Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Assessment Supplementary Guidance

May 22, 2025

Information-technology Promotion Agency, Japan (IPA)

Table of Contents

Introduction

This Supplementary Guidance is intended to provide answers to the questions received after the publication of the "STAR-1 Conformance Requirements and Assessment Methods (JST-CR-01-01-2024/2024R1)" and the "STAR-1 Assessment Guide (JST-EG-01-01-2024/2024R1)" regarding the assessment methods required in those methods, interpretation of assessment items, etc.

This information may be incorporated into the next revision of the Assessment Guide but is compiled as a preliminary report and shall be referred to in conjunction with the Assessment Guide.

Revision History

Revision date	**Contents**
May 22, 2025.	First edition published

[STAR-1 Conformance Requirement Concept]

[Question 00-1]

What kind of information is specifically assumed to be "configuration information related to IoT functions (communication functions)," which is given as an example of "information assets to be protected in STAR-1" in Section 2.4 "Concept of Information Assets to be Protected" of STAR-1 Assessment Guide?

In Appendix A, the Glossary lists WiFi SSIDs and WPA encryption keys as examples for wireless communication. Shall configuration information such as IP addresses and host names of control servers and information servers for controlling IoT devices also be considered applicable?

[Guidance]

The "configuration information related to communication functions" assumes all the configuration information used in using the communication functions during the operation of IoT devices.

In addition, "protection" does not only mean "protection of confidentiality," but also mean "protection of integrity" and "protection of authenticity." For each setting information, it is required to determine what kind of protection is necessary in terms of confidentiality, integrity, and authenticity, and to take the necessary measures. However, depending on the results of the review, it may be determined that the configuration information does not require protection.

For example, even the same IP address may be divided into "configuration information to be protected" and "configuration information that does not require protection." As an example of the former, if the IP address of a control server is read from an IoT device, the IP address of an "update file provision server" may be applicable in the sense that the control server may be attacked next. On the other hand, an example of the latter would be the IP address of a "public server" whose IP address itself is publicly known.

As such, even if it is configuration information related to communication functions, it is considered that whether it is configuration information that requires protection may vary depending on the product status and type of configuration information. Therefore, the “configuration information related to communication functions” is considered as a “**candidate for information that should be considered for protection**” and “**selecting configuration information that need to be protected by the vendor**” from that list.

For configuration information that is determined to require protection, appropriate protection measures shall be applied. For configuration information that does not require protection, a record of the rationales and reasons for not requiring protection shall be kept as evidence in the technical documents, etc.

[Question 00-2]

Are all the information assets listed in the examples in Section 2.4 "Information Assets to be Protected" of the STAR-1 Assessment Guide required to be protected?

If some of the information "collected, stored or communicated by the device" includes "generally sensitive information," is it necessary to include other information and treat it as "information assets to be protected"?

[Guidance]

The information assets listed in the examples of "information assets to be protected" are "**candidate for information that should be considered for protection,**" and it does not mean that all the information assets listed there must be protected. Depending on the nature of the information collected by the device, "**the vendor is responsible for examining whether the information assets require protection or not**" and "**selecting the information assets that need to be protected**." For the information assets that are determined to require protection, appropriate protection measures shall be applied. For the information assets that are determined not to require protection, a record of the rationales and reasons for not requiring protection shall be kept as evidence in technical documents, etc.

In relation to the above, if some of the information collected, stored, or communicated by a device includes "generally confidential information," the vendor may determine whether or not to treat such information as "information assets to be protected" based on the extent to which "generally confidential information" is included in the information collected, stored, or communicated by the device, in light of the main usage environment and purpose of the device.

For example, if the device is intended for general consumer use and, based on the main usage environment and purpose of the device, it can be reasonably assumed that most of the information collected, stored, or communicated by the device is "information that is not generally considered confidential," then even if the device may contain "generally confidential information," it is acceptable to determine that all information collected, stored, or communicated by the device is information assets that do not require protection. On the other hand, if the device is an enterprise-grade device and the information it collects, stores, or communicates is expected to contain a non-negligible amount of "generally confidential information," then all information collected, stored, or communicated by the device should be considered information assets that require protection.

[Question 00-3]

To what extent does the checklist need to cover functions that users can change their availability by changing their settings?

[Guidance]

Functions that require conformance assessment using the checklist shall be **enabled by default**, and those that are disabled by default are not subject to the assessment.

However, in the section explaining the settings changes (e.g., manuals), any security precautions, such as risks or functional limitations, that may result from changing settings shall clearly be indicated to users.

[Question 00-4]

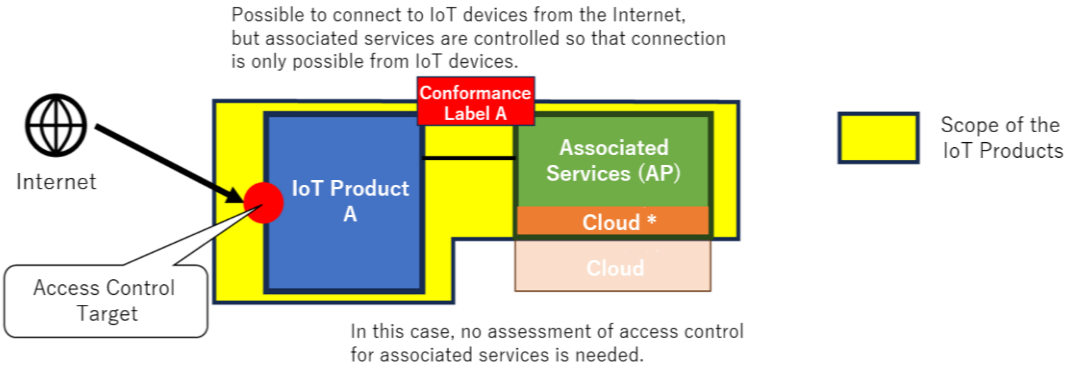
Are the following assessment items required for "associated services" correct?

