METI
Ministry of Economy, Trade and Industry

Japan Cyber STAR (JC-STAR)

IoT Product Security Conformity Assessment Scheme

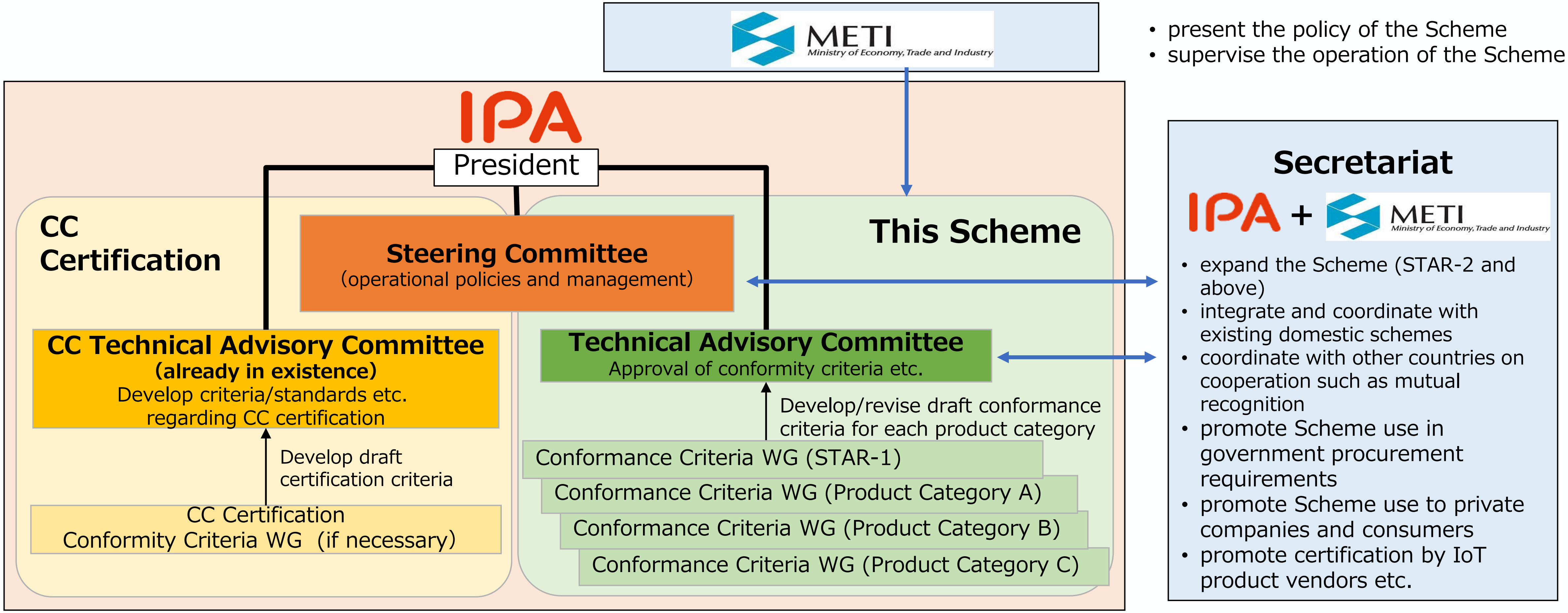
September 2024

Ministry of Economy, Trade and Industry, Japan

1. Operational Structure of the Scheme

- **The Scheme Owner will be IPA**, an incorporated administrative agency under the jurisdiction of METI.

- **The Technical Advisory Committee** will discuss the approval of conformance criteria and other technical matters of this Scheme. **Conformance Criteria WGs** will be established under the Technical Advisory Committee to formulate the draft conformance criteria for each product category.



METI Ministry of Economy, Trade and Industry

- present the policy of the Scheme
- supervise the operation of the Scheme

IPA

President

CC Certification

Steering Committee
(operational policies and management)

This Scheme

CC Technical Advisory Committee
(already in existence)
Develop criteria/standards etc. regarding CC certification

Develop draft certification criteria

CC Certification Conformity Criteria WG (if necessary)

Technical Advisory Committee
Approval of conformity criteria etc.

