall be defined.

Requirement 2:

An organizational structure for handling incident response (e.g., Product Security Incident Response Team (PSIRT), incident response team) and a set of response processes and policies, including the collection, triage, and analysis of vulnerability information, as well as countermeasures and updates, shall be defined.

Requirement 3:

For products developed and operated by multiple stakeholders (*1), the communication framework among stakeholders (contact information, communication methods, etc.) is documented.

(*1): Partners in the software supply chain, providers involved in product services, etc.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-14

STAR-3 Security Requirements

Model numbers of IoT products shall be provided to users in one of the following ways.

(1) The model number and serial number of the IoT product shall be described directly on the IoT product itself.

(2) The model number and serial number shall be recognizable by users from the GUI or web UI, etc., of the IoT products, and from the GUI or web UI, etc., of the software or applications (smartphone applications, etc.) accompanying the IoT products.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

Regarding the product model number, the product shall satisfy either Requirement 1 or Requirement 2 below as a mechanism for providing information to satisfy STAR-3 security requirements.

Requirement 1:

The product model number and serial number shall be printed on the product itself.

Requirement 2:

There shall be a mechanism implemented that allows the product model number and serial number to be confirmed by actually accessing the product's GUI, web UI, etc., or the GUI, web UI, etc., of software or applications (such as smartphone apps) associated with the product.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. "Direct Marking on the Product Itself"

Direct marking on the product itself is considered in accordance with the requirements even if it is done by affixing a label.

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-15

STAR-3 Security Requirements

A uniquely identifiable software bill of materials (SBOM) that includes third-party components used in IoT products shall be created and operated. Specifically, all of the following requirements (1) through (4) shall be satisfied.

(1) For the management of known vulnerabilities in the operation phase after product shipment, the SBOM for software that is a component of the product (including third-party components) shall be created and updated during the support period.

(2) During the support period, the SBOM shall be periodically checked for vulnerabilities based on the information in the SBOM, and a process shall be implemented to determine the priority of the vulnerabilities to be addressed before updating the SBOM or implementing operational countermeasures.

(3) During the support period, there shall be a process to manage the licenses of the components used based on SBOM information.

(4) It shall be ensured that software cannot be installed by means other than official updates after the product is shipped, or a mechanism shall be implemented that allows only authorized software to be installed.

Conditions for being Not Applicable (NA)

Not applicable

1. **STAR-3 Conformance Requirements**

Regarding software management, including third-party components, the mechanism for creating and operating a SBOM, which includes software identification information, component information, and other data necessary to satisfy STAR-3 Security Requirements, shall satisfy all of the following Requirements 1 through 8.

Requirement 1:

It specifies the process for creating and generating machine-readable and human-readable SBOMs for all components, including third-party components.

Requirement 2:

SBOM is created in accordance with Requirement 1.

Requirement 3:

It specifies a process for periodically verifying, based on the created SBOM, that the components in use (including third-party components) do not include older versions containing vulnerabilities.

It also specifies that the SBOM shall be updated during the support period.

Requirement 4:

It stipulates a process for determining the response priority based on the impact on the product when a component containing a vulnerability is detected, and for deciding whether to implement an update or an operational workaround.

Requirement 5:

It stipulates a process for managing the licenses of components used (including third-party components) based on the created SBOM.

Requirement 6:

Manufacturers shall specify the frequency they deem sufficient for "regular vulnerability checks" as part of secure management.

Requirement 7:

Requirement 1 and Requirements 3 through 6 shall be explicitly stated in technical documents, etc.

Requirement 8:

Either Requirement 8-1 or Requirement 8-2 shall be satisfied.

Requirement 8-1:

The software shall be configured so that it cannot be installed by any means other than official updates, and that configuration shall be made unchangeable.

Requirement 8-2:

If software installation by means other than official updates is permitted, all of the following conditions shall be satisfied.

(1) A mechanism shall be established that allows users to install software only when installation is permitted.

(2) A mechanism shall be established whereby only administrators can change the settings regarding whether installation is permitted.

(3) A mechanism shall be established whereby administrators grant users permission to install software Establish a system whereby administrators grant users permission to install software.

(4) "Installation Disabled" shall be set as the default setting at the time of product shipment.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Scope of SBOM Application

A) IoT devices: Firmware of the applicable IoT devices

B) Associated services: Software for which the manufacturer is responsible for updates

2.1.2. Hierarchy for Describing the SBOM

Since there are no globally established best practice standards for creating SBOMs, these conformance requirements do not specify the level of detail to be covered by the SBOM; manufacturers may determine this on a case-by-case basis within a scope appropriate for managing vulnerabilities as normally assumed. However, note that depending on future trends regarding SBOMs, it is possible that specific levels of detail may be defined in the future.

Example) If the scope of the SBOM is limited to major components and components with direct dependencies on them, the SBOM shall include components with direct dependencies, as shown in the example below.

A) Example of Static Dependencies

- Components such as libraries and header files required at compile time
- Components required when the program links to external libraries or files
- Components required by the programming environment when using a package manager

B) Examples of dynamic dependencies

- Components included when adding functions via plugins
- Components such as dynamic-link libraries (DLLs) and shared libraries
- Dynamically generated components, such as JavaScript

C) Examples of remote dependencies

- Components such as resources and services accessed via the Internet

2.1.3. Examples of SBOM data fields

The following are examples of data fields defined by CISA as minimum elements.

- SBOM Author
- Software Producer
- Component Name
- Component Version
- Software Identifiers
- Component Hash
- License

- Dependency Relationship
- Tool Name
- Timestamp
- Generation Context

2.1.4. Example of SBOM Format

1) Example of Structure Format

As a standard format that satisfies the data field requirements for an SBOM, the following examples of recommended formats are provided.

- CycloneDX
- Software Package Data Exchange (SPDX)
- SPDX Lite*Assumes manual SBOM creation

2) Example of File Format

Examples of machine-readable SBOM file formats are shown below.

- For CycloneDX: JSON, XML, Protocol Buffers (Protobuf)
- For SPDX: SPDX Tag/Value, RDF/XML, YAML, JSON
- For SPDX Lite: SPDX Tag/Value, RDF/XML, YAML, JSON

2.1.5. Examples of How to Check for Vulnerabilities in Components Included in an SBOM

A) Vulnerability analysis using software component analysis (SCA) tools

*Analysis methods, such as binary analysis and source code analysis, vary depending on the tool.

B) Manual verification using vulnerability reporting sites such as JVN

2.2. Term

Not applicable

Category 4: Secure Storage

Security Requirement Number: S3.1-16

STAR-3 Security Requirements

Securely stored information that is stored in the storage of IoT products (including securely stored information that is stored on storage media such as SD cards) shall be securely stored.

Conditions for being Not Applicable (NA)

Not applicable

1. **STAR-3 Conformance Requirements**

As a mechanism for securely storing securely stored information saved on storage media to satisfy the STAR-3 Security Requirements, all securely stored information shall, for each information asset, satisfy the following Requirement 1 and "protective measures equivalent to any of Requirements 2 through 6 or measures of a higher level." Furthermore, when removable storage is available, Requirements 7 and 8 shall also be satisfied.

