

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
CANBERRA

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

(Tokyo, 17 May 2012)

Not yet in force
[2012] ATNIF 10

Preamble

The Government of Australia and the Government of Japan (hereinafter referred to as "the Parties" and separately as "a Party"),

AFFIRMING their commitment to the promotion of bilateral security cooperation through the implementation of the Joint Declaration on Security Cooperation, signed at Tokyo on 13 March, 2007;

HAVING a mutual interest in the protection of classified information; and

WISHING to ensure the reciprocal protection of classified information exchanged between the Parties;

Have agreed as follows:

ARTICLE 1 Definitions

For the purposes of this Agreement:

- a. "Classified Information" means all information which requires protection against unauthorised disclosure in the interest of the national security of the Providing Party and which is subject to a Security Classification and generated by, or for the use of, or under the jurisdiction of, the Competent Authorities of the Government of Japan or the Government of Australia. The information may be in any form, including oral, visual, electronic, magnetic, or documentary forms, or equipment or technology, and may also include any reproductions or translations;
- b. "Providing Party" means the Party which transmits Classified Information to the Receiving Party;
- c. "Receiving Party" means the Party to which Classified Information is transmitted;
- d. "Security Classification" means the identification assigned to Classified Information by a Party to indicate the necessary level of protection that information must be afforded to prevent it from unauthorised disclosure;
- e. "Competent Authorities" means agencies of the Receiving Party which are designated by the Party as authorities responsible for the protection of Transmitted Classified Information. The Competent Authorities shall be specified in the Procedural Arrangement;

- f. "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;
- g. "National Laws and Regulations" means the laws and regulations relating to this Agreement that include, but are not restricted to:
 - (i) in relation to Japan, Self-Defense Forces Law (Law No. 165, 1954) and National Public Service Law (Law No. 120, 1947), and
 - (ii) in relation to Australia, the laws that shall be specified in the Procedural Arrangement;
- h. "Third Party" means any government, individual, or entity other than the Parties;
- i. "Third Partner" means the government of a third State or an intergovernmental organisation with which the Receiving Party has concluded an agreement or arrangement concerning the protection of classified information;
- j. "Personnel Security Clearance" means the eligibility, granted by a Competent Authority of a Party, subject to that Party's procedures, for an individual to access Classified Information to a specified level;
- k. "Security Policies" means each Party's policies for the protection of Classified Information and Transmitted Classified Information, including National Laws and Regulations, as specified in the Procedural Arrangement and as may be modified from time to time; and
- l. "Contractor" means an individual or entity, including subcontractor, that performs a contract with the Receiving Party.

ARTICLE 2

Protection of Transmitted Classified Information

Transmitted Classified Information shall be protected according to the terms set forth in this Agreement and is also to be protected in accordance with the Procedural Arrangement and any Implementing Arrangements, subject to the National Laws and Regulations in force of the Receiving Party.

ARTICLE 3

National Security Authority and Competent Authorities

1. The National Security Authority for each Party shall be:
 - a. For the Government of Japan:
Ministry of Foreign Affairs; and
 - b. For the Government of Australia:
Attorney-General's Department.
2. The National Security Authority shall serve as a point of coordination and liaison with regard to the implementation and interpretation of this Agreement.
3. The National Security Authority and the Competent Authorities shall monitor the implementation of this Agreement within their competence.

ARTICLE 4
Security Classifications

1. The Providing Party shall mark all Classified Information with one of the following Security Classifications:
 - a. For the Government of Japan, Classified Information that is designated as "Defense Secret" according to the Self-Defense Forces Law is marked BOUEI HIMITSU (KIMITSU) 防衛秘密 or BOUEI HIMITSU 防衛秘密 and the other Classified Information is marked KIMITSU 機密 GOKUHI 極秘 or HI 秘 and
 - b. For the Government of Australia, Classified Information is marked TOP SECRET, SECRET, HIGHLY PROTECTED, CONFIDENTIAL, PROTECTED, RESTRICTED, or IN CONFIDENCE.
2. 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 Security Classification in writing.
3. The Receiving Party shall mark all Transmitted Classified Information with the name of the Providing Party and the corresponding Security Classification of the Receiving Party, as described in paragraph 4 of this Article.

4. The corresponding Security Classifications are:

In Australia

In Japan

TOP SECRET

Kimitsu 機密
/Bouei Himitsu
(Kimitsu) 防衛秘密

SECRET
/HIGHLY PROTECTED

Gokuhi 極秘
/Bouei Himitsu 防衛秘密

CONFIDENTIAL
/PROTECTED

Hi 秘

RESTRICTED
/IN CONFIDENCE

No Japanese
correspondent, but
shall be protected as
if it is Hi 秘 unless
otherwise advised by
the Government of
Australia.

5. The Providing Party shall inform the Receiving Party of any change in the Security Classification of Transmitted Classified Information. Upon receipt of such information, the Receiving Party shall change the Security Classification of the Transmitted Classified Information accordingly. If the Receiving Party so requests, the Providing Party shall inform the change in writing.

6. The Receiving Party shall not downgrade the Security Classification of the Transmitted Classified Information without the prior written consent of the Providing Party.

