MEMORANDUM of COOPERATION

BETWEEN

THE MINISTRY OF ECONOMY, TRADE, AND INDUSTRY OF JAPAN

AND THE DEPARTMENT FOR SCIENCE, INNNOVATION AND TECHNOLOGY OF THE UNITED KINGDOM

ON MUTUAL RECOGNITION OF IOT SECURITY REGIMES

The Ministry of Economy, Trade, and Industry of Japan and The Department for Science, Innovation and Technology of the United Kingdom (hereinafter referred to individually as "Participant" and collectively as "Participants")

With the aim of promoting the harmonisation of standards, reducing the costs for manufacturers and improving the security of connected devices in both countries;

In order to work towards establishing effective mechanisms for the mutual recognition of IoT devices cyber security regimes established in Japan, and the United Kingdom of Great Britain and Northern Ireland;

HAVING REGARD to the desirability of establishing high standards for the cyber security of IoT devices;

RECOGNISING that mutual recognition of our respective IoT cyber security regimes should promote improvements in trade;

HAVE ACCEPTED AS FOLLOWS:

PARAGRAPH 1

Objective

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 cyber security between the Participants, with the aim of pursuing 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 items and definitions are utilised for the purpose of this MoC:

1. "**Conformity Assessment Procedures**" means, in the case of Japan and the UK, the process of determining whether an IoT Product complies with the Requirements;

2. "**Consistency check**" means the process of reviewing a Self-declaration and the information that is provided by the manufacturer in an application, and any included supporting documents to determine whether conformity with the IT security Requirements specified by the Participant is plausibly and comprehensibly assured;

3. "**Cyber Security Scheme**" means, in the case of Japan, the JC-STAR Level 1 scheme. In the case of the UK, the product security regulatory regime created by Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 and Regulations made under that Act;

4. **"IoT Products"** means, in the case of Japan, the IoT devices including both consumer and industrial products that can be connected directly or indirectly to the internet using IP or Internet Protocol will be covered in the scope of this Scheme, excluding general-purpose IT products to which users can easily alter security measures such as via software (PCs, tablets, smartphones, etc.) specified by the Information-technology Promotion Agency supervised by the Ministry of Economy, Trade, and Industry. In the case of the UK, a product that is within scope of the UK's Cyber Security Scheme;

5. "**Label**" means Japan's JC-STAR-1 Label;

6. "**Law-Compliant / Compliant with UK's Law**" means compliant with the UK's product security regulatory regime created by Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 and regulations made under that Act;

7. "**Requirements**" means, in the case of Japan, the IT security requirements applicable to the relevant product category set out under the JC-STAR-1; and in the case of the UK, the security requirements and the requirement to have a statement of compliance accompany a IoT Product as required under the UK's Law; and

8. "**Self-declaration**" means a manufacturer's statement that declares that an IoT device meets the IT security requirements applicable to the relevant product category for the duration specified in line with the Participant's Requirements;

PARAGRAPH 3

Recognition of Label and Law

1. Each Participant will endeavour to recognise the other Participant's Cyber Security Scheme as credible.

2. A Participant will endeavour to recognise the other Participant's Cyber Security Scheme as follows:

    a) An IoT Product that is compliant with the UK's Law will undergo a simplified application process for obtaining a Label under Japan's Cyber Security Scheme stipulated by the Information-technology Promotion Agency of Japan by showing the statement of Self-declaration of the Law-Compliant IoT Product open to the public online.

    b) In line with subparagraph (c) below, an IoT Product that has been issued with a Label upon compliance with Japan's Conformity Assessment Procedures, and also holds a valid label, will be treated as compliant with the UK's Requirements.

    c) Recognition of an IoT Product in line with the aims of this MoC does not preclude a product also having to comply with other applicable UK law, such as applicable product safety regulations.

3. For the avoidance of doubt, this paragraph does not extend to Labels issued to or compliance with Requirements in relation to an IoT Product pursuant to any mutual recognition arrangement with third parties. Where a Participant is discontent with the decision of the other Participant as to the Labelling or fulfilling Requirements of a IoT device, both Participants will endeavour to resolve this discontent through mutual consultations, and may share relevant information for this purpose. If the Participants are not able to resolve this discontent, the Label of the IoT device and the compliance with Requirements concerned will not be capable of being recognised under subparagraph 2 of Paragraph 3.

PARAGRAPH 4

Forms of cooperation

1. The Participants may exchange information regarding the development of applicable standards, cyber security threats and attack methods on IoT devices, Requirements, and other practices concerning IoT cyber security, and share best practices, as appropriate.

2. The Participants will endeavour to have a consultation at least once annually to provide updates on their 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 Cyber Security Schemes and laws, 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

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. Costs and expenses borne by METI would be 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 in line with 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 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 items 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

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 an IoT device:

    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 Items

1. The Participants will take appropriate measures to fulfil their responsibilities under this MoC.

2. This MoC will commence on 01 – 01 - 2026 and will continue for an initial period of three (3) years, and upon discontinuation 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 MoC, the Participants will consult to determine how any outstanding matters should be dealt with.

4. Any contractual obligations to third parties and other Joint Declarations of Intent will remain unaffected.

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

SIGNED in duplicate in the United Kingdom on 5/11/2025 in the English language.

Signed by:

Nobutaka TAKEO
Director, the Cybersecurity Division, Commerce and Information Policy Bureau

Ministry of Economy, Trade and Industry
Japan

Signed by:

Rod Latham
Director for Cyber Security and Digital Identity

Department of Science, Innovation and Technology
The United Kingdom