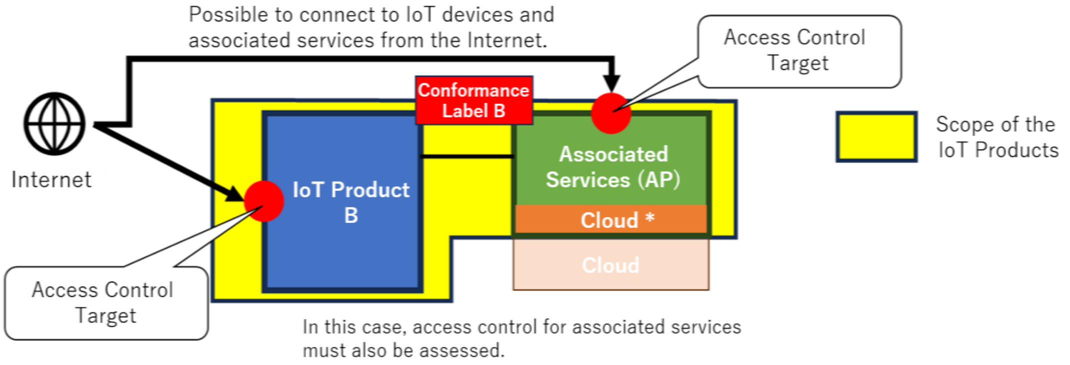
- Protection of authentication for "information assets to be protected" on "associated services" accessed from IoT devices subject to conformance label acquisition.
- Protection of "information assets to be protected" stored in "associated services."
- Measures against eavesdropping of communications via the Internet between IoT devices subject to conformance label acquisition and "associated services."
- Deletion of data on "associated services."

[Guidance]

It depends on **whether the Internet can directly access the associated services**. Direct access to "associated services" from the Internet means, for example, this could involve accessing associated services provided via the Internet from outside home, such as on the cloud, and operating IoT devices from those services. In this case, access control is required on the side of the associated services.

Therefore, if access to associated services is only possible from the IoT device side, the above four assessments apply. However, if access to associated services is also possible directly from the Internet side, access control on the "associated services" side shall also be included in the assessment.


Possible to connect to IoT devices from the Internet, but associated services are controlled so that connection is only possible from IoT devices.
Internet
Conformance Label A
IoT Product A
Associated Services (AP)
Cloud *
Cloud
Access Control Target
Scope of the IoT Products
In this case, no assessment of access control for associated services is needed.


Possible to connect to IoT devices and associated services from the Internet.
Access Control Target
Internet
Conformance Label B
IoT Product B
Associated Services (AP)
Cloud *
Cloud
Access Control Target
Scope of the IoT Products
In this case, access control for associated services must also be assessed.

[Question 00-5]

In the assessment item, it is stated that the algorithms are those listed in the "e-Government Recommended Ciphers List" among the "List of Ciphers to be Referenced for Procurement in e-Government (CRYPTREC Ciphers List)." Is it not allowed to use any other list?

In addition, is it safe to assume that there is no specification regarding the security strength of cryptography? Or do we need to follow the "https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf" in CRYPTREC's "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection) "?

[Guidance]

Among the CRYPTREC cryptographic algorithms, it is possible to adopt algorithms listed in the "Recommended Candidate Cryptographic Algorithms List" in addition to those listed in the "e-Government Recommended Ciphers List." The "Operational Monitoring Ciphers List" contains algorithms that have been approved for continued use to maintain compatibility, so adopting these algorithms shall be avoided as much as possible.

In addition, regarding the security strength of cryptography, make sure to follow the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)." Note that even if you adopt an algorithm listed in the "e-Government Recommended Ciphers List" of the CRYPTREC Cipher List, if you do not use it in accordance with the "Standards for Cryptographic Strength Requirements (Algorithm and Key Length Selection)," it will not be considered as using an algorithm from the e-Government Recommended Ciphers List.

[Question 00-6]

Can the application agent inform users through manuals, websites, etc.? Or does the applicant company have to do it?

[Guidance]

In principle, it shall **be done by the applicant company.**

However, it is acceptable for the said application agent to handle the **sales in Japan only when** the application agent **is exclusively conducting the sales in Japan** on behalf of the applicant company. This shall be explained in the checklist.

[Question 00-7]

Among the devices that do not use IP communication, are devices that do not have a TCP port but have unused USB/Bluetooth/D-sub, etc., applicable?

[Guidance]

If the device cannot use IP communication, it is not applicable. However, if IP communication is possible through USB, Bluetooth, etc., without a TCP port, it may be considered applicable.

[Question 00-8]

Does "physical contact during product operation" include contact with the control panel of the product device or near-field communication such as NFC?

[Guidance]

The phrase "no physical contact during product operation is assumed" does not refer to the type of contact method, but rather to the fact that an attacker will not enter the vicinity of the product (i.e., an attacker will not directly touch the operation panel, NFC, or USB on the device in operation). It is assumed that such an environment is in place.

On the other hand, "physical contact at disposal" includes contact with the control panel of the product device and near-field communication such as NFC, so countermeasures against them are necessary.

[Question 00-9]

Is it correct to assume that the measures of attack on "functions that can cause harm through malfunction or misuse" in "(4) Potential attack points" is limited to attacks via the Internet?

[Guidance]

In STAR-1, the attacks via the Internet shall be assumed.

[Question 00-10]

Necessary information will be announced on our website. If the website is not yet ready when I apply for the conformance label, can I apply only after the website is completed? Or would it be acceptable to provide the URL information to be posted and check "to be posted" on the checklist?

[Guidance]

It is acceptable to provide the URL information to be posted and indicate that it is "scheduled to be posted."

In this case, the schedule for when you plan to publish the information shall be included as well.

[STAR-1 Conformance Requirement S1.1-01]

[Question 01-1]

Is it correct to interpret that access control using NFC tools is considered access control based on appropriate authentication being performed?

[Guidance]

If NFC tools function as authentication by physical possession, and access to information assets to be protected via IP communication is not possible without NFC tools, access control by further implementation as described in "(2) an implementation similar to or more advanced than any of the following items" is recognized as being implemented.

On the other hand, even if "NFC use is required for IP address changes," if "other IoT devices or users can access information assets to be protected via IP communication (without using NFC tools)," then "NFC use" cannot be considered "access control based on appropriate authentication."

[STAR-1 Conformance Requirement S1.1-02]

[Question 02-1]

When introducing IoT products, how should I determine cases where the default password is "not used" (i.e., it can be read as not subject to conformance requirement) but "there is" a user authentication mechanism that uses passwords via a network (i.e., it does not satisfy the conditions for being Not Applicable (NA))?

[Guidance]

If the default password is not used, it shall be assessed as "a blank (i.e., a password with a length of 0 character) default password is being used."