ARTICLE 5
Principles for
Protecting Transmitted Classified Information

Each Party shall apply the following rules to Transmitted Classified Information, subject to its National Laws and Regulations in force:

- a. The Receiving Party shall take appropriate measures to provide all Transmitted Classified Information a degree of protection equivalent in effect to that afforded to it by the Providing Party;
- b. The Receiving Party shall not release Transmitted Classified Information to a Third Party unless otherwise provided for in this Agreement or agreed in writing by the Parties;
- c. The Receiving Party shall take appropriate measures to prevent unauthorised disclosure of Transmitted Classified Information;
- d. The Receiving Party shall take appropriate measures to ensure that necessary inspections are carried out and relevant Security Policies are complied with in order to protect Transmitted Classified Information;
- e. The Receiving Party shall establish procedures for the identification, location, inventory and control of

Transmitted Classified Information, which are to be outlined in the Procedural Arrangement;

- f. The Receiving Party shall not use or permit the use of Transmitted Classified Information for any purpose other than that for which it is provided without the prior written approval of the Providing Party;
- g. The Receiving Party shall observe intellectual property rights such as patents, copyrights, or trade secrets applicable to Transmitted Classified Information;
- h. The Providing Party may specify in writing additional limitations on the use, disclosure, and release of, and access to Transmitted Classified Information by the Receiving Party, and the Receiving Party shall comply with any such limitations; and
- i. The Receiving Party may release Transmitted Classified Information to a Third Partner if the Providing Party specifies that the information is releasable to the Third Partner.

ARTICLE 6

Access to Transmitted Classified Information

Prior to the release to an individual, including a Contractor, of any Transmitted Classified Information, the Receiving Party shall, subject to its National Laws and Regulations in force, take appropriate measures to ensure that:

- a. No individual shall be entitled to access Transmitted Classified Information solely by virtue of rank, appointment, or a Personnel Security Clearance;
- b. Access to Transmitted Classified Information shall be limited to those individuals who:
 - (i) Require access to the Transmitted Classified Information for the performance of their official duties, and
 - (ii) Hold a current Personnel Security Clearance to the necessary level;
- c. The granting of a Personnel Security Clearance shall be consistent with the interests of national security and based upon all available information indicating whether the individual is trustworthy and reliable in the handling of Transmitted Classified Information;
- d. An appropriate investigation for the granting of a Personnel Security Clearance shall be conducted so that the criteria referred to in paragraph c of this Article have been met with respect to any individual to be granted access to Transmitted Classified Information;

- e. All individuals who are granted access to Transmitted Classified Information shall be informed of their responsibilities to protect the information; and
- f. An assurance in writing shall be provided to the Providing Party, upon its request, that the individual receiving the Transmitted Classified Information possesses the necessary level of Personnel Security Clearance and requires access for the performance of their official duties.

ARTICLE 7

Release of Transmitted Classified Information to Contractors

The Receiving Party may release Transmitted Classified Information to a Contractor, where the Parties mutually determine in writing, or if the Providing Party otherwise specifies that the information is releasable to a Contractor. Prior to the release to a Contractor of any Transmitted Classified Information, the Receiving Party shall, subject to its National Laws and Regulations in force, take appropriate measures to ensure that:

- a. The Contractor and the Contractor's facilities have the capability to protect the Transmitted Classified Information; and
- b. Initial and periodic security inspections are carried out at the Contractor's facilities to ensure that Transmitted Classified Information is protected in accordance with the terms set forth in this Agreement and any Implementing Arrangements.

ARTICLE 8

Security of Facilities

The Receiving Party shall, subject to its National Laws and Regulations in force, take appropriate measures to ensure that:

- a. All facilities where Transmitted Classified Information is handled are secured in accordance with the terms set forth in this Agreement and any Implementing Arrangements;
- b. For each such facility, individuals are appointed who shall have the responsibility and authority for the control and protection of Transmitted Classified Information and shall hold a current Personnel Security Clearance to the necessary level; and

- c. Each facility that handles Transmitted Classified Information shall maintain a register of individuals holding a current Personnel Security Clearance who are authorised to have access to such information.

ARTICLE 9

Storage of Transmitted Classified Information

1. The Receiving Party shall, subject to its National Laws and Regulations in force, take appropriate measures to ensure that Transmitted Classified Information shall be stored in a manner that ensures access only by those individuals who have been authorised to access Transmitted Classified Information in accordance with Article 6 of this Agreement.
2. Subject to National Laws and Regulations in force, all information systems used to store Transmitted Classified Information in electronic form shall be protected in accordance with procedures that may be developed between the Parties or between Competent Authorities of the Parties.

ARTICLE 10

Transmission

Classified Information shall be transmitted between the Parties through Government-to-Government channels. While in transit, 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 and Regulations in force of the Providing Party.

ARTICLE 11

Security Requirements during Transmission

1. The minimum requirements for the security of the Classified Information during transmission between the Parties shall be as follows:
 - a. Classified Information in the form of documents or other media
 - (i) Classified Information in the form of documents or other media 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 organisational address of the intended recipient, the outer envelope or the security pouch

bearing the organisational address of the recipient, the organisational address of the sender, and the registry number, if applicable.