Develop/revise draft conformance criteria for each product category

Conformance Criteria WG (STAR-1)

Conformance Criteria WG (Product Category A)

Conformance Criteria WG (Product Category B)

Conformance Criteria WG (Product Category C)

Secretariat

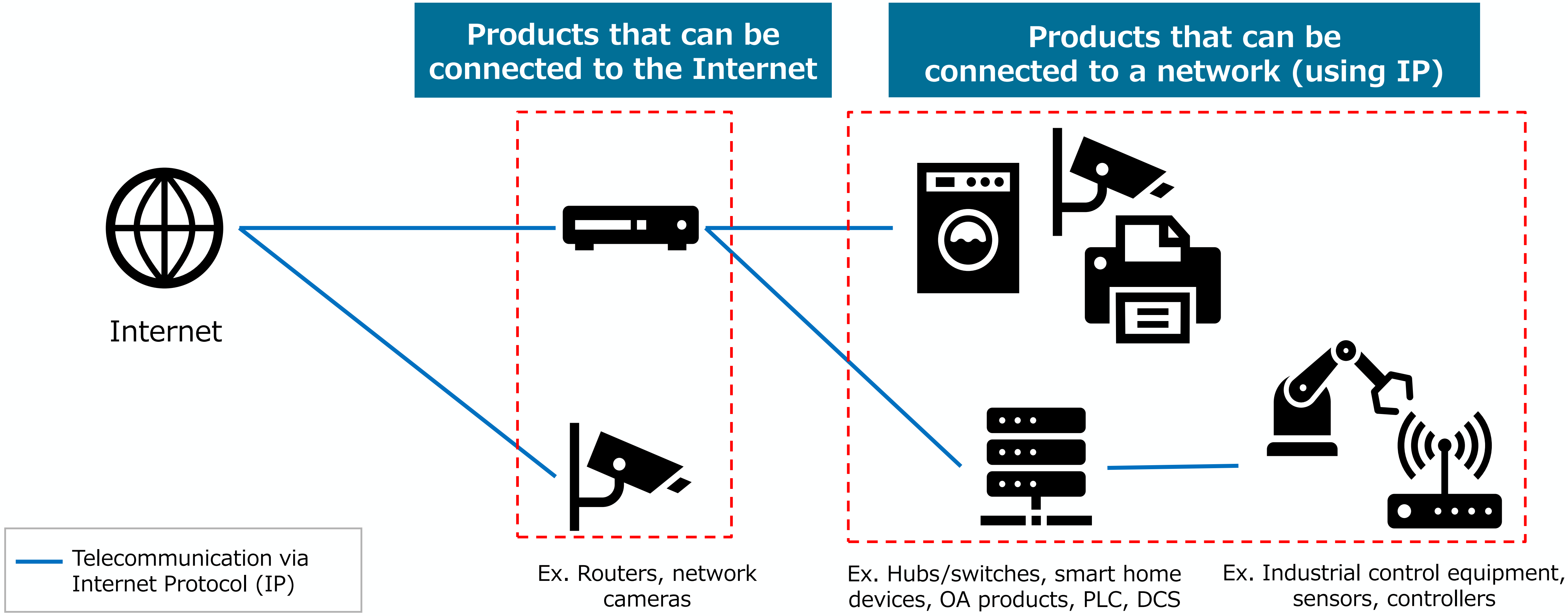
IPA + METI Ministry of Economy, Trade and Industry

- expand the Scheme (STAR-2 and above)
- integrate and coordinate with existing domestic schemes
- coordinate with other countries on cooperation such as mutual recognition
- promote Scheme use in government procurement requirements
- promote Scheme use to private companies and consumers
- promote certification by IoT product vendors etc.

2. Scope of Products Covered by the Scheme

- **IoT products** (IoT devices and their associated services) **that can be connected directly or indirectly to the internet using IP** will be covered in the scope of this Scheme. This includes **both consumer and industrial** products.