[Question 02-2]

If an IoT device vendor sets a password before installation, and the user does not know the password, and the user does not perform any maintenance on the device, would this conformance requirement regarding the rules for setting the default password not apply?

[Guidance]

It will not be considered "Not Applicable (NA)." Refer to "2.2.1 Password handling for authentication of administrators and customer engineers" in "2.2 Conformance Decision in Exceptional Cases."

[Question 02-3]

In the case of a device that can only be connected after setting the connection information using an NFC tool instead of the default password, is it correct to interpret this as satisfying Requirement (2) without requiring a password change?

[Guidance]

"Access control using NFC" and "access control using passwords" are treated as two different methods.

In other words, if access is not possible without NFC use (no passwords are used), there is no “user authentication mechanism using passwords via a network,” and therefore it is not applicable to this conformance requirement."

On the other hand, if the configuration allows access by "using a password via a network (without using NFC)," a "user authentication mechanism using a password via a network" is required. In this case, the default password is interpreted as a 0-character password, and if there is no mechanism described in the Requirement (2), Assessment Item 2 will be considered non-conforming.

[STAR-1 Conformance Requirement S1.1-03]

[Question 1]

The authentication screen for IoT devices can be accessed via a network, but if this network is a closed network (VPN-SIM) that cannot be accessed by unspecified users, does it fall under "Not Applicable (NA)"? In other words, what kind of network is the "network" in "no mechanism for user authentication through the network for IoT devices"?

For example, if the remote access is via VPN-SIM (via a closed network) and the local network is a wired network within a locked and managed building, and the authentication screen cannot be accessed unless someone enters the building and directly touches the device, how can this be determined?

[Guidance]

Only when all the following conditions are met, a device can be exceptionally designated as being "Not Applicable (NA)" as a device without a mechanism for user authentication via a network. In this case, the rationales for the determination of being "Not Applicable (NA)" shall be clearly stated in the evidence.

i) When a connection is made through a network, it shall be confirmed that the connection can be made only through a closed network (VPN-SIM).

ii) The attention to the fact that the IoT device "shall be connected via a closed network (VPN-SIM) when used via a network" shall be clearly indicated.

[STAR-1 Conformance Requirement S1.1-04]

[Question 04-1]

Are measures to make brute force attacks difficult a necessary function (requirement) even if, for example, a VPN connection is used to block access from outside via the Internet?

[Guidance]

Only when all the following conditions are met, a device can be exceptionally designated as being "Not Applicable (NA)" as a device without a mechanism for user authentication via a network. In this case, the rationales for the determination of being "Not Applicable (NA)" must be clearly stated in the evidence.

i) When a connection is made through a network, it shall be confirmed that the connection can be made only through a closed network (VPN).

ii) A caution to the effect that "when such IoT devices are used via a network, they shall be connected via a closed area network (VPN)" shall be clearly indicated. Normally, this information shall be made known to users, but if the system is designed so that only the installation contractor, customer engineers, or system administrators can perform VPN connection settings and maintenance (e.g., locked management, built-in at the time of installation), it is acceptable to keep a record in technical documents.

[Question 04-2]

Are functions that are left in place to maintain compatibility with older models (disabled by default settings) not applicable to device checks?

[Guidance]

Those functions disabled by default settings are not applicable to device check.

However, security precautions such as risks and functional limitations associated with changing settings shall be clearly indicated to users in the section explaining the setting changes (e.g., manuals).

[Question 04-3]

If the certification trial restriction function is available but not enabled by default, would it be considered conforming if the user manual or other documentation recommends that users enable the confirmation trial restriction?

[Guidance]

The same approach is used as in Supplementary Explanation 2.2.2 of S1.1-12. In other words, in principle, if the system is not enabled by default, it is considered non-conforming. As an exception, it is considered conforming based on the explanation only if "the installation operator or system administrator performs the enabling process at the time of installation."

[Question 04-4]

In Assessment Item 1, the following three methods are stated as responses to restrictions on authentication attempts for consecutive failures of user authentication over the network.

A) Prohibition of additional authentication
B) Authentication outage for a certain period
C) Fixed time delay in issuing authentication response

Do I need to implement all of A to C for this response? Or is it sufficient to select and implement any one of them?

[Guidance]

If any one of these methods is implemented, it is considered conforming.

[STAR-1 Conformance Requirement S1.1-05]

[Question 05-1]

Regarding the disclosure of vulnerabilities of IoT devices, if I distribute IoT devices only to users who have signed a contract, is it acceptable to use the form of individual disclosure to users who sign a contract?

[Guidance]

Individual distribution to contractors is acceptable. However, the rationales for this shall be included in the checklist along with the reason why only distribution to contractors is acceptable. In addition, the vulnerability disclosure policy URL field of the application form shall be filled in with "Information not disclosed as this is a product distributed exclusively to contractors."

[Question 05-2]

In applying on behalf of an overseas product, is it acceptable to publish the vulnerability disclosure policy on the website of the applicant agent, since the website for Japan is managed by the applicant agent on behalf of the overseas product?

[Guidance]

It is acceptable to make reference information as Japanese and post it on the website of the applicant agent. However, the original text of the vulnerability disclosure policy must be posted on the applicant company's website, and a link to that information shall be provided, along with additional explanations of how the applicant agent will respond (in Japanese).

[Question 05-3]

What is a declaration of legal immunity for good faith reporting?

[Guidance]

It is a declaration by the manufacturing vendor of the extent to which it will tolerate conduct within the scope of the exemption in order to have the vulnerability reported. It is expected that no legal action will be taken against acts within that scope.

[STAR-1 Conformance Requirement S1.1-06]

[Question 06-1]

Regarding firmware package version verification, would it be sufficient to check the product (as a whole) in terms of granularity?

[Guidance]

The firmware to be stated on the application form is subject to version check. On the other hand, firmware not stated in the application form is not subject to version verification.

[Question 06-2]

Is it necessary to check the version of each OSS package in STAR-1?

[Guidance]

Version check of the firmware stated in the application form is required. Even if the firmware is multiple or OSS, all versions shall be checked as well.

[STAR-1 Conformance Requirement S1.1-07]

[Question 07-1]

In the Requirement, it is stated that "It shall be enabled for users to perform software updates in an easy and understandable procedure when applying updates." Is it correct to understand that this is not applicable to cases where updates are managed by maintenance personnel or the manufacturer?