Note that different measures may be adopted for each information asset. Furthermore, multiple measures may be used in combination.

Requirement 1:

For the information assets listed below among the securely stored information, "sensitive information protection" shall be implemented.

- CSP (Critical Security Parameter)
- Configuration information related to communication functions
- Configuration information related to security functions
- Audit logs

Requirement 2:

Securely stored sensitive information requires confidentiality protection and shall be encrypted or hashed using the cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)" and shall use key lengths that comply with the provisions of the "Standards Regarding Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 3:

Securely stored information requiring protection of integrity shall be stored in a manner that allows the integrity of the data to be verified through a signature using the cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to

in the procurement for the e-Government system (CRYPTREC Ciphers List)" and shall use key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 4:

Securely stored information requiring integrity protection shall be stored in a manner that allows the integrity of the data to be verified through message authentication using the cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)" and shall use hash functions that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 5:

Securely stored information shall be stored in a secure area provided by virtualization technology, a sandbox provided as a function of operating systems such as iOS or Android, or a security chip.

Requirement 6:

Securely stored information shall be stored in a storage area embedded in an IoT device that cannot be easily removed, in an area where direct reading or writing of data via an externally accessible interface is not possible, or in an area that does not have such an interface.

Requirement 7:

If the device has the function to store secure information on removable storage, it shall be stored in a manner that satisfies "Requirement 1" and "Requirements 2 through 4."

Requirement 8:

If the device has a function to store information on removable storage in a format readable by other devices, it shall be equipped with a mechanism to store the information in a form that is readable only to the necessary extent under appropriate access control.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[securely stored information]

The following information. Refer to Section 2.4.

- CSP (Critical Security Parameter)
- PSP (Public Security Parameter)
- Configuration information related to communication functions
- Configuration information related to security functions
- Program code
- Logs (telemetry data and audit logs)

Security Requirement Number: S3.1-17

STAR-3 Security Requirements

CSPs (Critical Security Parameters) used in IoT products shall not be hard-coded into IoT devices. Furthermore, all of the following requirements (1) and (2) shall be satisfied to prevent tampering with PSPs (Public Security Parameters) hard-coded into IoT devices (such as device-specific identifiers or authentication codes used to verify identities).

(1) The full scope of the PSPs (Public Security Parameters) hard-coded into IoT devices shall be understood and listed.

(2) All PSPs (Public Security Parameters) listed in (1) shall be implemented in such a way that they are resistant to tampering by physical, electrical, or software means.

Conditions for being Not Applicable (NA)

There is no hard-coded CSP (Critical Security Parameter) or PSP (Public Security Parameter). (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that there is no hard-coded CSP (Critical Security Parameter) or PSP (Public Security Parameter).)

1. **STAR-3 Conformance Requirements**

To verify that no CSP is hard-coded in order to satisfy the STAR-3 Security Requirements, the following Requirement 1 shall be satisfied.

Furthermore, if there is a hard-coded PSP, it shall satisfy all of the following Requirements 2 and 3 as a means of protecting the PSP to satisfy the STAR-3 Security Requirements. If there is no hard-coded PSP, Requirements 2 and 3 do not apply.

Requirement 1:

No CSP is hard-coded.

Requirement 2:

A list of hard-coded PSPs shall be provided.

Requirement 3:

All hard-coded PSPs are protected against tampering by one of the following means.

- Physical protection, such as a Trusted Platform Module (TPM) or secure element
- Protection via electronic tamper-response mechanisms, such as data erasure triggered by sensor detection
- Software-based protection using cryptography. However, this shall be the cryptography described in the "e-Government Recommended Ciphers List" of "The list of ciphers

that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) " and shall use key lengths that comply with the provisions of the "Standards Regarding Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[CSP (Critical Security Parameter)]

[PSP (Public Security Parameter)]

Refer to Section 2.4.

Security Requirement Number: S3.1-18

STAR-3 Security Requirements

In order to confirm that CSPs (Critical Security Parameters) are not included in the SSPs (Sensitive Security Parameters) directly described in the source code, all of the following requirements (1) and (2) shall be satisfied.

(1) All SSPs (Sensitive Security Parameters) directly described in the source code shall be known and listed.

(2) Among SSPs (Sensitive Security Parameters), CSPs (Critical Security Parameters) that are used during the operation of IoT products shall not be included in the list in (1).

Conditions for being Not Applicable (NA)

There is no SSP (Sensitive Security Parameter) in the source code. (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that there is no hard-coded SSP (Sensitive Security Parameter) in the source code.)

1. STAR-3 Conformance Requirement

When SSPs are written directly in the source code, to verify that CSPs are not included in the source code as STAR-3 Security Requirements, all of the following Requirements 1 and 2 shall be satisfied.

Requirement 1:

The SSPs written directly in the source code are listed.

Requirement 2:

The listed SSPs shall not include any CSPs (Critical Security Parameters) used during operation (*1).

(*1) During operation of the IoT products:

The period during which the IoT products are being used by the user. This excludes periods such as development, pre-shipment testing, and failure analysis.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[CSP (Critical Security Parameter)]

[PSP (Public Security Parameter)]

Refer to Section 2.4.

[SSP (Sensitive Security Parameter)]
Information assets comprising both CSP and PSP.

Security Requirement Number: S3.1-19

STAR-3 Security Requirements

Among the CSPs (Critical Security Parameters) used by IoT products, the CSPs (Critical Security Parameters) used to check the integrity and authenticity of software updates and to protect communications with associated services shall be unique to each IoT device.

Conditions for being Not Applicable (NA)

If the CSP is not used to check the integrity and authenticity of software updates or to secure communications with associated services. (It shall be stated in the "Reason for being Not Applicable (NA)" that the CSP is not used to check the integrity and authenticity of software updates or to secure communications with associated services.)

1 **STAR-3 Conformance Requirements**

Regarding CSPs (Critical Security Parameters) used to verify the integrity and authenticity of firmware (software) updates to IoT products, as well as to share cryptographic keys used in encrypted communications, both Requirement 1 and Requirement 2 below shall be satisfied to reduce the risk of automated attacks against IoT products.

Requirement 1:

CSPs (Critical Security Parameters), which are used to verify the integrity and authenticity of firmware (software) package updates and to share cryptographic keys used in encrypted communications, shall be generated in such a way as to be resistant to automated attacks.

Requirement 2:

The CSP (Critical Security Parameter) generated in Requirement 1 shall be unique per IoT device.

2 **Supplementary Explanation**

2.1. Supplementary Explanation of Conformance Requirements

This conformance requirement stipulates that when using keyed message authentication codes to verify the integrity and authenticity of firmware (software) package updates, a different CSP shall be assigned to each IoT product, even within the same product class. On the other hand, note that when using digital signatures to verify the integrity and authenticity of firmware (software) package updates, IoT products do not use CSPs.

2.2. Term

[CSP (Critical Security Parameter)]

Refer to Section 2.4.