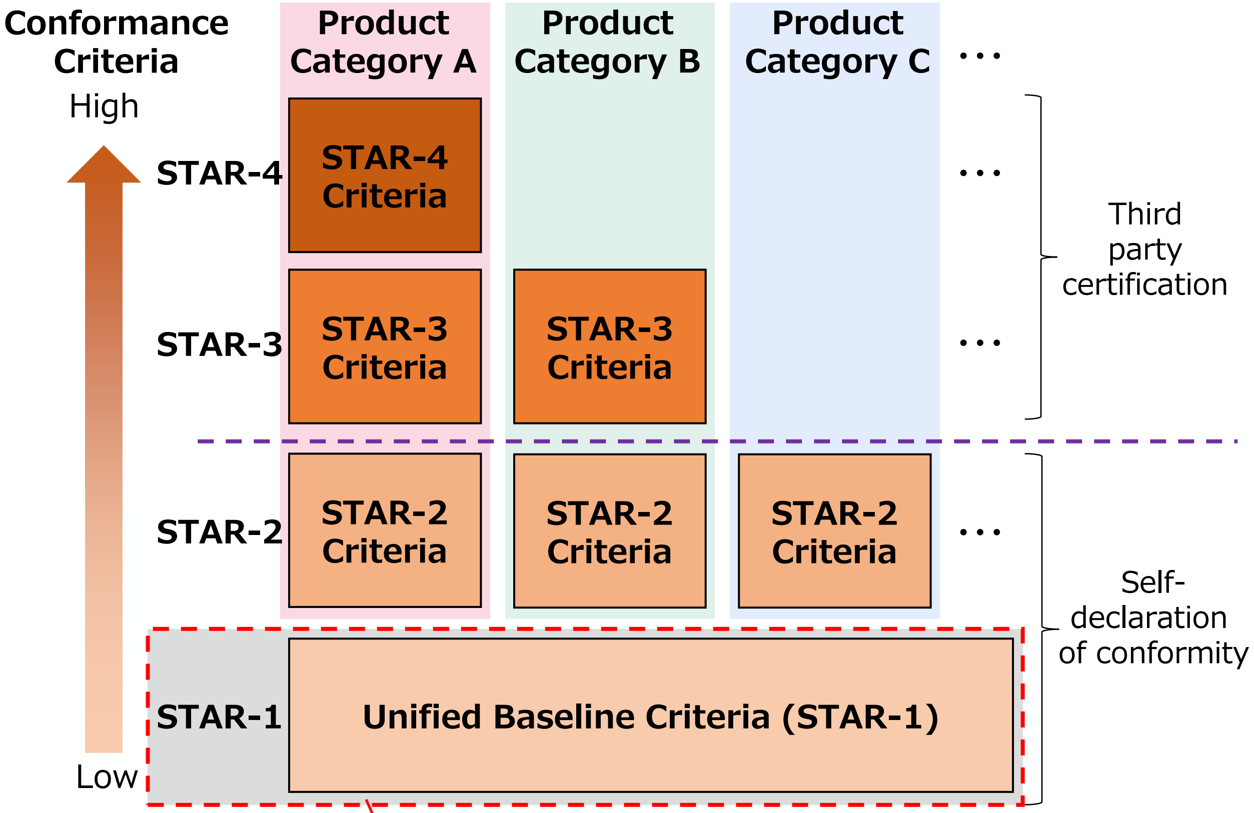
*Excludes general-purpose IT products to which users can easily alter security measures such as via software products (PCs, tablets, smartphones, etc.)



Products that can be connected to the Internet
Products that can be connected to a network (using IP)
Internet
Telecommunication via Internet Protocol (IP)
Ex. Routers, network cameras
Ex. Hubs/switches, smart home devices, OA products, PLC, DCS
Ex. Industrial control equipment, sensors, controllers

3. Conformity Assessment Levels in the Scheme

- **The Scheme will be multi-level** with four conformity assessment levels.
- The criteria for **STAR-1 will be a unified baseline** to address minimum threats common to all IoT products in scope. The criteria for **STAR-2, STAR-3 and STAR-4 will be organized per product category**.



STAR-1 launch by March 2025

Level	Positioning	Conformance Criteria	Evaluation/ Certification
STAR-3 and above	General conformance criteria for each IoT product category that is **intended for use in critical systems of government agencies, critical infrastructure providers, and large companies**, and is **evaluated and certified by an independent third party**.	Per product category	Third party
STAR-2	**IoT product vendors self-declare** that their product conforms to the basic **conformance criteria for each IoT product category** in addition to STAR-1.		Self-declaration of conformity
STAR-1	**IoT product vendors self-declare** that their product conforms to the **unified baseline conformance criteria** for all IoT products in scope.	Common to all product categories	

4. Security Requirements, Conformance Criteria, and Evaluation Procedures in the Scheme (1/2)

- A **comprehensive list of security requirements that may be covered by the Scheme ("Long List")** was first created based on **overlapping domestic and international security requirements**.
- The **security requirements** for each conformity assessment level were then **extracted from this "Long List" to counter the assumed threats at each level**, beginning with STAR-1.

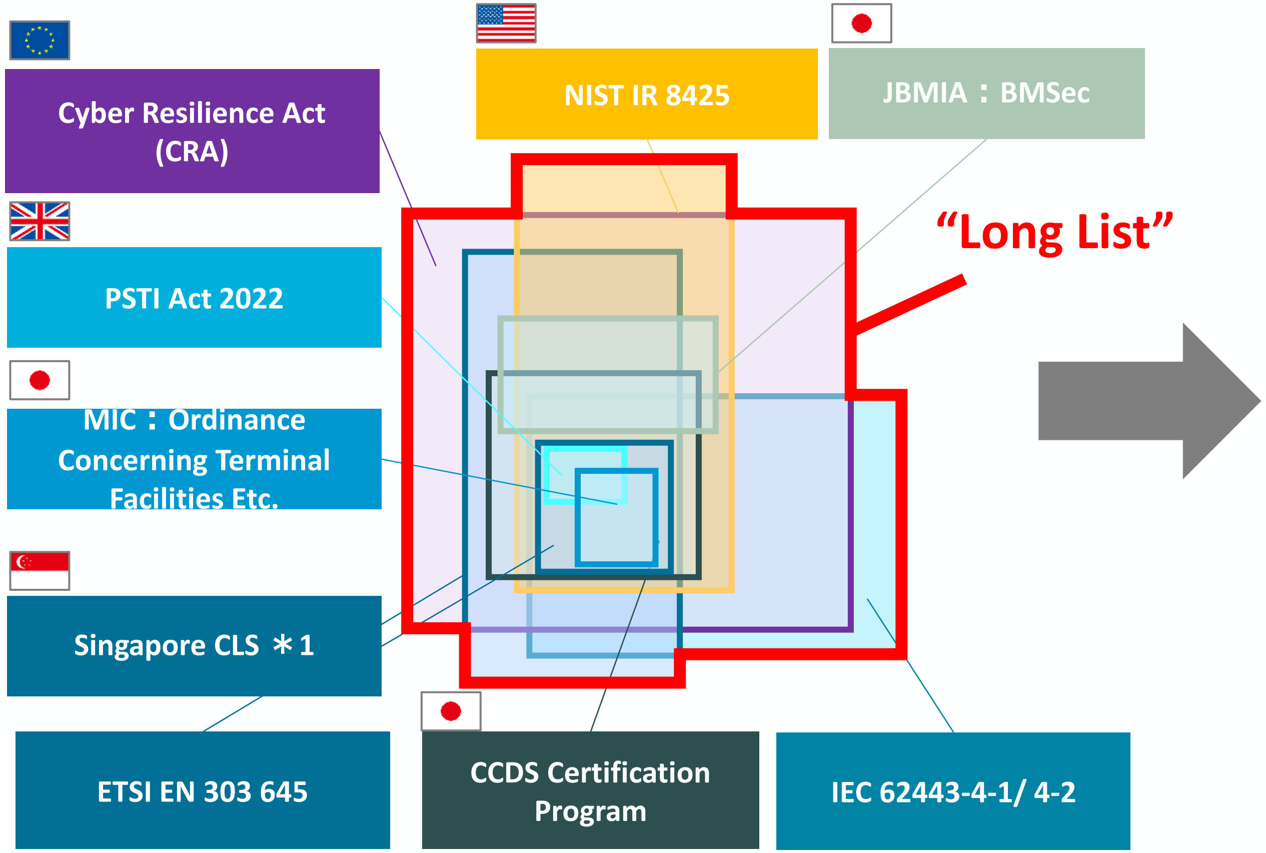
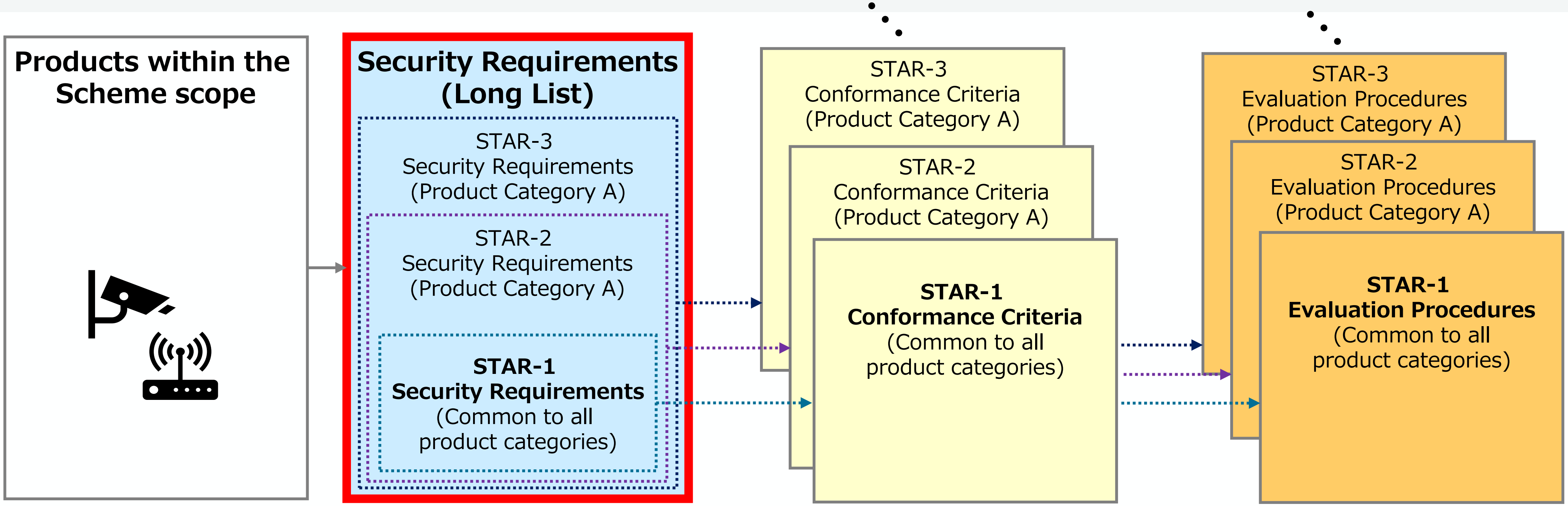