[Guidance]

It will not be considered "Not Applicable" in such case.

However, it can be made conforming by organizing an update procedure that is actually performed and managed by maintenance personnel, etc.

[Question 07-2]

The Requirement states "When the product implements an update mechanism, the update shall be simple for the user to apply." However, the bottom of page 5 of the Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Conformance Requirements and Assessment Methods (JST-CR-01-01-2024/2024R1) defines "An 'IoT device' means an Internet-capable device that can send and receive data using the Internet Protocol (IP) and for which it is difficult for the user to easily add security software to the IoT device itself by installing software products or other means." This seems inconsistent. How shall this be interpreted?

[Guidance]

Updates are required to be able to be performed by users (or maintenance personnel, etc.) as a "basic product function" to address defects and vulnerabilities. In particular, S1.1-07 means that users must be able to easily implement updates. On the other hand, the condition that it is difficult to add security measures means that "it is impossible/difficult to embed other security software into the product."

In other words, the difference is that the former is supplied to the IoT products under the responsibility of the IoT manufacturing vendor itself, while the latter is available to those other than the IoT manufacturing vendor for those IoT products, and the former can be easily applied by the user, while the latter is difficult to apply.

[Question 07-3]

Is it correct to interpret that the security software referred to in the Conformance Requirement indicates software that has functions and processes that shall satisfy the security requirements of this Scheme?

[Guidance]

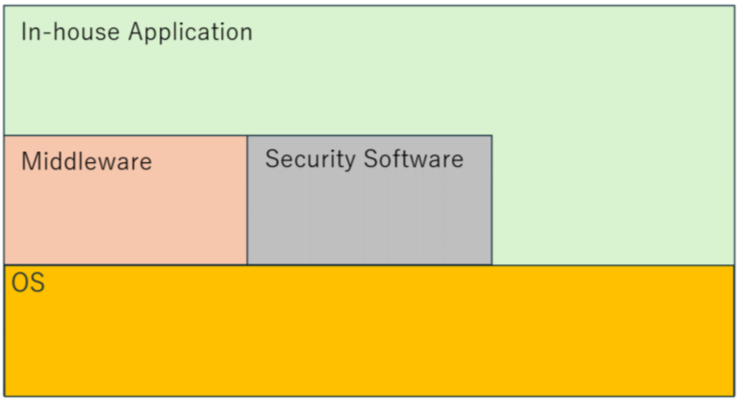
As a simple concept, software that is included in IoT devices from the beginning (excluding trial products, installers, etc.) is identified for use by the IoT manufacturing vendor and is not considered "additional security features by the customer" but rather "security functions" that are provided under the IoT manufacturing vendor's control. This is because it is assumed that, for such software, IoT manufacturing vendors will be able to determine the support status and users will be able to receive updates uniformly, either through some form of assurance that update files will be provided by the IoT manufacturing vendor or through the provision of alternative update methods.

On the other hand, for software created by third parties, users' usage status varies, and IoT manufacturing vendors cannot grasp the support status. Therefore, in such cases, this is considered to be “addition of security features by customers themselves” and is not applicable to JC-STAR.

Note that the OS update function that was included from the outset does not fall under "(addition of security functions) at your own discretion" but rather "(updates are performed) automatically." It is certainly possible to select “cancel,” but the reason for this is that the update will be enforced unless you intentionally cancel it.

The following is a concrete example to illustrate.

Figure 1: Software configuration of IoT devices



* Middleware, security software, and OS shall be general-purpose software. (e.g., OS: Windows, middleware: SQL server, security software: Virus Buster)

Example of Security Software Implementation

#A: STAR-1 security requirements are implemented entirely through in-house applications:
All security updates are provided by IoT device vendors.

#B: STAR-1 security software (for general purpose) with the ability to implement security Requirements:
Security updates can be applied at the user's discretion.

#C: All functions required to implement STAR-1 security requirements are realized in the OS (for general purpose):
Security updates can be applied to the updated OS at the user's discretion.

However, the update method shall be performed according to the procedure provided by the IoT device vendor.

#D: STAR-1 conformance label security requirements are implemented in both proprietary applications and general-purpose operating systems:
The security functionality to realize the requirements is composed of vendor-supplied in-house applications and a general-purpose OS, and depending on the required security updates, the procurer/user may or may not be able to update the security functions at their own will.

#E: STAR-1 conformance label security requirements are implemented outside of in-house applications:
Security updates can be applied by users on their own volition to updated software (security software, middleware, and operating systems) that is available on the market. General-purpose OS and middleware are constrained by vendor precautions that shall be taken in applying updates (e.g., application operations during/after update).

#A is applicable as firmware (software) support including security functions is required.

For #B and #E, if the security software is installed by the user, the vendor of the IoT device is not involved in any way with the security function and is therefore excluded from the scope. However, if the security software is fixedly installed as a product component, it is considered to incorporate a component supplied by another company as firmware (software) that "includes security functions" and is applicable.

Since #C and #D should have been identified by the IoT device vendor's involvement with the OS for the operation of the applications, they are considered to be fixtured under the control of the IoT device vendor and are applicable.

[STAR-1 Conformance Requirement S1.1-08]

[Question 08-1]

- Is it acceptable to conform to the S1.1-08 Assessment Requirement by using a combination of a proprietary difference file format and CRC checks as a means of verifying software integrity?
- Is encryption of firmware using hash values or digital signatures mandatory in order to conform to the Assessment Requirement in S1.1-08?

[Guidance]

In preparation for mutual recognition with similar schemes in other countries (e.g., Europe, the U.S., Singapore), we consider it desirable to keep the technical requirements equivalent to those in those schemes. For this reason, the mechanism used to verify the integrity of update files shall be cryptography. CRC is not recognized as cryptography and shall therefore be treated as non-conforming to the Assessment Requirement.

[Question 08-2]

Is it possible to conform to the Assessment Requirement in S1.1-08 by using HTTPS communication to download update software and CRC checks to verify the integrity of the downloaded software?

[Guidance]

If the update file is transmitted using a secure communication channel such as HTTPS, the integrity check before installation may be a CRC check.

In that case, both of the following as mechanisms for confirming completeness in the checklist shall be clearly indicated;

- Update files are downloaded using HTTPS communication (i.e. tamper-proof between the start and completion of the update file download).
- Integrity of the update file is verified by checksum (i.e. error prevention from the creation of the update file to the start of download).