Category 5: Secure Communication

Security Requirement Number: S3.1-20

STAR-3 Security Requirements

All of the protective measures listed in the following (1) and (2) shall be taken for sensitive communication information transmitted over the network.

(1) IoT products shall confirm the validity of the destination of the sensitive communication information.

(2) For sensitive communication information, IoT products themselves shall take protective measures against eavesdropping and tampering of information.

Conditions for being Not Applicable (NA)

There is no sensitive communication information transmitted over the network (It shall be stated in the "Reasons for being Not Applicable (NA)" that there is no sensitive communication information transmitted over the network).

1 **STAR-3 Conformance Requirements**

As communication protective measures to satisfy the STAR-3 Security Requirements for sensitive communication information, all of the following Requirements 1 through 6 shall be satisfied. If there is an app linked to IoT products, sensitive communication information sent from the app shall also be subject to protection against unauthorized access and eavesdropping or tampering.

Requirement 1:

IoT products shall verify the validity of the communication destination through appropriate authentication.

Requirement 2:

One of the following measures A) or B) shall be implemented.

A) When IoT products send or receive sensitive communication information, they shall adopt cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)," using key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)" and transmit the information via a communication protocol that ensures confidentiality and integrity.

B) Sensitive communication information that has been stored after being encrypted in accordance with Requirement 2 of S3.1-16 shall be transmitted over the network without being decrypted. Furthermore, the integrity of sensitive communication information shall

be ensured using cryptography specified in "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)."

Requirement 3:

If TLS is used as the encryption protocol, the device shall satisfy the requirements of the protocol versions and cipher suites classified as "Recommended security type" or higher, as specified in the "Guidelines for Configuration of TLS" published by CRYPTREC.

Requirement 4:

Measures for Requirements 1 through 3 shall be enabled by default.

Requirement 5:

A list of unencrypted protocols available on IoT products based on the configuration shall be provided. Furthermore, these protocols shall be disabled by default.

Requirement 6:

The device shall have a mechanism whereby unencrypted protocols, which are disabled by default under Requirement 5, can be enabled only by users with special privileges (such as administrator privileges) who have been properly identified and authenticated. Furthermore, security precautions, including the risks associated with enabling these protocols, shall be clearly notified to users in the documentation explaining how to change settings (e.g., the user manual).

2 Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Examples of Sensitive Communication Information Not Transmitted Over a Network

Note that even when sensitive communication information is exchanged using link-local addresses to achieve logically one-to-one direct communication over a network, it is still considered "sensitive communication information transmitted over a network."

Only when sensitive communication information is exchanged using methods that allow only physical one-to-one connections, such as serial ports or USB, it is considered "not sensitive communication information transmitted over a network."

2.2. Term

[sensitive communication information]

The following information. Refer to Section 2.4.

- CSP (Critical Security Parameter)

- Configuration information related to communication functions
- Configuration information related to security functions
- Alert information
- Audit logs

Security Requirement Number: S3.1-21

STAR-3 Security Requirements

Secure management processes shall be implemented for each lifecycle of generating, distributing, storing, and updating CSPs (Critical Security Parameters) used in IoT products.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

Regarding CSPs, to achieve a lifecycle that satisfies the STAR-3 Security Requirements, all of the following Requirements 1 and Requirements 2 shall be satisfied.

Requirement 1:

The lifecycle for the CSPs (Critical Security Parameters) used shall be defined, and the secure processes to be implemented for managing them shall be clearly specified in technical documents, etc.

Requirement 2:

The process for securely updating CSPs shall be clearly specified in technical documents or similar materials.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Examples of CSP (Critical Security Parameter) Lifecycle and Management

Definitions shall be established with references such as the "Cryptographic Key Management System Design Guidelines (Basic Edition)" issued by IPA. The cryptographic key lifecycle and cryptographic key lifecycle management functions serve as useful references.

2.2. Term

[CSP (Critical Security Parameter)]

Refer to Section 2.4.

Security Requirement Number: S3.1-22

STAR-3 Security Requirements

IoT products with wireless LAN function shall implement a function to encrypt communications using an appropriate method and device authentication using IEEE 802.1X in the wireless communication section.

Conditions for being Not Applicable (NA)

IoT products do not have wireless LAN functions. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have wireless LAN functions.)

1. STAR-3 Conformance Requirements

Regarding wireless LAN communications, as security measures to satisfy the STAR-3 Security Requirements, all of the following Requirements 1 through 4 shall be satisfied.

Requirement 1:

Either the WPA3 Enterprise (Wi-Fi Protected Access 3 Enterprise) or WPA2 Enterprise (Wi-Fi Protected Access 2 Enterprise) shall be supported.

Requirement 2:

The default setting for the wireless communication segment shall require connections using WPA2 or higher.

Requirement 3:

WEP and WPA shall not be supported, or they shall be disabled by default.

Requirement 4:

The EAP (PPP Extensible Authentication Protocol) standard used for IEEE 802.1X authentication shall support the TLS, TTLS, PEAP, or EAP-FAST authentication methods.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Category 6: Minimizing Exposed Attack Surfaces

Security Requirement Number: S3.1-23

STAR-3 Security Requirements

In order to reduce the risk of external cyber attacks on IoT products, interfaces that are unnecessary for the use of IoT products and at risk of being attacked shall be disabled, and vulnerability tests for IoT products shall be performed. Specifically, all of the following requirements (1) and (2) shall be satisfied.

(1) For the following interfaces that are used frequently in IoT products and are assumed to be at risk of vulnerability, etc., those interfaces that are unnecessary for the use of IoT products and at risk of being attacked shall be disabled.

A) TCP/UDP ports

B) Bluetooth

C) USB

(2) Known vulnerabilities shall be checked by vulnerability scanning tools for IoT products to ensure that no vulnerabilities that could be exploited by attacks are detected.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To reduce the risk of cyber attacks, interfaces that are unnecessary for normal use and pose a risk of attack shall be disabled, and to ensure there are no known vulnerabilities that could be exploited in an attack, all of the following Requirements 1 through 4 shall be satisfied.

However, if a vulnerability is detected under Requirement 4, Requirement 5 shall be implemented for an evaluation to determine whether the detected vulnerability could be exploited in an attack. If the evaluation determines that there is no problem, the product is deemed to "satisfy Requirement 4."

Requirement 1:

For each of the following interfaces installed in the product and made available through configuration, the product shall satisfy all of the requirements A) through C). Whether or not the interface is available by default is irrelevant.

A) If TCP/UDP is included and available, the product shall satisfy all of the following requirements.

- For TCP and UDP ports that are open (LISTEN) by default for inbound communication, the target port numbers, communication protocols, intended uses,

timing of opening, and conditions of use shall be explicitly stated in technical documents, etc. Note that for products supporting IPv6, this applies to both IPv4 and IPv6.

- It shall be ensured that the open ports do not include those ports which do not need to be open by default, such as the ports that are not needed to use or whose purpose of use is unclear.