Cyber Resilience Act (CRA)
PSTI Act 2022
MIC：Ordinance Concerning Terminal Facilities Etc.
Singapore CLS ＊1
ETSI EN 303 645
NIST IR 8425
JBMIA：BMSec
CCDS Certification Program
IEC 62443-4-1/ 4-2
"Long List"

Image of "Long list"	
1. No universal default passwords	1-1. For devices that use passwords, passwords that match a defined quality scale are set, or can be set by the user.
	1-2. …
	1-3. …
	1-4. …
	1-5. …
2. Implement a means to manage reports of vulnerabilities	2-1. Require manufacturers to publish a vulnerability disclosure policy that describes the means by which reports and inquiries about the security of their products are received in [defined manner and format].
	2-2. …
	2-3. …
・・・	・・・

4. Security Requirements, Conformance Criteria, and Evaluation Procedures in the Scheme (2/2)

- For STAR-1, a draft of security requirements, conformance criteria and evaluation procedures was organized by referencing domestic and international schemes, as well as the results of a POC on 10 products.
  The STAR-1 was finalized in the IPA Technical Advisory Committee.

- **For STAR-2 and above, priority product categories will first be identified**. Security requirements, conformity criteria, and evaluation procedures will be **discussed in Conformance Criteria WGs of each product category with relevant stakeholders starting FY2024**.