In such a case, the confirmation of cryptography in S1.1-08, Assessment Item 5, the cryptography used for HTTPS communication shall be assessed.

The inclusion of both ensures that the update file is protected from tampering from the time it is created until the download is complete and assures a level of integrity equivalent to verification by digital signature or hash function, so it is considered satisfying the Assessment Requirement.

[STAR-1 Conformance Requirement S1.1-09]

[Question 09-1]

No questions asked.

[Guidance]

-

[STAR-1 Conformance Requirement S1.1-10]

[Question 10-1]

No questions asked.

[Guidance]

-

[STAR-1 Conformance Requirement S1.1-11]

[Question 11-1]

In the checklist of STAR-1 Assessment Guide published on the website of Ministry of Economy, Trade and Industry (METI), it is stated that "Information assets to be protected that require integrity protection shall be stored in a form where data integrity can be confirmed by message digests using hash functions listed in the 'e-Government Recommended Ciphers List' of the 'The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) '." and this has been removed.

As a result, it seems that the method of storing passwords in hashed form to protect their confidentiality can no longer be used. Is this understanding correct?

[Guidance]

This does not mean that hashing to protect the confidentiality of passwords can no longer be used. Hashing and storing passwords to protect password confidentiality can be considered conforming to Assessment Item 1.

[Question 11-2]

When NetworkManager is used to configure network connections such as Wi-Fi on an IoT device that uses Linux or other operating systems, NetworkManager stores network connection information (such as Wi-Fi SSIDs and passwords) in plain text on the file system. (However, since only the root user is granted access to this file, it can be said that a certain degree of protection is provided.)

If I consider Wi-Fi SSIDs and passwords to be information assets to be protected for their confidentiality, shall this information be stored and used in encrypted form?

[Guidance]

If appropriate access control is in place, protection measures similar to those in S1.1-11 Assessment Item 5, "a storage area that cannot be easily removed and is embedded in the IoT device, and on the storage area, data cannot be directly read" shall be used.

In particular, "The information assets to be protected shall be stored in the storage area, data cannot be directly read or written via an externally invoked interface or there is no such interface." can be interpreted as "stored in an area protected by access controls that restrict access to accounts protected by passwords, etc."

Therefore, to ensure the confidentiality of the information managed by NetworkManager, it is necessary to protect not only the root account, but also the general user account. For example, a configuration change that requires root privileges to execute the command nmcli, which operates NetworkManager, shall be made in conjunction with this change.

[Question 11-3]

Regarding "the information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media, such as SD cards, etc.) are securely stored,"

- User file data stored on NAS is generally stored unencrypted on the NAS file system (it is possible to remove the HDD and connect it to another PC to read the data). Is encryption required to acquire STAR-1?
- When an external USB drive is connected to a NAS to store user files, it is generally possible for the user to refer to the files by connecting the external USB drive to another PC, but this becomes difficult when encryption is implemented. Is encryption required to acquire STAR-1 in such a case as well?

[Guidance]

As for NAS, many products that can support encryption are already sold on the market, so encryption support is required by default.

However, this does not preclude the establishment of settings that allow users to disable encryption at their own will. In such a case, security precautions, such as the risks associated with unencrypted data, shall be clearly indicated to users in the section explaining the setting changes (e.g., manuals).

Note that the scope of the device check is limited to the part of the device that is enabled by default.

[Question 11-4]

Regarding "the information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media, such as SD cards, etc.) are securely stored;"

- When storing video data to an SD card attached to an NW camera, it is stored in a video format that can be played back on a PC without encryption, but encryption makes this difficult. Is encryption still necessary to acquire STAR-1 in such a case?
- If it is difficult to implement a function to employ and store cryptography on SD cards, is it acceptable to determine that the recorded information is stored securely as long as appropriate access controls are in place when viewing the recorded information?
- Is it acceptable to make a conformance decision when a device has a function that uses cryptography to store data on an SD card, but the function is disabled by default and its use is left to the user's decision?
- If the device has a function to store data to an SD card in encrypted form, but the default setting is to store data in unencrypted form, is it acceptable to include instructions in the manual or other documentation to enable encryption when the recording function is used for the first time, and determine this to be conforming?

[Guidance]

For storage on SD cards, the vendor can decide whether to make them subject to encryption or not subject to encryption, depending on the type of information assets to be protected, from the perspective of the device's intended use and convenience. In such cases, make sure that all the following responses are satisfied. If these are satisfied, it is considered "conforming."

1) In a place where users can easily check (e.g., instruction manual, user manual), it shall be explained whether representative data to be protected for the intended use of the device and data related to security are "subject to encryption" or "not subject to encryption" respectively. In particular, explanation of representative data "not subject to encryption" is required.

2) If the typical data to be protected as the intended use of the device is "stored unencrypted," a note to the effect that "typical data is stored unencrypted" shall be included in a place (e.g., package, brochure, website) where users can check before purchase.

3) If the user can select "encrypted" or "unencrypted" by changing the setting, the security precautions, such as the risk if the setting is not encrypted, shall be clearly indicated to users in the section explaining the setting changes (e.g., manuals).

[Question 11-5]

Regarding the area where direct data reading/writing via externally invoked interfaces is not possible in Section 2.1.3. in Assessment Item 5, it is stated that "An area where data cannot be directly read or written via an externally invoked interface is a storage area that data can only be read or written by software components that do not have an externally invoked interface (e.g., boot monitor, BIOS), and other software components cannot read/write, either directly or indirectly." Please provide the interpretation of this statement.

[Guidance]

"To be stored in the storage area where data cannot be directly read or written via an externally invoked interface or there is no such interface." is interpreted as "being stored in an area protected by access controls that restrict access to accounts protected by passwords, etc." In other words, when settings are saved, it is done by accessing the area with the authorization of access control by an account protected by a password, etc.

"Other software components" refers to "software components other than the software component that has the interface to control access to the area." "Indirectly" means any other software component without "a software component with an interface that controls access to the area," and does not include "a software component with an interface that controls access to the area."

[Question 11-6]

Regarding the secure storage methods for assets to be protected as assumed in STAR-1,

1) Is it correct to understand that the requirement of S1.1-11 is satisfied if the system is designed to allow information updating only through internal programs such as WebGUI, and if measures are implemented to make the system inaccessible through external interfaces?

