AGREEMENT BETWEEN
THE GOVERNMENT OF JAPAN
AND THE GOVERNMENT OF CANADA
ON THE SECURITY OF INFORMATION

Preamble

The Government of Japan and the Government of Canada (hereinafter referred to as “the Parties” and separately as a “Party”),

Wishing to ensure the reciprocal protection of classified information exchanged between the Parties,

Have agreed as follows:

ARTICLE 1
Scope

1. Nothing in this Agreement shall be interpreted as compelling the exchange of information between the Parties.

2. The provisions of this Agreement shall not affect the implementation of any existing bilateral agreements in force between the Parties.

ARTICLE 2
Definitions

For the purposes of this Agreement:

a. “Classified Information” means any information which is assigned a Security Classification by a Party, and which requires protection against unauthorized disclosure, access, or destruction in the interest of national security of the country of the Providing Party and in accordance with the national laws, regulations, and procedures of the Providing Party. This information may be in any form, including oral, visual, electronic, magnetic, documentary forms, or in the form of material, equipment, or technology. For the Government of Canada, a reference to Classified Information in this Agreement also includes Canadian Protected Information, unless otherwise specified;

b. “Competent Authorities” (CAs) means, in relation to the Government of Japan, the government agencies, and in relation to the Government of Canada, the government organizations, which are designated by each Party as the authorities responsible, within their respective competence under the national laws, regulations, and procedures, for the protection of Classified Information and Transmitted Classified Information;

c. “Contractor” means an individual or a legal entity, including a subcontractor, that performs a contract with the Receiving Party;

d. “Need to Know” means the need to have access to Classified Information and Transmitted Classified Information, which is limited to authorized individuals for the performance of officially assigned duties;

e. “National Security Authority” (NSA) means a government authority designated by each Party to serve as a point of coordination and liaison with regard to the implementation and interpretation of this Agreement;

f. “Personnel Security Clearance” means the eligibility for an individual to access Classified Information and Transmitted Classified Information up to a specified level, which is granted subject to each Party’s procedures;

g. “Providing Party” means the Party which transmits Classified Information to the Receiving Party;

h. “Receiving Party” means the Party to which Classified Information is transmitted by the Providing Party;

i. “Security Classification” means the identification assigned by a Party to indicate the necessary level of protection that information must be afforded;

j. “Third Party” means any government, individual, firm, institution, organization, other legal entity of a third country, or an international organization not being a Party to this Agreement. For the purpose of this Agreement, an individual who holds a Personnel Security Clearance, has a Need to Know and has been granted access to Transmitted Classified Information pursuant to Article 17 of this Agreement is not considered a Third Party; and

k. “Transmitted Classified Information” means Classified Information which is transmitted directly or indirectly between the Parties. Classified Information becomes Transmitted Classified Information upon receipt by the Receiving Party. All reference in this Agreement to Transmitted Classified Information and to the transmission of Classified Information shall include reference to Protected Information which is transmitted from the Government of Canada to the Government of Japan.

ARTICLE 3
Protection of Transmitted Classified Information

Transmitted Classified Information shall be protected under the terms set out in this Agreement, provided that those terms are consistent with the national laws, regulations, and procedures of the Receiving Party.

ARTICLE 4

Changes in National Laws and Regulations

Each Party shall notify the other Party of any changes to its national laws and regulations that would affect the protection of Transmitted Classified Information under this Agreement. In that case, the Parties shall consult each other as provided for in Article 20, to consider possible amendments to this Agreement. In the interim, Transmitted Classified Information shall continue to be protected according to the provisions of this Agreement, provided that those provisions are consistent with the national laws and regulations of the Receiving Party, unless otherwise approved in writing by the Providing Party.

ARTICLE 5

Security Classifications and Markings

1. Classified Information to be provided under this Agreement shall be marked with one of the following Security Classifications:

a. For the Government of Japan, Classified Information is marked GOKUHI (KIMITSU) 極秘 (機密), TOKUTEI HIMITSU (KIMITSU) 特定秘密 (機密), GOKUHI 極秘, TOKUTEI HIMITSU 特定秘密, HI 秘, or JUYO KEIZAI AMPO JOHO 重要経済安保情報;

b. For the Government of Canada, Classified Information is marked TOP SECRET, TRÈS SECRET, SECRET, CONFIDENTIAL or CONFIDENTIEL.

2. The Government of Japan, which has no corresponding Security Classification to Protected Information, shall handle and protect Canadian information marked as PROTECTED C or PROTÉGÉ C as if it is GOKUHI 極秘 or TOKUTEI HIMITSU 特定秘密, and Canadian information marked as PROTECTED B, PROTÉGÉ B, PROTECTED A or PROTÉGÉ A as if it is HI 秘, unless otherwise mutually determined by the Parties.