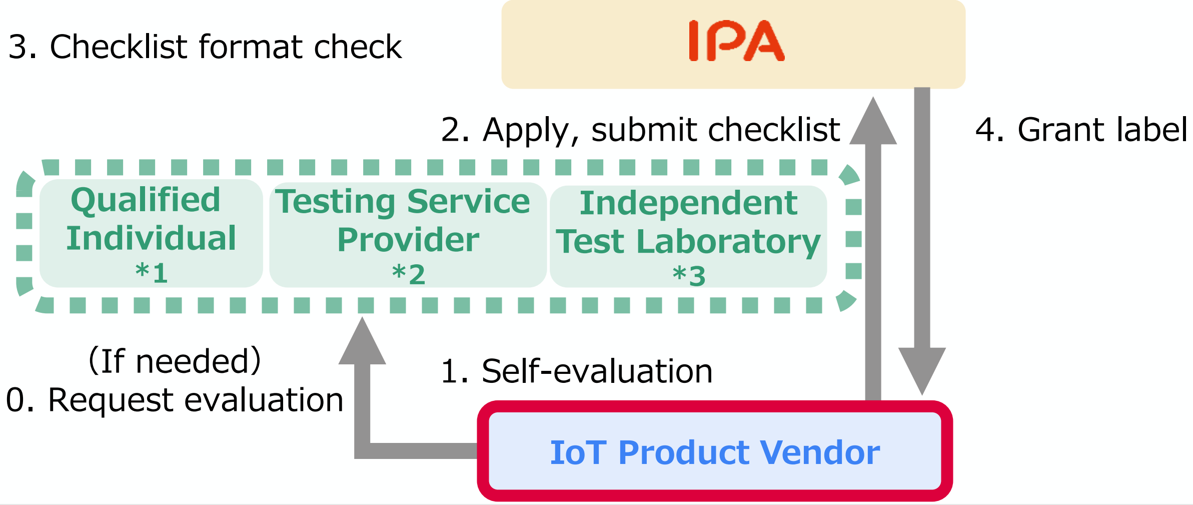
Products within the Scheme scope
Security Requirements (Long List)
STAR-3 Security Requirements (Product Category A)
STAR-2 Security Requirements (Product Category A)
STAR-1 Security Requirements (Common to all product categories)
STAR-3 Conformance Criteria (Product Category A)
STAR-2 Conformance Criteria (Product Category A)
STAR-1 Conformance Criteria (Common to all product categories)
STAR-3 Evaluation Procedures (Product Category A)
STAR-2 Evaluation Procedures (Product Category A)
STAR-1 Evaluation Procedures (Common to all product categories)

5. Entities That Perform Conformity Assessment

- **For STAR-1 and STAR-2**, IoT product vendors **may self-declare conformity, or may outsource evaluation** to a qualified individual*1, testing service provider*2, or independent test laboratory*3.

- **For STAR-3 and above, evaluation by an independent test laboratory*3 will be required.**

STAR-1, STAR-2 (Self-declaration of conformity)



3. Checklist format check

IPA

2. Apply, submit checklist

4. Grant label

Qualified Individual *1

Testing Service Provider *2

Independent Test Laboratory *3

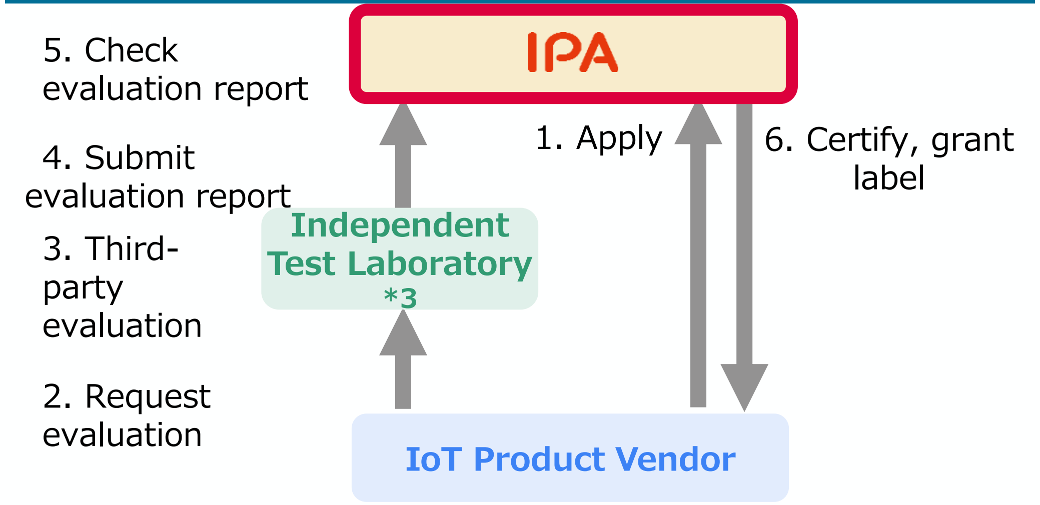
(If needed)
0. Request evaluation

1. Self-evaluation

IoT Product Vendor

1. The **IoT product vendor conducts self-evaluation** based on the STAR-1 or STAR-2 conformance criteria/evaluation procedures and creates a checklist. The evaluation may be outsourced to a qualified individual, testing service provider, or independent test laboratory. *Whether STAR-2 will require evaluation by qualified individuals, testing service provider, or independent test laboratory is to be considered.
2. The IoT product vendor applies and submits the checklist to IPA.
3. IPA performs a format check of the checklist.
4. IPA grants the label to the IoT product.