2) If measures that can only be implemented by customer engineers are taken for troubleshooting or maintenance, is it correct to understand that the requirement of S1.1-11 is satisfied?

[Guidance]

"To be stored in the storage area where data cannot be directly read or written via an externally invoked interface or there is no such interface." is interpreted as "being stored in an area protected by access controls that restrict access to accounts protected by passwords, etc." In other words, when settings are saved, it is done by accessing the area with the authorization of access control by an account protected by a password, etc.

For both 1) and 2), implementation of access control (i.e., to whom and how access rights are granted, and whether measures are taken to prevent access to data storage areas by circumventing such access control) shall be checked.

[Question 11-7]

It is stated that "the following Assessment Items 1 to 5 or equivalent/better protection measures," but depending on the content of the information assets to be protected, it may be necessary to ensure both confidentiality and integrity. Even in such a case, would it be considered "Conforming (Y)" if any of the measures in Assessment Items 1 to 5 are taken? For example, even if only Assessment Item 1 is satisfied, doesn't it mean that integrity is not satisfied?

[Guidance]

If you have information assets that require different protection measures, you will need to assess each of them separately. Information assets that require confidentiality and integrity shall satisfy Assessment Requirements for both confidentiality and integrity.

[Question 11-8]

What does "via an externally invoked interface" in Assessment Item 5 refer to?

[Guidance]

Any interface that may allow external access to storage, bypassing the functionality that controls access to storage, falls under the category of "externally invoked interface." For more information, refer to Section 2.1.3 in the Assessment Guide S1.1-11.

[STAR-1 Conformance Requirement S1.1-12]

[Question 12-1]

What type of communication would fall under the "transmitted over a network" category?

Does this only apply to communications that are transmitted without the user's intention when the user is using the default settings? Or does it also apply to communication protocols such as syslog (RFC5424) or SNMPv1 which depending on the user's configuration may transmit information assets to be protected (system logs and login information for devices) to the Internet without any protection measures?

[Guidance]

Communications enabled by default settings are applicable, while those disabled are not applicable.

For items that can be used by changing the settings, any sections explaining configuration changes (e.g., manuals) shall clearly be indicated to users any security risks or functional limitations that may result from such changes.

[Question 12-2]

If a function is enabled by default to transmit via a communication protocol employing cryptography (such as https), but at the same time unencrypted communication (such as http) is also enabled by default, is this considered non-conforming? Shall it be mandatory to enforce encrypted communication such as https by default and disable unencrypted communication methods?

[Guidance]

Communications that are enabled by default settings are applicable, and those that are disabled are not applicable.

If both https and http are available, make sure that all the following responses are satisfied. If it satisfies these requirements, it is considered "conforming."

1) The default configuration shall be set to accept only https (i.e., http is not accepted in the default configuration).
2) It is acceptable for users to change their settings so that http can be used.
3) Security precautions, such as risks and functional limitations of changing settings, shall be clearly indicated in places that explain how to change settings (e.g., manuals) so that users can understand the risks and functional limitations of changing settings.

When applying the exception in Section 2.2.2, it is necessary not only to add the following note: "Disable unencrypted http and enable encrypted https when installing the device." as well as that "the installation of IoT devices by an installation operator is a prerequisite (it is documented in the manual, etc., which installation by anyone other than the installation operator or system administrator is not permitted)." The presence of both annotations indicates conforming (one alone is non-conformance). In addition, any section explaining how to enable http (e.g., manuals) shall clearly be indicated to users the security risks and functional limitations associated with making this change.

[Question 12-3]

Please give instructions about the case where there is no default setting for http/https and the users need to specify the destination including "http://" and "https://" as the data destination.

For example,
"https://sample.com/" is set as the destination. > communication is possible.

"sample.com" is set as the destination (omitting "https://"). > communication not possible due to description format error.

If setting is omitted (blank) > No communication as no destination.

In IoT products with such specifications, the following measures are considered;

1) The default setting shall be set to use only https. (i.e., http is not accepted in the default settings.)
2) It is acceptable to enable the use of http by allowing users to change their settings.
3) Security precautions, such as risks and functional restrictions when changing settings, shall be clearly indicated in places that explain how to change settings (e.g., manuals) so that users can understand the risks and functional restrictions when changing settings.

In this case, shall it be interpreted as a. or b. below?

a. Assuming that there are no default settings, 1) does not apply, so if 2) and 3) are satisfied, it can be interpreted as "conforming."
b. In order to satisfy 1), it is necessary to add another setting item such as "allow http communication" (the default is that communication is not possible unless https is specified).

[Guidance]

It is interpreted as "b." In order to satisfy 1), it is necessary to add another setting item such as "allow http communication" (the default is that communication is not possible unless https is specified).

[Question 12-4]

Regarding explanation in the second half of condition B) of Section 2.6 in the Assessment Guide (page 12), "Concept of the scope of required (or excludable) secure communication," the phrase "For example, ……by the home router settings," for instance, if meter devices or door phones installed outdoors are physically protected (e.g., by a protective casing) to prevent wired connections, can they be considered to satisfy this requirement (outside the scope of "secure communication required")?

[Guidance]

That is correct as you understand.

[Question 12-5]

Regarding eavesdropping protection of "information assets to be protected" transmitted over a network, in the STAR-1 Assessment Guide Supplementary Explanation "2.2.1. Handling when using in an environment where communication with the Internet is not possible," it is stated that "even if communication is not encrypted...(omitted)...it is considered to satisfy Assessment Item 2."

On the other hand, in a network where encryption is not possible, even if the Supplementary Explanation is applicable (satisfies Assessment Item 2), Assessment Item 1 (encryption is required) cannot be satisfied, and this Conformance Requirement cannot be satisfied, so the description appears to be contradictory.

[Guidance]

This is an error that should be "it is considered to satisfy Assessment Item 3." It has been corrected in the Supplementary Explanation of the updated version of the STAR-1 Assessment Guide (JST-EG-01-01-2024R1).

[Question 12-6]

Are there any guidelines for using HTTPS?

[Guidance]

Although this is intended for TLS server-client (browser) type systems, the TLS cipher configuration guidelines may be helpful. In particular, this information is used to help you select the appropriate cryptographic suite.

URL: https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html
(Japanese version only)

[Question 12-7]

Is it mandatory that all cryptography employed in HTTPS satisfy the "e-Government Recommended Ciphers List"?