3. For Classified Information where a marking is not physically possible, the Providing Party shall inform the Receiving Party of the Security Classification. If the Receiving Party so requests, the Providing Party shall inform the Receiving Party of the Security Classification in writing.

4. The Receiving Party shall mark, where practicable, all Transmitted Classified Information with the name of the Providing Party and the corresponding Security Classification of the Receiving Party, as described in paragraphs 5 and 6 of this Article.

5. The corresponding Security Classifications in relation to paragraph 1 of this Article are:

In Japan	In Canada
GOKUHI (KIMITSU) 極秘 (機密) or TOKUTEI HIMITSU (KIMITSU) 特定秘密(機密)	TOP SECRET or TRÈS SECRET
GOKUHI 極秘 or TOKUTEI HIMITSU 特定秘密	SECRET
HI 秘 or JUYO KEIZAI AMPO JOHO 重要経済安保情報	CONFIDENTIAL or CONFIDENTIEL

6. Security Classifications for Canadian Protected Information in relation to paragraph 2 of this Article are:

In Japan	In Canada
No corresponding Security Classification, but shall be protected as if it is GOKUHI 極秘 or TOKUTEI HIMITSU 特定秘密, unless otherwise mutually determined by the Parties.	PROTECTED C or PROTÉGÉ C

No corresponding Security Classification, but shall be protected as if it is HI 秘, unless otherwise mutually determined by the Parties.	PROTECTED B or PROTÉGÉ B
No corresponding Security Classification, but shall be protected as if it is HI 秘, unless otherwise mutually determined by the Parties.	PROTECTED A or PROTÉGÉ A

ARTICLE 6

National Security Authority and Competent Authorities

1. The National Security Authorities shall be:

a. For the Government of Japan:

Ministry of Foreign Affairs;

b. For the Government of Canada:

Department of Public Works and Government Services, or its successor.

2. The NSAs and the CAs shall monitor the implementation of this Agreement within their competence.

3. The Parties shall notify each other in writing of their respective CAs through diplomatic channels.

ARTICLE 7

Principles for Protecting Transmitted Classified Information

1. The Receiving Party shall not release Transmitted Classified Information to any Third Party without the prior written approval of the Providing Party.

2. The Receiving Party shall, in accordance with its national laws, regulations, and procedures, afford Transmitted Classified Information a level of protection equal to that which it affords its own Classified Information at the corresponding level of Security Classification.

3. The Receiving Party shall not use Transmitted Classified Information for any purpose other than that for which it is provided without the prior written approval of the Providing Party.

4. The Providing Party may specify in writing additional limitations on access to and on the use, disclosure, and release of Transmitted Classified Information by the Receiving Party, and the Receiving Party shall comply with any such limitations.

5. The Receiving Party shall observe intellectual property rights such as patents, copyrights, or trade secrets applicable to Transmitted Classified Information, in accordance with its national laws, regulations, and procedures.

6. Each Party shall maintain a register of individuals with a Personnel Security Clearance and who are authorized to have access to Classified Information and Transmitted Classified Information.

7. The Receiving Party shall establish procedures for the identification, location, inventory, and control of Transmitted Classified Information to manage the dissemination of and access to Transmitted Classified Information.

8. The Providing Party shall inform the Receiving Party of any subsequent change in the Security Classification of the Transmitted Classified Information which it has provided to the Receiving Party.

ARTICLE 8
Access to Transmitted Classified Information

1. No individual shall be entitled to have access to Transmitted Classified Information solely by virtue of rank, appointment, or a Personnel Security Clearance.

2. Access to Transmitted Classified Information shall only be granted to those individuals who have a Need to Know and who have been granted a Personnel Security Clearance in accordance with the national laws, regulations, and procedures of the Receiving Party.

3. The Receiving Party shall take appropriate measures to ensure that the determination on the granting of a Personnel Security Clearance to an individual is consistent with the interests of national security and based upon all relevant information indicating whether the individual is trustworthy and reliable in the handling of Transmitted Classified Information.

4. The Receiving Party shall take appropriate measures to ensure that the criteria referred to in the preceding paragraph have been met, in accordance with its national laws, regulations, and procedures, in respect of any individual to be granted access to Transmitted Classified Information.

5. Before a representative of the Providing Party provides Classified Information to a representative of the Receiving Party, the Providing Party shall obtain an assurance from the relevant Competent Authority of the Receiving Party that the proposed recipient has a Need to Know and holds the necessary level of Personnel Security Clearance appropriate to the corresponding level of Security Classification in accordance with Article 5.