STAR-3 and above (Third party evaluation/certification)



5. Check evaluation report

IPA

4. Submit evaluation report

1. Apply

6. Certify, grant label

3. Third-party evaluation

Independent Test Laboratory *3

2. Request evaluation

IoT Product Vendor

1. The IoT product vendor applies to IPA.
2. The **IoT product vendor requests evaluation to an independent test laboratory**.
3. The independent test laboratory conducts evaluation based on the STAR-3 and above conformance criteria/evaluation procedures.
4. The independent test laboratory submits an evaluation report to IPA.
5. IPA, as the certification body, checks the evaluation report for any problems.
6. IPA grants the label to the IoT product.

*1: “Qualified individuals” refers to those with a designated qualification (e.g. Registered Information Security Specialist) and have completed training on IoT security evaluation or taken an oath that they understand the evaluation guide.

*2: “Testing service providers” refers to those whose services are registered as a Device Testing Service of the Information Security Service Standards Assessment and Registration System, which examines and registers conformity to the Information Security Service Standards defined by METI, and whose services are listed in the Information Security Service Standards Compliance Service List.

*3: An accreditation scheme based on ISO/IEC17025 will be established to accredit entities that can conduct evaluations of STAR-3 and above under the Accreditation System of National Institute of Technology and Evaluation (ASNITE) of the National Institute of Technology and Evaluation (NITE). Only these accredited entities with sufficient capabilities and systems will be considered “independent test laboratories” and will be able to conduct evaluations for STAR-3 and above.

*4: IPA will make inquiries to relevant government agencies, including METI, regarding supply chain risk before granting the label, and will grant the label based on the inquiry result.

6. Implications of the Label

- The label is only an indication of conformity to the established conformance criteria and **does not guarantee that the IoT product is fully secured**.

Conformity Assessment Level	Implication of the Label
STAR-1, STAR-2 (Self-declaration of conformity)	The label is a **self-declaration by the IoT product vendor that the IoT product conforms to the conformance criteria** defined at the time the label is acquired (including reacquisition at the time of renewal). The attestation entity is the IoT product vendor. IPA, as a label granting body, will perform a format check of the checklist describing the evaluation results, but IPA does not certify the security conformity of the IoT product.
STAR-3 and above (Third-party certification)	The label indicates that **IPA, as the certification body, has certified that the product conforms to the conformance criteria** defined at the time the label is acquired (including at the time of re-evaluation). The attestation entity is IPA. **IPA will certify conformity to the conformance criteria after checking the evaluation report by an independent test laboratory**, which will be aligned with the conformance criteria and evaluation procedures as stipulated in the Scheme. However, while IPA is responsible for appropriately checking the evaluation report by the independent test laboratory, IPA makes no warranty, explicit or implied, with respect to the labeled product.