[Guidance]

It is acceptable to support cryptography that is not included in the "e-Government Recommended Ciphers List" or "Recommended Candidate Ciphers List," but such cryptography shall be set to "default disabled." If they are not "disabled by default," they are considered non-conforming. In addition, in the section explaining the settings changes (e.g., manuals) to enable these cryptographies, security precautions such as risks and functional restrictions shall be clearly indicated so that users are aware of them.

[Question 12-8]

Regarding rtsp communications, would it be considered non-conforming if I do not implement rtsps or srtp encrypted communications function and cannot provide instructions for activation at the time of installation?

In addition, if it is considered conforming, would one of the following methods be acceptable?

1) Turning off rtsp communication by default.
2) Implementing encrypted communication (e.g., rtsps and srtp) functions.
3) The vendor determines that real-time streaming of video and audio communicated via rtsp is not subject to encryption (it does not fall under the category of information assets to be protected).
4) Since it is difficult to satisfy Assessment Items 1-2, the content of "use IoT products only in a protected communication environment (VPN environment, connection environment via leased line, physically/logically protected network environment)" shall be clearly stated in the medium accessible to users so that Assessment Item 3 can be satisfied.

[Guidance]

That is correct as you understand.

[Question 12-9]

If there is a port where "assets to be protected" are temporarily transmitted unencrypted but closed and inaccessible during operation, is it correct to assume that the information transmitted through this port is not applicable to [S1.1-12] because it cannot be eavesdropped during operation? Or if "assets to be protected" are transmitted unencrypted, even temporarily, are measures required to protect against eavesdropping?

[Guidance]

In the initial setting, only when both of the following conditions A) and B) are met, and by documenting the procedure and leaving a trail (evidence), even if the protection measures are "ineffective at the time of shipment of IoT products," in exceptional cases, it can be deemed that "protection measures against eavesdropping are effective" by changing the initial settings at the time of installation of IoT devices.

A) It is assumed that the IoT device is installed by the installation operator (it is documented in manuals, etc., that only the installation operator or system administrator may install the IoT device).
B) The installation work instructions, manuals, or other documents indicate a caution or warning about an item that instructs the user to "enable protection against eavesdropping" in the settings of the relevant IoT device at the time of installation.

This information is described in S1.1-12. "2.2.2. Concept of Assessment Item 2 on initial setup" in (JC-STAR) STAR-1 Assessment Guide.

[STAR-1 Conformance Requirement S1.1-13]

[Question 13-1]

Regarding Assessment Item 3, it is stated that "the management process that allows the attack situation to be monitored and appropriate action to be taken, if necessary," but

(1) Does "allows the attack situation to be monitored" mean that IoT products need to detect the attack?

(2) Is it correct to understand that “appropriate action” includes action taken by the administrator?

(3) For example, if an attack is detected, and there is a management process in place to record it, and the administrator has stated that they will take appropriate action as necessary based on the records, would this be considered "conforming"?

[Guidance]

Since S1.1-13 requires a "management process," not only technical measures but also operational measures are acceptable.

(1) This does not mean that IoT products themselves must detect attacks. It can be done by establishing a system to collect alert information, etc., from NICT, IPA, and other bodies in a timely and appropriate manner.

(2) It is required to decide in advance what countermeasures will be taken depending on the severity of the attack situation. For example, in the most serious situation, "immediate disablement" is assumed to be necessary, so it is necessary to decide "how" to change the setting to disable. The "administrator's action" may be an option in the management process, but even in that case, it is necessary to decide "how" the administrator will take the appropriate action. It is not enough for "administrators to take appropriate action" simply.
It is also necessary to consider whether the most serious attack situations (i.e., when it is confirmed that a specific attack is being carried out) can be "handled by the administrator alone."

(3) As stated in (2) above, a statement to the effect that "to take appropriate action" is not sufficient. It is necessary to decide in advance what "appropriate action as necessary" entails, and what criteria will be used to determine and implement such measures.

[Question 13-2]

What are the recommended vulnerability scanners and port scanners?

[Guidance]

The recommended vulnerability scanner is intended to be a generally recognized scanner to be appropriately selected by IoT products vendors. However, it is necessary to be able to check i) and ii) of Assessment Item 5 in the STAR-1 Assessment Guide (S1.1-13).

Examples of vulnerability scanners available at no cost include OpenVAS, Vuls, and Greenbone Vulnerability Management (GVM). Other paid vulnerability scanners (e.g., Nessus) are also available.

NMAP is one example of a free port scanners.

These scanners shall be selected by IoT device vendors as appropriate for their intended use and budget. In addition, refer to the "A Guide to Security Validation to Ensure Cybersecurity of Devices" published by Ministry of Economy, Trade and Industry (METI).
URL: https://www.meti.go.jp/policy/netsecurity/wg3/kensyou_tebiki_r6kaitei.pdf
(Japanese version only)

[Question 13-3]

In relation to the annotation "*In principle, both document assessment and device check shall be conducted. However, if there is no recommended port scanner or vulnerability scanner, the device check can be excluded (document assessment only),"

(1) Since Bluetooth and USB fall under the absence of a recommended vulnerability scanner at this time, shall the contents described be assessed as a substitute for vulnerability confirmation testing?

(2) If there are no recommended port scanners or vulnerability scanners, does this include cases where the company conducting the test does not have port scanners or vulnerability scanners?

(3) Is it correct to interpret that only if the device itself has a function to use the http/https protocol, it shall be verified that no vulnerabilities corresponding to the known vulnerabilities CVE-ID listed in the guidelines are detected?

[Guidance]

(1) As you asked, the contents stated shall be assessed as an alternative to vulnerability testing for Bluetooth and USB at this point.

(2) The phrase "no recommended scanners" does not include "simply not having them." In general, it is limited to cases where there is "no recommended scanner itself."

(3) As you asked, only if the device has a function to use the http/https protocol, it shall be confirmed that no vulnerabilities corresponding to the CVE-ID have been detected.

[Question 13-4]

Regarding the Bluetooth check method, does the device check pair with "Bluetooth" and assume that the device is given an IP address and a TCP/IP port scan?

[Guidance]

Since Assessment Item 4 does not specify the connection method for (A) TCP/UDP, if a profile that uses Bluetooth for TCP/IP communication (e.g., DUN, PAN, IPSP) is used, TCP/IP port scanning (and vulnerability scanning) using the same connection method is required.

[Question 13-5]

Regarding the USB check method, does the device check involve connecting USB, assigning an IP address to the device, and performing a TCP/IP port scan?

[Guidance]

Since the connection method is not specified for A) TCP/UDP in Assessment Item 4, if a profile (IP over USB class) that uses USB for TCP/IP communication is used, TCP/IP port scanning (and vulnerability scanning) using the same connection method is required.

[Question 13-6]

Regarding the scope of vulnerability testing in Assessment Item 5, does it apply to all the webpages on the Internet? Or is only the login screen to be inspected?

Does this apply to web servers (e.g., Apache and other middleware services)? Or does the web interface (e.g., IoT management screen) also apply?

[Guidance]

The intent of Assessment Item 5 is to confirm that all settings and implementations (including web applications) that use http/https that can be connected from the Internet do not contain vulnerabilities by focusing on only the most important items. Therefore, webpages that can be connected from the Internet other than login screens that use http/https are also applicable.

In addition, verification by device check in Assessment Item 5 is required regardless of whether it is on an IoT device or associated services. However, since it is expected that separate inspections will be conducted to ensure that vulnerabilities confirmed in device check of Assessment Item 5 are not included in the development of web applications and websites as part of secure coding, the results of those vulnerability inspections may be used as a substitute of device check of Assessment Item 5. In this case, vulnerability inspection results reports conducted during the development of web applications and websites shall be stored as evidence.

In relation to S1.1-13, the maintenance status of the cloud/server on which the associated services are running is not included in the scope of the associated services and is considered to be properly maintained outside the framework of this Scheme. In other words, there is no need to perform device checks on the cloud or server itself.

If the vendor can change settings such as closing unnecessary ports on the cloud or server, the associated services (i.e., settings on the cloud or server running the service) will be assessed by applying Assessment Items 1 to 3 of S1.1-13.

[Question 13-7]

As a method of "minimizing exposed attack surfaces," would hardware measures such as locking device with special keys be acceptable?

[Guidance]

Since access from the communication interface is assumed, no hardware measures can protect it basically. However, in the case of USB, there may be exceptional circumstances where the USB interface cannot be used due to the protective casing.

[STAR-1 Conformance Requirement S1.1-14]

[Question 14-1]

No questions asked.

[Guidance]

-

[STAR-1 Conformance Requirement S1.1-15]

[Question 15-1]

If there are no user-configurable parameters, is it acceptable not to include a delete function?

[Guidance]

Since information assets (including personal information) generated by users during operation are subject to deletion, it depends on whether such information is generated or not. The presence or absence of user-configurable parameters does not determine whether the delete function is required or not.

[STAR-1 Conformance Requirement S1.1-16]

[Question 16-1]

Regarding Conformance Requirement (4) in S1.1-16, if the device is not sold as a stand-alone unit, but is provided as part of a service under the following conditions, how shall the "support period" be interpreted?

- It is provided on a system-by-system contract basis, including other devices.
- There is no support period set as a stand-alone device.
- Support is assured for the duration of the contract, and there is no set deadline for contract renewal.
- The entire device is replaced if any need arises during the contract period.
- Since the devices are collected at the end of the contract, they are not used outside of the contract period (outside of support period).

[Guidance]

It shall be determined based on how long the product is likely to remain embedded into the system. In other words, the maximum service provision (possible) period equals to support period.

In addition, as far as publicity is concerned, it is sufficient to state that "support is assured for the duration of the service provision contract."

[Question 16-2]

Regarding public notification, is it necessary to follow the description of the Assessment Guide and provide information on the website? In other words, to whom does it need to be informed?

If the actual users (e.g., only contractors through corporate sales) are made aware of this and all users are notified, can it be deemed to conform to the requirement if the information is included in the contract?

[Guidance]

The support period for the applied product must be stated in the application form, and this information will be posted on the "Product Information Page" of the website managed by IPA. Therefore, it is acceptable to assume that a certain level of awareness has been achieved by the agreement in the application form.

For Assessment Item 4, it is sufficient to confirm that the support period does not contradict this. In other words, as long as it does not contradict the support period stated in the application form, the applicant may announce the support period on its company's website, or the applicant may choose to inform only the contractors or prospective purchasers.

If the support period is defined in a separate contract, it is acceptable if the support period differs from the one stated in the application form.

[Question 16-3]

Conventionally, we have announced information regarding the end of product support and sales after the dates had been decided. As information to be disclosed by the manufacturer as required in Assessment Item 4, are the following descriptions regarding the support period acceptable?
Example 1) "Support end date undecided."
Example 2) "Support ends after two years."

[Guidance]

Publication of the support period will be posted on the "Product Information Page" of the website managed by IPA. Therefore, it is acceptable to assume that a certain level of publicity has been made at this point with the agreement in the application form. It is sufficient only to confirm that the support period does not contradict this in Assessment Item 4.

On the assumption that the support period does not violate the support period listed on the "Product Information Page" of the website managed by IPA, it is acceptable to make the support period known on your company's website, etc. If the support period has not yet been determined, no indication of the support period is acceptable.

[Question 16-4]

Is it acceptable to use the application as evidence to prove the support period?

In such a case, how shall the checklist be described, even though it cannot be certified by technical documents?

[Guidance]

It is acceptable to use the application form as evidence. In that case, it is sufficient to simply state "as described in the application form."

[Question 16-5]

For products that have not yet been released, is it sufficient to indicate the name of the medium on which the information will be published and the means of obtaining it [*], as the information has not been made public to users, etc.?
[*] Describing information in the user's manual included with the product or describing in the user's manual provided to users when purchasing the product.

Example 1) The description that satisfies the requirement of Assessment Item 1 of Conformance Requirement S1.1-16 is planned to be included in the user's manual, but it cannot be disclosed because the product has not yet been released. In this case, is it sufficient to state "described in the user's manual of the product" or "planned to be described in the user's manual of the product"?

Example 2) The description that satisfies the requirements of Assessment Item 4 of Conformance Requirement S1.1-16 will be published on our website, but since the product has not yet been released, we cannot disclose the URL information, etc. In this case, is it sufficient to state "described on the manufacturer's website" or "to be posted on the manufacturer's website"?

[Guidance]

The "means of public notification" and the "date of publication" of the planned publication shall be described in the checklist.

As a means of public notification, it is acceptable to state that the information is "to be described in the user's manual of the product" or "to be described on the manufacturer's website."