B) If the device is equipped with and capable of using Bluetooth, it shall satisfy all of the following requirements.

- All available Bluetooth profiles shall be explicitly stated in technical documents, etc.
- The Bluetooth profiles used by default and their intended purposes shall be clearly stated in technical documents, etc.
- The Bluetooth profiles used by default shall not include any profiles that are unnecessary for use.

C) If the device is equipped with and capable of using USB, it shall satisfy all of the following requirements.

- All available USB device class names shall be explicitly stated in technical documents, etc.
- The class names and intended uses of the USB device classes used by default shall be explicitly stated in technical documents, etc.
- The USB device classes used by default shall not include any device classes that are unnecessary for the intended use.

Requirement 2:

All of the following requirements shall be satisfied.

- If there are any interfaces on the product that cannot be enabled through physical measures or equivalent means (disabled interfaces), the specific disabled interfaces and the means of disabling them shall be clearly identified. If there are no such interfaces, it shall be clearly stated that "there are no interfaces disabled by physical measures, etc."
- Information regarding the disabled interfaces and the means of disabling them shall be explicitly stated in the technical documents, etc.

Requirement 3:

All of the following requirements shall be satisfied.

- If ports with a particularly high risk of being exploited by attacks by default (e.g., telnet (23/TCP and 2323/TCP), etc.) are in use, there shall be a management process in place to monitor attack activity and take appropriate countermeasures as necessary. If such ports are not in use, it shall be clearly stated that "No ports with a particularly high risk of being

exploited by attacks are in use."

- This management process shall be explicitly described in technical documents, etc.

Requirement 4:

Regarding vulnerability testing, all of the following requirements shall be satisfied.

i) It shall be verified that no vulnerabilities with a CVSSv3 Severity score of 4.0 or higher have been detected on open TCP/UDP ports.

ii) If configurations or functions using the HTTP/HTTPS protocols are implemented, it shall be verified that no vulnerabilities corresponding to the known CVE-IDs listed at the URL below have been detected.

[URL]

NIST: NATIONAL VULNERABILITY DATABASE

https://nvd.nist.gov/vuln/search

[Search Criteria]

Search Type: Advanced

Category: All of the following shall be covered; "CWE-78 OS Command Injection," "CWE-89 SQL Injection," "CWE-352 Cross-Site Request Forgery (CSRF)"Include all of the following: "CWE-22 Path Traversal," "CWE-300: Channel Accessible by Non-Endpoint," "CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)," and "CWE-384: Session Fixation"

iii) Vulnerability testing using vulnerability scanning tools shall be conducted as necessary. At that time, the vulnerability scanning tools used and the scan results shall be clearly stated in technical documents, etc., and confirmed that no vulnerabilities were detected.

Requirement 5:

If vulnerabilities are detected under Requirement 4, the following analysis and evaluation shall be conducted for all detected vulnerabilities and confirmed that the vulnerabilities do not have a problem for the use of the IoT device. If it can be confirmed that none of the detected vulnerabilities have a problem, the determination shall be made that "there are no vulnerability problems."

- Analysis of whether the detected vulnerability is a false positive, and evaluation of whether the vulnerability has no problem for the use of the IoT device.
- Analysis of whether the vulnerability can be considered already mitigated through separate countermeasures, and evaluation of whether, as a result of those countermeasures, the vulnerability has no problem for the use of the IoT device.
- Analysis of whether it is possible to prove that the detected vulnerability has no impact in the actual operational environment of the IoT device, and evaluation to prove that there is no impact.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Examples of interfaces in Requirement 2 that cannot be changed to an operational state through physical measures

- RJ45 and USB ports that are not necessary for normal user operation shall be protected from external exposure by enclosures or covers that cannot be easily opened, such as those secured with security screws.
- USB ports intended solely for powering the device shall be physically configured so that command or debug operations are not permitted (e.g., by physically disabling the signal lines used for data communication).

2.1.2. Examples of interfaces that are not in an operational state due to measures equivalent to the physical countermeasures described in Requirement 2

- The driver has been removed, rendering the interface unusable.
- The interface has been disabled, and the configuration change function has been removed or left unimplemented.

2.2. Term

Not applicable

Security Requirement Number: S3.1-24

STAR-3 Security Requirements

In the initialized state, security-related information that can be viewed without authentication from network interfaces enabled on IoT products shall be minimized, including the following;

A) Configuration information of device

B) Kernel version

C) Software version

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To reduce the risk of cyber attacks, security-related information accessible without authentication via the network shall be limited to the absolute minimum; therefore, all of the following Requirements 1 through 4 shall be satisfied.

Requirement 1:

A list of all security-related information that is accessible via the network without authentication by default, along with the purpose for making it accessible (a valid purpose for making such security-related information accessible), shall be explicitly stated in technical documents, etc.

Requirement 2:

In light of the purpose, the scope of all security-related information accessible via the network without authentication is limited to the minimum necessary. It shall not include security-related information for which there is little need to make it accessible.

Requirement 3:

A list of all security-related information accessible via the network without authentication by default shall be provided to users through media accessible to them, such as manuals.

Requirement 4:

If there are settings that allow users to modify the scope of all security-related information accessible via the network without authentication, the following information shall also be provided to users.

- Security-related information for which access settings can be changed
- Procedures for changing access settings

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-25

STAR-3 Security Requirements

IoT devices shall have all of the following protective measures (1) and (2) against physical attacks.

(1) Unnecessary physical interfaces of IoT devices shall have a mechanism to protect them from exposure.

(2) Debugging interfaces of IoT devices shall be physically or logically disabled.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To reduce the risk of cyber attacks, the following Requirements 1 through 4 shall all be satisfied as protective measures for the interface.

Requirement 1:

The device shall have a mechanism to protect physical interfaces that are unnecessary for its intended use from exposure.

Requirement 2:

Debug interfaces shall be disabled by physical or logical means.

Requirement 3:

An overview of the protective measures implemented in accordance with Requirements 1 and 2 shall be explicitly stated in technical documents, etc.

Requirement 4:

The procedures and conditions for enabling the debug interface shall be explicitly stated in technical documents, etc.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Examples of Protection Against Exposure of Physical Interfaces

- RJ45 and USB ports that are not necessary for normal user operation shall be protected from external exposure by enclosures or covers that cannot be easily opened, such as those secured with security screws.
- USB ports intended solely for powering the device shall be physically configured so that the command or debug operations are not permitted (e.g., by physically disabling the signal

lines used for data communication).

2.1.2. Examples of Target Debug Interfaces

- JTAG (Joint Test Action Group) *IEEE 1149.1 standard
- Compact JTAG *IEEE 1149.7 standard
- UART (Universal Asynchronous Receiver/Transmitter)
- SWD (Serial Wire Debug)
- FINE

2.1.3. Example of Disabling the Debug Interface

Note that this does not prevent the temporary deactivation of the debug interface from being reinstated during maintenance by the manufacturer.

- Examples of Physical Disabling
  - The interface is housed in a sturdy enclosure, and the enclosure is secured with security screws, etc., to prevent it from being easily opened.
  - The interface is made inaccessible by a screw-fastened cover.
- Examples of Logical Disabling
  - The debug interface settings are disabled in the firmware version shipped with the product.
  - If use of the debug interface is required after shipment, the console function is disabled, the scope of log output is set to a minimum, and the debug interface settings are enabled.

2.2. Term

Not applicable

Security Requirement Number: S3.1-26

STAR-3 Security Requirements

In designing and implementing IoT products, manufacturers shall enable only those services that are used or required for the intended use or operation of the devices.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To reduce the risk of cyber attacks, manufacturers shall confirm that unnecessary services are not running by satisfying all of the following Requirements 1 through 3.

Requirement 1:

All services enabled by default (such as background processes, kernel extensions, commands, programs, or tools) shall be the minimum necessary for the intended use, operation, or required services of the target device.

Requirement 2:

The product shall not respond to requests that could be used to exploit it as a jump host/jump server for denial-of-service attacks (at a minimum, the NTP monlist command, DNS `ANY` requests, and UPnP SSDP). Additionally, the product shall use a patched version that has been addressed reflection attacks.

However, elements that are necessary for communication and cannot be mitigated (such as SYN- ACK) may be excluded from these measures.

Requirement 3:

Unnecessary services on LAN and WAN interfaces shall be disabled by default.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-27

STAR-3 Security Requirements

Manufacturers shall employ code minimization practices in implementing and testing software deployed in IoT products.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

As part of secure coding, to minimize code, manufacturers shall adopt a technique similar to either A) or B) below.

A) Automated tools (static analysis tools, compilers, etc.) shall be used to identify and remove dead code, unnecessary debug code, and unused code.

B) Package managers, etc., shall be used to install only the components necessary for operating the service or software.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Code Covered by Conformance Requirements

The code subject to these conformance requirements is limited to source code developed in-house. Third-party components, such as OSS, are excluded.

2.2. Term

Not Applicable

Security Requirement Number: S3.1-28

STAR-3 Security Requirements

Manufacturers shall design and implement software deployed in IoT products based on the principle of least privilege. Specifically, all of the following requirements shall be satisfied.

(1) Minimization of default privileges

Default privilege settings shall be kept to the minimum necessary to ensure that unnecessarily broad privileges are not granted.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To reduce the risk of cyberattacks, as a means of verifying that software access permissions can be configured in accordance with the principle of least privilege, the default permissions for daemons, processes, etc., shall be configured to the minimum necessary level.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. This is an example of minimizing privileges in default settings.

- Example 1: A minimal number of daemons and processes running with "root" privileges. In particular, processes that use network interfaces shall run as non-privileged users rather than the "root" user.
- Example 2: Software running on devices that include multi-user operating systems (e.g., Linux®) uses different users for each component or service.

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-29

STAR-3 Security Requirements

During the implementation and testing phases of the product, secure coding practices shall be implemented and reviewed against the source code created. Specifically, at a minimum, the following practices shall be included.

(1) Security-conscious coding conventions and implementation principles shall be prescribed.

(2) Coding conventions shall be notified to engineers and training shall be provided.

(3) The codes created shall be reviewed and security testing shall be conducted.

(4) Coding conventions and implementation principles shall be updated.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To confirm that software development was conducted using secure coding practices, all of the following Requirements 1 through 5 shall be satisfied.

Requirement 1:

Security-conscious coding conventions and implementation principles shall be specified.

Requirement 2:

There shall be a process to notify engineers with the coding conventions and provide training on them.

Requirement 3:

There shall be a process to review and perform security testing on the source code that has been created.

Requirement 4:

There shall be a process for updating coding conventions and implementation principles.

Requirement 5:

The developed source code shall be created through the processes described in Requirements 1 through 4 above.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Code Covered by the Conformance Requirements

The source code subject to these conformance requirements is limited to source code developed

in-house. Third-party components, such as OSS, are excluded.

2.1.2. Security-conscious coding conventions and implementation principles

The evaluation will confirm that manufacturers have established coding conventions in accordance with best practices by referring to the reference documents listed below.

- Secure Programming Course (IPA) (in Japanese only): https://www.ipa.go.jp/security/awareness/vendor/programming/index.html
- How to Build a Secure Website (IPA) (in Japanese only): https://www.ipa.go.jp/security/vuln/websecurity.html
- Secure Coding (JPCERT/CC) (in Japanese only): https://www.jpcert.or.jp/securecoding/
- SEC BOOKS ESCR Ver. 3.0: Coding Practices Guide for Embedded Software Development [C Language Edition] ESCR Ver. 3.0 (IPA) (in Japanese only): https://www.ipa.go.jp/sec/publish/tn18-004.html

2.2. Term

Not applicable

Security Requirement Number: S3.1-30

STAR-3 Security Requirements

When incorporating third-party components into IoT products, a process that satisfies all of the following requirements (1) and (2) shall be adopted to ensure that known vulnerabilities are not included.

(1) Vulnerabilities shall be managed with respect to third-party components that are clearly used.

(2) When vulnerabilities are detected, appropriate action shall be taken.

Conditions for being Not Applicable (NA)

Third-party components are not used in the target IoT products. (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that no third-party components are used.)

1. STAR-3 Conformance Requirements

To ensure that no vulnerable third-party components are used, in conjunction with S3.1-15, both Requirement 1 and Requirement 2 below shall be satisfied.

Requirement 1:

In accordance with Requirement 2 of S3.1-15, an SBOM shall be created for the third-party components in use.

Requirement 2:

During the development phase of firmware (software) packages, the SBOM created in Requirement 1 shall be used to incorporate only third-party components that are free of vulnerabilities.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Category 7: Ensuring Software Integrity

Security Requirement Number: S3.1-31

STAR-3 Security Requirements

Secure boot mechanisms shall be implemented for IoT products to verify the integrity of software loaded during the system startup process.

Examples of secure boot mechanisms include the following. An implementation similar to any of these shall be conducted.

A) Verification of digital signatures

B) Security measures equivalent to digital signature verification

Conditions for being Not Applicable (NA)

Not applicable

1. **STAR-3 Conformance Requirements**

As a secure boot mechanism to satisfy the STAR-3 Security Requirements for software loaded at system startup, all of the following Requirements 1 through 4 shall be satisfied.

Requirement 1:

A secure boot mechanism that employs digital signatures or equivalent measures shall be implemented.

Requirement 2:

The implemented secure boot mechanism shall be suitable for providing assurance of the software integrity.

Requirement 3:

When using digital signatures or cryptography, the cryptography specified in the "e-Government Recommended Ciphers List" within "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) shall be adopted, and shall use key lengths that comply with the provisions of the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)."

Requirement 4:

Information detailing setup procedures for using secure boot shall be available to users.

2. **Supplementary Explanation**

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Certificates Used for Verifying Digital Signatures

The certificate used to verify digital signatures under Requirement 1 shall be a certificate whose reliability is ensured. At a minimum, it shall be possible to verify that manufacturers are legitimate. Such certificates include public certificates, root certificates managed by manufacturers themselves, or root certificates issued by a CA contracted by manufacturers.