ARTICLE 9
Visit Procedures

1. Visits that involve access by individuals of one Party to Classified Information held by the other Party shall be undertaken only with the prior approval of the other Party. Approval for such visits may be granted only to those individuals who have a Need to Know and hold the necessary level of Personnel Security Clearance as set out in Article 8.

2. Requests for visits shall be submitted by a CA of the visiting Party through Government-to-Government channels to a CA of the other Party and shall include verification of the fact that the visiting individuals have a Need to Know and hold the necessary level of Personnel Security Clearance as set out in Article 8.

ARTICLE 10

Transmission of Classified Information

Classified Information shall be transmitted between the Parties through Government-to-Government channels. The Providing Party shall be responsible for custody, control, and security of all Classified Information until its receipt by the Receiving Party, subject to the national laws, regulations, and procedures of the Providing Party.

ARTICLE 11

Security Requirements during Transmission of Classified Information

The minimum requirements for the security of Classified Information during transmission between the Parties shall be as follows:

a. For Classified Information in the form of documents or other media:

(i) Classified Information shall be transmitted in a sealed or tamper-indicating envelope enclosed within another sealed or tamper-indicating envelope or within a security pouch, the innermost envelope bearing only the Security Classification of the documents or other media and the organizational address of the intended recipient, the outer envelope or the security pouch bearing the organizational address of the recipient, the organizational address of the sender, and the registration number, if applicable.

(ii) No indication of the Security Classification of the enclosed documents or other media shall be shown on the outer envelope or the security pouch.

(iii) Receipts shall be prepared for packages containing Classified Information. A receipt for the enclosed Classified Information shall be signed by the Receiving Party's final recipient and returned to the Providing Party's sender.

b. For Classified Information in the form of, or which is contained in, equipment:

(i) Classified Information shall be transmitted in sealed and covered vehicles, or be securely packaged or protected, in order to prevent identification of its contents and kept under continuous control to prevent access by unauthorized individuals.

(ii) Classified Information that is awaiting shipment shall be placed in protected storage areas that provide protection commensurate with the level of Security Classification of the Classified Information. Only authorized individuals with the necessary level of Personnel Security Clearance shall have access to the equipment.

(iii) Receipts shall be obtained on every occasion when Classified Information changes hands en route and is delivered to the Receiving Party's final recipient. All receipts shall be returned to the Providing Party's sender.

c. For Electronic Transmissions:

(i) Classified Information shall be protected during transmission using encryption appropriate for the level of Security Classification. Information systems' standards for processing or storing Transmitted Classified Information or conveying Classified Information shall receive security accreditation by the appropriate authority of the Party employing the system.

(ii) The Receiving Party shall maintain a record of the receipt of Transmitted Classified Information. This record shall be made available to the Providing Party upon request.

ARTICLE 12
Security of Facilities

1. Each Party shall be responsible for the security of all governmental facilities where Transmitted Classified Information is kept.

2. For each governmental facility, the Receiving Party shall ensure that government officials are appointed who shall have the responsibility and authority for the control and protection of Transmitted Classified Information.

ARTICLE 13
Storage of Transmitted Classified Information

The Receiving Party shall store Transmitted Classified Information in a manner that ensures access is limited to individuals authorized as set out in Article 8.

ARTICLE 14
Destruction of Transmitted Classified Information

When no longer required to retain it for the purpose for which it was provided, Transmitted Classified Information shall be destroyed by the Receiving Party in a manner that prevents its reconstruction in whole or in part in accordance with the national laws, regulations, and procedures of the Receiving Party.

ARTICLE 15
Reproduction of Transmitted Classified Information

When the Receiving Party reproduces Transmitted Classified Information in the form of documents or other media, it shall also reproduce all original Security Classification markings applied to the Transmitted Classified Information or mark them on each copy. The Receiving Party shall place any reproduced Transmitted Classified Information under the same controls as the original Transmitted Classified Information. The Receiving Party shall limit the number of copies to that required for official purposes.

ARTICLE 16

Translation of Transmitted Classified Information

The Receiving Party shall ensure that any translation of Transmitted Classified Information is carried out by individuals who have a Need to Know and hold the necessary level of Personnel Security Clearance as set out in Article 8. The Receiving Party shall keep the number of copies of a translation to a minimum and control any distribution. Any translations shall bear markings of the Security Classification of the Receiving Party corresponding to the original Security Classification and suitable notation in the language into which the translation was made indicating that the translation contains Transmitted Classified Information. The Receiving Party shall place the translation under the same controls as the original Transmitted Classified Information.