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

(iii) Receipts shall be prepared for packages containing Classified Information in the form of documents or other media that are transmitted between the Parties, and 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. Classified Information in the form of or contained in equipment

(i) Classified Information in the form of or contained in equipment shall be transmitted in sealed, 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 unauthorised individuals.

(ii) Classified Information in the form of or contained in equipment that is temporarily awaiting shipment shall be placed in protected storage areas that provide protection commensurate with the level of Security Classification of the Classified Information. Only authorised personnel with the appropriate Personnel Security Clearance shall have access to the storage areas.

(iii) Receipts shall be obtained on every occasion when Classified Information in the form of or contained in equipment 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. Electronic Transmissions

(i) Classified Information transmitted by electronic means shall be protected during transmission using encryption appropriate for that level of Classified Information. 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 log of Transmitted Classified Information received by electronic means from the Providing Party. This

log shall be made available to the Providing Party upon request.

2. The requirements outlined in paragraph 1 above for the security of Classified Information during transmission between the Parties shall correspondingly apply to the transmission of Transmitted Classified Information between Competent Authorities of the Receiving Party.

ARTICLE 12 Changes in Security Policies

1. On request, the Receiving Party shall provide the Providing Party with a copy of its Security Policies.

2. The Receiving Party shall promptly notify the Providing Party in writing of any changes to relevant Security Policies that would adversely affect the protection of Transmitted Classified Information under this Agreement. In such cases, the Parties shall consult on possible amendments to this Agreement or possible modifications to the Procedural Arrangement. In the interim, Transmitted Classified Information shall continue to be protected according to the terms set forth in this Agreement and is also to be protected in accordance with the Procedural Arrangement, unless otherwise approved in writing by the Providing Party.

ARTICLE 13 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 shall only be granted to individuals who possess the necessary level of Personnel Security Clearance and who require such access for the performance of their official duties.

2. Requests for visits shall be submitted by the relevant Competent Authority of the visiting Party through Government-to-Government channels to the relevant Competent Authority of the other Party and shall include verification of the fact that the visiting individuals hold a Personnel Security Clearance to the necessary level.

ARTICLE 14 Visits by Security Personnel

Implementation of the requirements provided for in this Agreement can be advanced through visits by security personnel,

designated as such by the National Security Authority or a Competent Authority of the visiting Party. Accordingly, the security personnel, after prior consultation, shall be permitted to visit the other Party, to discuss the other Party's security procedures and observe their implementation in the interest of achieving reasonable comparability of their respective security systems at mutually agreed venues and in a mutually satisfactory manner. The other Party shall assist the visiting security personnel in determining whether Transmitted Classified Information is being adequately protected.

ARTICLE 15

Destruction of Transmitted Classified Information

1. Transmitted Classified Information in the form of documents or other media shall be destroyed by burning, shredding, pulping, or other means preventing reconstruction in whole or in part of the Transmitted Classified Information contained therein.
2. Transmitted Classified Information in the form of or contained in equipment shall be destroyed beyond recognition so as to preclude reconstruction of the Transmitted Classified Information in whole or in part.

ARTICLE 16

Loss or Compromise of Transmitted Classified Information

1. The Providing Party shall be informed immediately of all losses or compromises, as well as suspected losses or compromises, of Transmitted Classified Information, and the Receiving Party shall investigate to determine the circumstances.
2. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided in writing to the Providing Party.

ARTICLE 17

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. Competent Authorities, within their competence, may mutually determine Implementing Arrangements, which are subordinate to this Agreement and which shall specify supplementary provisions regarding the handling of Transmitted Classified Information.

ARTICLE 18
Disputes and Consultation

1. The Parties shall consult closely with 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 Competent Authorities of the Parties shall settle disputes that may arise concerning the implementation of the Implementing Arrangements through consultation between the Competent Authorities.
4. Where a dispute cannot be settled under the provisions of paragraph 3 of this Article, the dispute shall be settled in accordance with the provisions of paragraph 2 of this Article.

ARTICLE 19
Entry into Force, Amendment, Duration, and Termination

1. This Agreement shall enter into force on the date on which written notifications have been received by both Parties, through diplomatic channels, that their respective internal legal procedures for entry into force of the 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 annually thereafter unless:
 - a. The Parties otherwise agree; or
 - b. A Party gives to the other notice in writing of its desire to terminate this Agreement, in which event this Agreement shall be terminated one hundred and eighty days after the date on which the notice is given.
4. Notwithstanding the termination of this Agreement, all Transmitted Classified Information provided pursuant to this Agreement shall continue to be protected according to the terms set forth in this Agreement.

IN WITNESS WHEREOF, the undersigned, being duly authorised thereto by their respective governments, have signed this Agreement.

DONE in duplicate at Tokyo this seventeenth day of May 2012 in the English and Japanese languages, both texts being equally authentic.

FOR THE GOVERNMENT
OF AUSTRALIA:

FOR THE GOVERNMENT
OF JAPAN: