

MEMORANDUM OF COOPERATION
BETWEEN
THE MINISTRY OF ECONOMY, TRADE AND INDUSTRY OF JAPAN
AND
THE CYBER SECURITY AGENCY OF THE REPUBLIC OF SINGAPORE
ON MUTUAL RECOGNITION OF
INTERNET-OF-THINGS SECURITY SCHEMES
(JC-STAR STAR-1 AND SINGAPORE CYBERSECURITY LABELLING SCHEME LEVEL 1)

The Ministry of Economy, Trade and Industry of Japan and the Cyber Security Agency of the Republic of Singapore (hereinafter referred to individually as "Participant" and collectively as "Participants")

With the aim to raise overall cyber hygiene levels and better secure cyberspace internationally;

In order to work towards establishing effective mechanisms for the mutual recognition of the respective Internet-of-Things ("**IoT**") devices cyber security schemes of Japan and the Republic of Singapore;

The Participants intend to enhance cooperation between themselves for the mutual recognition of the Singapore Cybersecurity Labelling Scheme and JC-STAR.

HAVE ACCEPTED AS FOLLOWS:

PARAGRAPH 1

Objective

1. Acting within their powers and responsibilities and in accordance with their national laws and regulations, and in any event insofar as appropriate, the Participants will endeavour to strengthen cooperation in the area of IoT cybersecurity between the Participants, with the aim of facilitating the mutual recognition of the Participants' respective IoT Cyber Security Schemes, in line with the items of this Memorandum of Cooperation (hereinafter referred to as "this MoC").

PARAGRAPH 2

Definitions

The following details and definitions are utilized for the purpose of this MoC:

1. "**Conformity Assessment Procedures**" means, in the case of Singapore, the process of determining whether a IoT Product complies with the Requirements of the Singapore Cybersecurity Labelling Scheme, and in the case of Japan, means the process of determining whether a IoT Product complies with the Requirements of the JC-STAR (Japan's Cyber-Security Technical Assessment Requirements);
2. "**Cyber Security Scheme**" means, in the case of Japan, the JC-STAR scheme and in the case of Singapore, the Singapore Cybersecurity Labelling Scheme;
3. "**IoT Product**" means, in the case of Japan, a product that is within the scope of the Japan's Cyber Security Scheme and in the case of Singapore, means a product that is within the scope of the Singapore Cybersecurity Labelling Scheme;
4. "**Label**" means, in the case of Japan, the Japan Cybersecurity Label that is issued under the JC-STAR scheme, and in the case of Singapore, means the Singapore Cybersecurity Label that is issued under the Singapore Cybersecurity Labelling Scheme;
5. "**Requirements**" means, in the case of Japan, the security requirements applicable to the relevant product category set out under the JC-STAR STAR-1, and in the case of Singapore, means the security requirements specified under the Singapore Cybersecurity Labelling Scheme Level 1;

PARAGRAPH 3

Recognition of Labels

1. Each Participant will recognise the other Participant's IoT Cyber Security Scheme as credible.
2. A Participant will endeavour to recognise the other Participant's Labels as follows:
 - a) An IoT Product that has been issued with a valid Japan's JC-STAR Label upon compliance with Japan's Conformity Assessment Procedures will undergo a simplified application process for obtaining CLS Level 1 Label under Singapore's Cyber Security Scheme stipulated by Cyber Security Agency of the Republic of Singapore by showing its obtained Japan's Label (See Annex A and ANNEX B).
 - b) A IoT Product that has been issued with a valid Singapore's CLS Label upon compliance with Singapore's Conformity Assessment Procedures will undergo a simplified application process for obtaining a JC-STAR STAR-1 Label under Japan's Cyber Security Scheme stipulated by the Information-technology Promotion Agency of Japan by showing its obtained Singapore's Label (See Annex A).
3. For the purposes of mutual recognition under this paragraph:
 - a. All levels of Singapore's Cyber Security Scheme will be deemed equivalent to and recognised as Singapore's CLS Level 1.
 - b. All levels of Japan's Cyber Security Scheme will be deemed equivalent to and recognised as Japan's JC-STAR STAR-1.
4. For the avoidance of doubt, this paragraph does not extend to Labels issued to a Consumer IoT in line with any other mutual recognition arrangement with third parties.
5. Where a Participant is discontent with the decision of the other Participant as to the Labelling of IoT Product, both Participants will endeavour to resolve this discontent through mutual consultations and may share the relevant information for this purpose. If the Participants are not able to resolve this discontent, the Label of the IoT Product concerned will not be capable of being recognised under subparagraph 2 of Paragraph 3.
6. Each Participant will inform the other Participant if it revokes any Label issued to a IoT Product of that other Participant under subparagraph 2 of Paragraph 3, within thirty working days of taking such measure.
7. An IoT Product that has been issued with a Label upon compliance with Japan's or Singapore's Conformity Assessment Procedures falling within the scope and purview of this MoC will be recognised and accorded full recognition. This recognition applies to both newly issued labels and previously issued labels, provided that such labels remain valid and the IoT Products satisfy the criteria and requirements established.

PARAGRAPH 4

Forms of cooperation

1. The Participants may exchange information relating to the development of applicable standards, cybersecurity threats and attack methods on IoT Product, Requirements and other practices concerning IoT Cyber Security Schemes, and share best practices, as appropriate.

2. The Participants will endeavour to have a consultation at least once annually to provide updates on their Consumer IoT Cyber Security Schemes, laws and corresponding Requirements.
3. Within the context of this MoC, the Participants will endeavour to collaborate on further developments of their IoT Cyber Security Schemes, where appropriate.
4. Relevant documents issued for the purpose of information exchange, verification, provision of evidence and other activities arising from this MoC, if not in English, will be accompanied by translated copies in English, where appropriate and needed.

PARAGRAPH 5

Funding and Resources

1. Any collaborative activity carried out under this MoC, will be subject to the availability of funds and resources of each Participant at the material time. Unless otherwise decided in writing by both Participants, each Participant will bear its own costs and expenses for the conduct of all activities and programmes carried out within the framework of this MoC, subject to its budgetary appropriations.

PARAGRAPH 6

Confidentiality

1. The Participants will observe the confidentiality and secrecy of documents, information and other data received from the other Participant during the operation of this MoC, to the extent permitted under their national laws and regulations or international obligations.
2. The Participants will take reasonable and lawful measures to ensure that information provided or generated pursuant to this MoC is protected and used only for the purposes it was provided and will not be disclosed to any third party without prior written consent of the other Participant, to the extent permitted under their national laws and regulations.
3. All information provided or generated pursuant in line with this MoC will be safeguarded, used, transmitted, stored and handled in accordance with the Participants' national laws and regulations or international obligations.
4. The matters of this Paragraph will remain respected notwithstanding the discontinuation of this MoC.

PARAGRAPH 7

Dispute Settlement

1. The Participants will resolve any disputes or differences arising from the interpretation or implementation of this MoC amicably and in good faith through mutual consultations without reference to any national or international tribunal, or third party for settlement.
2. The items of this Paragraph will remain respected notwithstanding the discontinuation of this MoC.

PARAGRAPH 8

Relationship with national law and international law

1. Nothing in this MoC creates or is intended to create any legally binding rights and obligations for either Participant under their national law, or international law.
2. This MoC is not eligible for registration under Article 102 of the Charter of the United Nations.
3. This MoC or any actions taken thereto will not affect the rights and obligations of the Participants under any existing international agreements or conventions to which they are party.

PARAGRAPH 9

Modifications

1. This MoC may be modified at any time by mutual written consent of the Participants. Such modification will commence on a date as determined by the Participants and will form an integral part of this MoC.

PARAGRAPH 10

Preservation of Authority of a Participant

1. Nothing in this MoC will be construed to limit the authority of a Participant to determine, through its legislative, regulatory and administrative measures, the level of protection it considers appropriate for the safety of consumers.
2. Nothing in this MoC will be construed to limit the authority of a Participant to take all appropriate and immediate measures whenever it ascertains that a IoT Product:
 - a) compromises the health or safety of persons;
 - b) does not meet its laws and regulations;
 - c) compromises national security; or
 - d) otherwise fails to satisfy its Requirements.

PARAGRAPH 11

Final Provisions

1. The Participants will take appropriate measures to fulfil their responsibilities under this MoC.
2. This MoC will commence on 01-06-2026 and will continue for an initial period of three (3) years, and upon expiration of the initial period, this MoC will be automatically renewed for successive periods of three (3) years, unless discontinued by either Participant in line with subparagraph 3.
3. Either Participant may discontinue this MoC at any time. A Participant that wishes to do so should inform the other Participant of its intention to discontinue this MoC in writing six (6) months in advance of the intended discontinuation date. Upon discontinuation of this MoU, the Participants will consult to determine how any outstanding matters should be dealt with.
4. Any contractual obligations to third parties will remain unaffected.

The foregoing represents the consensus reached between the Participants on the matters referred to in this MoC.

SIGNED in duplicate in Japan on 18/3/2026 in the English language.

For and on behalf of Japan METI:

For and on behalf of the Cyber Security
Agency of Singapore:

INO Toshiro
State Minister of Economy, Trade
and Industry
Ministry of Economy, Trade and
Industry
Japan

MAHZAM Rahayu
Minister of State for Digital
Development and
Information and Minister of
State for Health
Cyber Security Agency of
The Republic of Singapore

Annex A: Equivalency of Japan and Singapore Scheme Requirements for General IoT

Japan's JC-STAR STAR-1 Requirements	Conformance status of Singapore's CLS Level 1 requirements
Conformance Requirement Number 1	None
Conformance Requirement Number 2	Full
Conformance Requirement Number 3	Full
Conformance Requirement Number 4	Full
Conformance Requirement Number 5	Full
Conformance Requirement Number 6	Partial Compliance with JC-STAR is required to be assessed.
Conformance Requirement Number 7	Full
Conformance Requirement Number 8	Full
Conformance Requirement Number 9	Partial Compliance with JC-STAR is required to be assessed.
Conformance Requirement Number 10	Full
Conformance Requirement Number 11	None
Conformance Requirement Number 12	None
Conformance Requirement Number 13	None
Conformance Requirement Number 14	None
Conformance Requirement Number 15	None
Conformance Requirement Number 16	Partial Compliance with JC-STAR is required to be assessed.

Singapore's CLS Level 1 requirements	Conformance status of Japan's JC-STAR STAR-1 requirements
Provision 5.1-1	Full
Provision 5.1-2	Full
Provision 5.1-3	Full

Provision 5.1-4	Full
Provision 5.1-5	Full
Provision 5.2-1	Full
Provision 5.3-2	Full
Provision 5.3-3	Full
Provision 5.3-7	Partial Compliance with CLS is required to be assessed.
Provision 5.3-8	Full
Provision 5.3-10	Full
Provision 5.3-13	Full
Provision 5.3-16	Full

Annex B: Equivalency of Japan and Singapore Scheme Requirements for Additional Home Gateway Requirements

Singapore's CLS Level 1 requirements	Conformance status of Japan's JC-STAR STAR-1 requirements
Provision 5.3-1	Full
Provision 7.3-1	Partial Compliance with CLS is required to be assessed.
Provision 7.3-4	None
Provision 5.3-6	None
Provision 7.3-6	None
Provision 7.3-7	Partial Compliance with CLS is required to be assessed.
Provision 5.3-9	Full