ARTICLE 17

Release of Transmitted Classified Information to Contractors

Prior to the release to a Contractor of any Transmitted Classified Information, the Receiving Party shall, subject to its national laws, regulations, and procedures, take appropriate measures to ensure that:

a. the Contractor's facilities have the capability to protect Transmitted Classified Information at the relevant level of Security Classification;

b. all individuals who have access to Transmitted Classified Information are informed of their responsibilities to protect Transmitted Classified Information;

c. information generated by Contractors using Transmitted Classified Information in whole or in part is marked with the comparable level of Security Classification of the Receiving Party and receives comparable protection to the original Transmitted Classified Information in accordance with the relevant provisions of this Agreement for the use, storage, destruction, and disclosure of Transmitted Classified Information;

d. initial and periodic security inspections are carried out by the CAs of the Receiving Party at each Contractor's facility where Transmitted Classified Information is stored or accessed to ensure that it is appropriately protected in the same manner as required by this Agreement;

e. CAs ensure that a register of individuals with a Personnel Security Clearance who are authorized to have access to Transmitted Classified Information is maintained at each Contractor's facility where Transmitted Classified Information is stored or accessed;

f. CAs ensure that individuals are appointed at each Contractor's facility who shall have the responsibility and authority for the control and protection of Transmitted Classified Information; and

g. CAs ensure that Contractors apply and maintain the requisite security measures for the protection of Transmitted Classified Information in the same manner as required by this Agreement.

ARTICLE 18
Loss or Compromise of Transmitted Classified Information

1. The Receiving Party shall investigate all cases in which it is known, or where there are grounds for suspecting, that Transmitted Classified Information has been lost, compromised, or disclosed to unauthorized individuals or legal entities.

2. The Receiving Party shall promptly and fully inform the Providing Party of all losses, compromises, or unauthorized disclosures, as well as suspected losses, compromises, or unauthorized disclosures of Transmitted Classified Information.

3. The Receiving Party shall provide in writing to the Providing Party the details of the final results of the investigation and of the actions taken to prevent recurrences.

ARTICLE 19
Procedural Arrangement and Implementing Arrangements

1. The Parties shall make a Procedural Arrangement, which is subordinate to this Agreement and shall specify supplementary provisions to implement this Agreement.

2. CAs, within their competence, may mutually determine Implementing Arrangements, which are subordinate to this Agreement and which specify supplementary provisions to implement this Agreement.

ARTICLE 20
Disputes and Consultation

1. The Parties shall consult each other regarding the implementation of this Agreement.

2. Any matter relating to the interpretation or application of this Agreement, the Procedural Arrangement and any Implementing Arrangements shall be resolved solely through consultation between the Parties.

3. The CAs of the Parties shall resolve differences that may arise concerning the implementation of any Implementing Arrangements through consultation between the CAs.

4. Where a difference cannot be resolved under the provisions of paragraph 3 of this Article, the matter shall be settled in accordance with the provisions of paragraph 2 of this Article.

ARTICLE 21
Visits by Security Representatives

Implementation of this Agreement can be promoted through reciprocal visits by security representatives of the Parties. With the mutual consent of the Parties, security representatives of each Party may be permitted to make visits to facilities of the other Party to discuss their respective security procedures and observe their implementation in the interests of achieving appropriate comparability of their respective security systems.

ARTICLE 22
Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement, in accordance with its national laws, regulations, and procedures and within the limit of its annual budgetary appropriations.

ARTICLE 23
Entry into Force, Amendment, Duration, and Termination

1. This Agreement shall enter into force on the date of the last note of an exchange of diplomatic notes in which the Parties notify each other that their respective internal procedures necessary for the entry into force of this Agreement have been completed.

2. This Agreement may be amended by written agreement between the Parties. Any amendment of this Agreement shall follow the same procedure as its entry into force.

3. This Agreement shall remain in force for a period of one year and shall be automatically extended for one-year periods thereafter unless either Party notifies the other Party in writing through diplomatic channels of its intention to terminate this Agreement at least ninety days prior to the expiration of each period of one year.

4. Notwithstanding the termination of this Agreement, all Transmitted Classified Information provided under this Agreement shall continue to be protected according to the terms set forth in this Agreement.

IN WITNESS WHEREOF the undersigned, being duly authorized by their respective Governments, have signed this Agreement.

DONE in duplicate at Tokyo on this 8th day of July 2025, in the Japanese, English, and French languages, each version being equally authentic.

For the Government of Japan:	For the Government of Canada:
岩屋　毅	Anita Anand