2.1.2. Scope of Requirements for Secure Boot

The secure boot mechanism is not required to include functions to verify software authenticity.

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Category 8: Ensuring that Personal Data is Secure

Security Requirement Number: S3.1-32

STAR-3 Security Requirements

Manufacturers shall take measures to satisfy the following requirements when IoT devices perform sensing.

(1) For information to be sensed, the purpose of collection and the overview of functions shall be described in the user manuals, etc., which can be easily understood.

Conditions for being Not Applicable (NA)

In case the IoT device does not have a sensing function. (It shall be stated in the "Reasons for being Not Applicable (NA)" that there is no sensing function.)

1. STAR-3 Conformance Requirements

All categories of personal information collected by Network Devices shall be explicitly stated in media accessible to users, such as manuals or websites. In particular, if personal information is collected for purposes other than those related to audit logs for auditing purposes, the purpose of collection and an overview of the functions shall be explained to users in an easy-to-understand manner for each category of personal information collected.

Note that this conformance requirement applies to all personal information, regardless of whether it is collected by default.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Examples of sensing functions anticipated in Network Devices: Biometric sensors used for multi-factor authentication, etc.

2.2. Term

Not applicable

Category 9: Making the System Resilient to Outages

Security Requirement Number: S3.1-33

STAR-3 Security Requirements

When the power supply and network function are turned off and restored due to a power outage or other reasons, the authentication values (passwords, private keys, etc.) used for access control and the software that has completed the setting and updating shall maintain the state immediately before the power was turned off without returning to the factory default settings.

Conditions for being Not Applicable (NA)

Not applicable.

1. STAR-3 Conformance Requirements

To ensure compliance with STAR-3 security requirements in the event of an unexpected system failure, the state management function shall satisfy all of the following Requirements 1 and 2.

Requirement 1:

When power is restored after the power supply suffers an outage (for battery-powered products, this is achieved by removing the battery to cause the outage), the device shall not revert to its factory default settings, and the authentication values, configuration information, and update status stored in the IoT device shall be retained.

Requirement 2:

After forcibly being disconnected from a communication cable or wireless connection and then reconnected, the device shall not revert to its factory default settings; instead, the authentication values, configuration information, and update status stored in the IoT device shall be retained.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-34

STAR-3 Security Requirements

IoT products shall implement a backup function that can correctly retain and restore configuration information at specific times.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To ensure that the device can be restored to its configuration state at a specific point in time, the backup measures for configuration information, which are intended to satisfy STAR-3 Security Requirement, shall satisfy all of the following Requirements 1 through 3.

Requirement 1:

The product shall have a backup function, and the configuration information immediately prior to the backup (including configuration values and authentication values determined to require backup) shall be saved in the backup file.

Requirement 2:

It shall be possible to restore the product to the state immediately prior to the backup using only backup files properly saved by the backup function.

Requirement 3:

Users shall be informed that if backup and restoration are performed using different firmware versions, the IoT device may not function properly, and that backup and restoration shall be performed using the same firmware version.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Category 10: Verifying and Protecting System Telemetry Data

Security Requirement Number: S3.1-35

STAR-3 Security Requirements

In order to detect security anomalies, IoT products shall implement the ability to record logs (telemetry data and audit logs). Specifically, all of the following requirements (1) through (3) shall be satisfied.

(1) Functions of acquiring and storing logs (telemetry data and audit logs) shall be implemented for IoT products. At a minimum, logs (telemetry data and audit logs) generated by firmware (software) or OS shall be acquired and stored. The target of security events to be recorded includes records of disconnections (reconnections) of devices and networks, records of login attempts (successful and unsuccessful attempts), records of login attempts that exceed threshold values, records of time changes (including time before and after the change), and records of the use of management functions, including acquisition and restoration of backups, records of software changes, records of hardware changes (when audit logs can be acquired), firewall operation status records (when firewall function is implemented), and remote management service operation status records (when CWMP, etc., is enabled).

(2) Logs (telemetry data and audit logs) shall have the necessary capacity for auditing, and if the storage capacity is exceeded, administrative measures shall be taken, such as sequentially overwriting older records. Note that the required storage capacity shall be separately reviewed based on the intended use of each product.

(3) The time management function shall be provided to record the date and time of security events on logs (telemetry data and audit logs).

Conditions for being Not Applicable (NA)

Not applicable

1. **STAR-3 Conformance Requirements**

To be used for detecting security anomalies, as a protective measure for logs (telemetry data and audit logs) to satisfy STAR-3 Security Requirements, the product shall satisfy all of the following Requirements 1 through 4. If the associated services include a function to store logs on external storage, it shall satisfy Requirement 5 in addition to Requirements 1 through 4.

Furthermore, if the product has a function to store logs in an external system through integration with systems other than the associated services, it shall satisfy Requirements 5 and 6 in addition to Requirements 1 through 4.

Requirement 1:

Log acquisition and storage functions covering all of the following security events shall be

implemented.

A) Records of device and network disconnections (and reconnections)
B) Records of login attempts (both successful and failed)
C) Records of login attempts exceeding the threshold
D) Records of time changes (including the times before and after the change)
E) Usage logs for administrative functions, including backup acquisition and restoration
F) Records of software changes
G) Records of hardware changes (if the product has a function to log configuration changes)
H) Records of firewall operation status (if a firewall function is implemented)
I) Records of remote management service operation status (if CWMP or similar is enabled)

Requirement 2:

It shall be clearly stated in technical documents, etc., that the storage capacity for the logs to be acquired, as well as the procedures that will be followed if the storage capacity is exceeded. Furthermore, even when logs are stored on external storage via associated services or integration with external systems, it shall be ensured that there is sufficient storage space within the IoT device to store at least "approximately one day's worth of logs under normal usage conditions" in case logs cannot be saved to external storage due to a communication failure.

Requirement 3:

If the logs exceed the storage capacity, a warning message or notification shall be displayed in a manner easily visible to the user.

Requirement 4:

Time management functions for recording the date and time of security events in the logs, as well as time synchronization functions using a time source, shall be implemented.

Requirement 5:

If the product has the function to store logs in external systems, such as external storage, through associated services or integration with external systems, it shall satisfy all of the following requirements.

A) For communications related to logs with associated services or external systems, settings that satisfy Requirements 1 through 3 of S3.1-20 shall be enabled by default.
B) When a communication failure is resolved, the product shall automatically send the stored logs to the associated services or external systems.

Requirement 6:

If the product has a function that stores logs in external systems through integration with external systems other than the associated services, all of the following requirements shall be satisfied.