7. Mechanisms for Ensuring Label Reliability

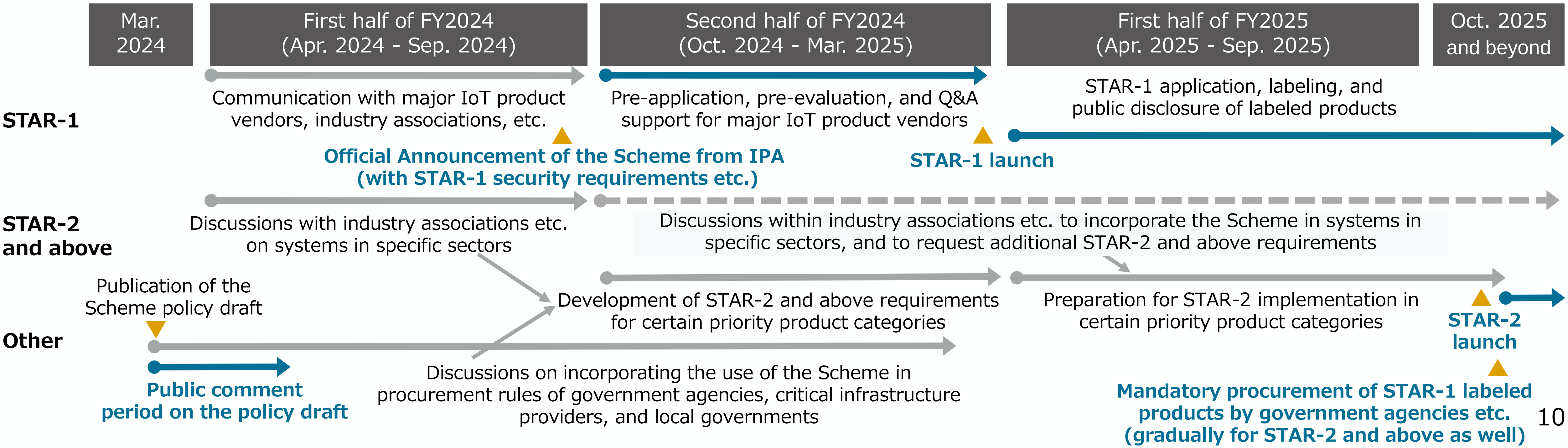
- Due to the voluntary nature of the Scheme, there is no obligation to display the label. **IoT product vendors may voluntarily affix the label** to the product itself, package, website, etc. **The label will include a QR code with the URL of a Scheme webpage providing details on each labeled product** (below).
- The **validity period of STAR-1 and STAR-2** labels will be **up to two years** from the date of label acquisition. The Scheme Owner will have the right to **inspect and conduct surveillance** on labeled products.

Outline of the Scheme	• URL of the webpage explaining the outline and details of the Scheme
Product Information	• Product name • Model number • IoT product manufacturer name *Disclosure to the public is optional • Country or region of manufacture *Disclosure to the public is optional • Product overview • Product webpage URL • Contact information for product inquiries • Certification numbers for other certifications
Security Information	• Vulnerability information of the product • Contact information for the reporting of vulnerabilities

Label Information	• Label identification number • Conformity assessment level of the product (STAR-1 to 4) • Product category of the product *for STAR-2 to 4 • Version of conformance criteria evaluated • Conformity assessment results (checklist or evaluation report) • Label status information • Date of label issue/renewal • Label expiration date • Label applicant name (IoT product vendor) • Evaluator category
Other Security-related Information	• Security-related information from IoT product vendors to procurers and end-users, if necessary

8. Future Schedule

- **For STAR-1**, the target for **scheme launch is during FY2024 (by March 2025).**
- **For STAR-2 and above**, security requirements, conformity criteria, and evaluation procedures for certain priority product categories will be **developed in the second half of FY2024**. The target for **scheme launch of these product categories is during or after the second half of FY2025**.
- METI will **coordinate the mandatory procurement of labeled products in government agencies**, etc. and **encourage critical infrastructure providers and local governments** to incorporate the use of the Scheme into their IoT product procurement rules.



Mar. 2024

First half of FY2024 (Apr. 2024 - Sep. 2024)

Second half of FY2024 (Oct. 2024 - Mar. 2025)

First half of FY2025 (Apr. 2025 - Sep. 2025)

Oct. 2025 and beyond

STAR-1

Communication with major IoT product vendors, industry associations, etc.

Pre-application, pre-evaluation, and Q&A support for major IoT product vendors

STAR-1 application, labeling, and public disclosure of labeled products

Official Announcement of the Scheme from IPA (with STAR-1 security requirements etc.)

STAR-1 launch

STAR-2 and above

Discussions with industry associations etc. on systems in specific sectors

Discussions within industry associations etc. to incorporate the Scheme in systems in specific sectors, and to request additional STAR-2 and above requirements

Development of STAR-2 and above requirements for certain priority product categories

Preparation for STAR-2 implementation in certain priority product categories

STAR-2 launch

Other

Publication of the Scheme policy draft

Public comment period on the policy draft

Discussions on incorporating the use of the Scheme in procurement rules of government agencies, critical infrastructure providers, and local governments

Mandatory procurement of STAR-1 labeled products by government agencies etc. (gradually for STAR-2 and above as well)