A) A document specifying the conditions under which integration with reliable external systems for log storage is possible shall be provided to users. At least one of these conditions shall be technically verifiable.
B) IoT devices shall have a function to verify that external systems with which they integrate for log storage satisfy the technically verifiable conditions specified in A).
C) The functions and measures described in B) shall be enabled by default.
D) Procedures for integrating with external systems using the functions described in B) shall be disclosed in media accessible to users, such as IoT product manuals and websites.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Audit Logs for Hardware Changes Due to Configuration Changes

The phrase "when audit logs can be acquired" in "records of hardware changes (when audit logs can be acquired)" refers to cases where, for IoT devices capable of adding or modifying units or modules, such as those involving changes to functions like interfaces or storage, the device possesses a function to record logs of configuration changes when units or modules are added, replaced, or removed, and where such records of hardware changes can be used as audit logs.

2.2. Term

[telemetry data]

It refers to data from devices which can provide information that can help manufacturers identify problems or gather information regarding the use of products.

[audit log]

It refers to data that records product processes and operations in a chronological and continuous manner in order to enable the detection of security anomalies in products.

Category 11: Allowing Users to Easily Erase Data

Security Requirement Number: S3.1-36

STAR-3 Security Requirements

All of the following requirements (1) and (2) shall be satisfied for the deletion function of data stored in the storage of IoT products during the use of IoT products.

(1) It shall be possible to delete at least the following data related to users via the IoT device itself or associated services (e.g., mobile applications) by users.

A) Information assets (including personal information) acquired while using IoT products

B) User configuration values

C) Authentication values set by users, encryption keys and digital signatures acquired while using IoT products

(2) The version of the firmware (software) package related to the updated security functions shall be maintained even after the data is deleted.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

For information stored on the storage device during product use, as a data deletion function to satisfy STAR-3 Security Requirements, the product shall satisfy "all of Requirements 1 through 3" or "all of Requirements 4 and 5," and also satisfy "Requirement 6."

Requirement 1:

The product shall have a function that allows users to delete at least all of the following information (data) regarding users A) through C) stored in the product's storage during use, as well as all personal information specified in S3.1-32. However, even if it pertains to the user, configuration information for the IoT product that is not disclosed to the user (information necessary for the product's functions) and technical data generated by the manufacturer to monitor the performance or system health of the IoT product are excluded from the scope of information that the user can delete (e.g., Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.), battery charge cycle count, error history, etc.).

A) Information assets (including personal information) acquired while the user is using the IoT products

B) User-configured settings

C) Authentication values set by the user, as well as cryptographic keys and digital signatures acquired while using IoT products

Requirement 2:

Data shall be deleted appropriately according to its intended use and the storage medium on which it is stored. The deletion level shall be "Clear" or higher, a level that can withstand simple, non-invasive data recovery techniques (such as salvage using commercially available data recovery software).

Requirement 3:

The instruction shall be provided to users on how to use the deletion functions described in Requirement 1 via media accessible to users, such as manuals.

Requirement 4:

For IoT devices or associated services that store information (data) falling under Requirement 1, and only in cases where it is impossible or difficult for users to resell such IoT devices or associated services on their own, contact information and procedures for requesting specialized service providers or IoT product vendors to delete such information (data) shall be provided in a manner that allows users to easily access them.

Requirement 5:

In cases where, pursuant to Requirement 4, a specialized service provider or vendor of IoT products deletes information (data) on behalf of the user, a process shall be established to verify that the party performing the deletion is deleting the information (data) at the "Clear" level or higher, a level that protects the data from simple, non-invasive data recovery techniques (such as salvage using commercially available data recovery software).

Requirement 6:

Even after data deletion, the version of the firmware (software) package containing updated security functions shall be maintained.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Category 12: Facilitating Product Installation and Maintenance

Security Requirement Number: S3.1-37

STAR-3 Security Requirements

IoT devices shall be able to restore secure default configuration settings.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

As a mechanism for restoring the device to its secure default configuration settings to be its initial state when necessary, the device shall satisfy all of the following Requirements 1 through 3.

Requirement 1:

The product shall have a function to restore the default configuration settings.

Requirement 2:

Procedures for restoring the system to the secure default configuration settings shall be provided to users via a medium accessible to them, such as a manual.

Requirement 3:

The procedure for restoring to the default configuration settings shall include steps to delete information prior to restoration using the function described in Requirement 1 of S3.1-36. It does not matter whether the steps in are performed automatically or manually.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. "Secure default configuration settings"

"Secure default configuration settings" refer to the secure configuration and settings specified by manufacturers.

Example of "restoring to secure default configuration settings": Settings modified by users, other than updated firmware, and configuration information changed during operation are restored to their factory default state.

2.2. Term

Not applicable

Category 13: Checking the Validity of Input Data

Security Requirement Number: S3.1-38

STAR-3 Security Requirements

For all interfaces of the IoT product, a function to verify the validity of input data and to reject requests if the input data is invalid and unauthorized shall be implemented.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

For input data, as a measure to reject unauthorized input in order to satisfy STAR-3 Security Requirements, all of the following Requirements shall be satisfied.

Requirement 1:

A list of all interfaces that accept and process input data shall be created. This list shall include at least the following:

A) User interfaces that allow data input from users

B) Application Programming Interfaces (APIs) that allow data input from external sources

C) Network interfaces that are remotely accessible and allow data input

Requirement 2:

For each interface listed in Requirement 1, the input rules for input data and contents of validation are defined. The contents of validation include the following:

A) Correct type (permitted data formats and data structures)

B) Permitted input value ranges, radix, and ordering

C) Permitted input radix

D) Permitted input order

E) Methods for handling invalid data, such as sanitization, escaping, and discarding

Requirement 3:

The input validation function shall operate as specified to reject invalid and unauthorized requests.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Reference document on input data validation:

OWASP "Input Validation Cheat Sheet"

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_She et.html

2.2. Term

Not applicable

Category 14: Processing Personal Data Appropriately

Security Requirement Number: S3.1-39

STAR-3 Security Requirements

Manufacturers shall explain what personal data is collected, how it is processed, and what functions are implemented to process it if personal data obtained from IoT products is processed.

Conditions for being Not Applicable (NA)

In case IoT products do not have a function to collect or process personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have a function to collect or process personal information.

1. STAR-3 Conformance Requirements

If a device has functions to collect and process personal information, in order to limit the processing of personal information to the minimum necessary for its intended purpose, all of the following Requirements 1 through 5 shall be satisfied as part of the information to be disclosed to satisfy STAR-3 Security Requirements.

Requirement 1:

All categories of personal information collected by IoT products for the purpose of processing personal information shall be explicitly stated in technical documents, etc.

Requirement 2:

The technical documents, etc., shall explicitly state the specific processing operations performed on all categories of the collected personal information as specified in Requirement 1.

Requirement 3:

The technical documents, etc., shall explicitly specify the handling methods (such as storage, disclosure, notification, and deletion) applied to the results of the processing described in Requirement 2.

Requirement 4:

Materials that clearly explain Requirements 1 through 3 to users shall be provided through media accessible to users, such as manuals or websites, etc.

Requirement 5:

Personal information not covered by Requirement 2 or S3.1-32 shall not be included in Requirement 1.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-40

STAR-3 Security Requirements

When IoT products collect logs (telemetry data, audit logs) and contain personal information (including information related to individuals), the collected personal information shall be limited to the minimum necessary to achieve the purpose of audits

Conditions for being Not Applicable (NA)

In case the logs do not contain personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that logs do not contain personal information.

1. STAR-3 Conformance Requirements

When logs (telemetry data, audit logs) are collected in a form that includes personal information (including personally identifiable information), the following Requirements 1 through 3 shall all be satisfied as a mechanism to satisfy STAR-3 Security Requirement.

Requirement 1:

All categories of personal information contained in the logs shall be explicitly stated in technical documents, etc. Note that if logs are used for purposes other than auditing, this shall also be documented in S3.1-39.

Requirement 2:

The purposes for which the personal information specified in Requirement 1 is used in audits shall be explicitly stated in technical documents or similar documents.

Requirement 3:

The scope of collection of the personal information specified in Requirement 1 shall be limited to the minimum necessary in light of the purposes specified in Requirement 2.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Security Requirement Number: S3.1-41

STAR-3 Security Requirements

When IoT products process personal information, they shall have a function to delete personal information that is no longer needed in order to limit the scope of collection and processing.

Conditions for being Not Applicable (NA)

In case IoT products do not have a function to collect or process personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have a function to collect or process personal information.)

1. STAR-3 Conformance Requirements

If the product has the function to collect and process personal information, it shall satisfy both of the following Requirement 1 and Requirement 2 as the deletion function required to satisfy STAR-3 Security Requirements.

Requirement 1:

The IoT product shall have a function that allows users to delete their personal data and processing results when the collected personal data is no longer needed (based on specific time periods, frequency of use, completion of processing, or user-specified data, etc.). However, personal data collected for the purposes of S3.1-40 may be subject to deletion only by the administrator.

Requirement 2:

Personal information and processing results shall be deleted appropriately depending on the storage on which they are stored. The deletion level shall be "Clear" or higher, a level that can protect against simple, non-invasive data recovery techniques (such as salvage using commercially available data recovery software).

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Category 16: Identifying and Testing Threats

Security Requirement Number: S3.1-42

STAR-3 Security Requirements

Manufacturers shall resolve any security issues detected as a result of third-party penetration testing.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

As a result of the penetration tests conducted by the JC-STAR Evaluation Body, either no security issues shall be reported, or all reported security issues shall be resolved.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

2.1.1. Penetration Tests

For details on the penetration tests that need to be conducted, refer to Section 2.10.

2.2. Term

Not applicable

Category 17: Providing Information on Products

Security Requirement Number: S3.1-43

STAR-3 Security Requirements

Product security-related information provided to users shall be in the specified language.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

As a general rule, security-related information shall be provided to users in Japanese. If the primary information is created in a language other than Japanese, the information shall be provided in that language, and a Japanese version, a simplified Japanese version, or a translated version shall be provided without delay. In particular, if IPA or a government-related agency requests that information be provided in Japanese, the request shall be addressed promptly.

However, for products covered by mutual recognition with JC-STAR, provision in English is permitted.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[user]

The scope of users shall include all natural persons and organizations that have access to and use the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-44

STAR-3 Security Requirements

Manufacturers shall take measures that satisfy all of the following Requirements (1) through (5) in regard to providing information on the security of IoT products.

(1) The procedures for secure use of IoT products, such as initial setup methods, etc., and usage methods that could impact security in the use of IoT products, shall be made known.

(2) The structure shall be implemented to inform the public of the contents and necessity of security updates for IoT products when such updates are released, as well as the consequences of not updating.

(3) Disclaimers of liability shall be made known for accidents and failures assumed or generally expected when updates are not performed.

(4) The policy for the support expiration date or termination of support for the target product or service shall be made known to the public.

(5) The risks assumed when disposing of or selling used IoT products with securely stored information remaining in the IoT products, and the secure termination method of using IoT products including data erasure, shall be made known.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

Regarding the provision of security-related information, the content to be communicated to satisfy STAR-3 Security Requirements shall satisfy all of the following Requirements 1 through 5.

Requirement 1:

Information shall be made available to users that outlines secure usage procedures for settings and usage methods that affect security, such as initial setup methods and password change procedures.

Requirement 2:

The mechanism and implementation methods shall be implemented to inform users about the content and necessity of security updates, the consequences of not applying them, and the implications of enabling services that are disabled by default. Specifically, the media and methods used to notify users of necessary information when security updates are released, as well as the department responsible, etc., shall be clearly defined.

Requirement 3:

When providing security updates, there shall be a process in place to publicize, in a location where

users can easily access and review the information, disclaimers regarding incidents and outages that may occur if the update is not applied, as well as disclaimers regarding generally foreseeable incidents and outages.

Requirement 4:

Security updates shall be provided free of charge during the validity period of the conformance label. However, this does not apply if the product is not sold or provided unless a maintenance contract is concluded.

Requirement 5:

In a location easily accessible and verifiable by users, the risks associated with disposing of or reselling IoT products while residual securely stored information remains within them, as well as methods for securely ending the use of the product, including data erasure, shall be explained.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[securely stored information]

Refer to the following information. Refer to Section 2.4.

- CSP (Critical Security Parameter)
- PSP (Public Security Parameter)
- Configuration information related to communication functions
- Configuration information related to security functions
- Program code
- Logs (telemetry data and audit logs)

Category 19: Ensuring Product Availability

Security Requirement Number: S3.1-45

STAR-3 Security Requirements

IoT devices shall have a mechanism to recover from network overload state caused by denial-of-service attack.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

To satisfy the STAR-3 Security Requirements, after a network overload state caused by a denial-of-service attack on an IoT device (such as recovery from depletion of memory or CPU resources) has been resolved, the Network Devices' functions shall automatically return to normal operation.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

[network overload state]

A state where the network is overloaded, preventing Network Devices from functioning normally.

Category 21: Ensuring Hardware Integrity

Security Requirement Number: S3.1-46

STAR-3 Security Requirements

To prevent unauthorized access to components and interfaces in devices through physical destruction or modification of the enclosure, a mechanism to improve the tamper resistance of the enclosure shall be implemented.

Conditions for being Not Applicable (NA)

Not applicable

1. STAR-3 Conformance Requirements

Regarding the tamper resistance of the enclosure, to satisfy the STAR-3 Security Requirements, a mechanism shall be implemented, equivalent to or exceeding all of the following, to protect the enclosure from physical destruction or modification.

A) It shall be a reinforced enclosure (using high-strength materials or structures, etc., for the enclosure). Specifically, it shall have an impact-resistant (vandal-resistant or proof) structure that satisfies IEC 62262 Protection Class IK08 (5.0 J) or an equivalent or higher standard.

B) It has a structure (*1) that cannot be easily opened with bare hands or a Phillips or flathead screwdriver.

(*1): Security screws (special screws or bolts that cannot be removed with standard tools) shall be used.

2. Supplementary Explanation

2.1. Supplementary Explanation of Conformance Requirements

Not applicable

2.2. Term

Not applicable

Appendix A: Revision History

June 10, 2026: Version 1.0 (2026) published