AGREEMENT BETWEEN THE GOVERNMENT OF JAPAN AND THE GOVERNMENT OF THE REPUBLIC OF KOREA ON THE PROTECTION OF CLASSIFIED MILITARY INFORMATION

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

Wishing to ensure the reciprocal protection of Classified Military Information exchanged between the Parties;

Have agreed as follows:

ARTICLE 1
PURPOSE

The Parties shall ensure the protection of Classified Military Information (hereinafter referred to as "CMI") under the terms set forth herein, provided that they are consistent with the national laws and regulations in force of the respective Parties.

ARTICLE 2
DEFINITIONS

For the purposes of this Agreement,

(a) "CMI" means any defense-related information that is generated by or for the use of or held by the Competent Authorities of the Government of Japan or the Government of the Republic of Korea, and that requires protection in the interests of national security of the respective Parties. The information shall bear a security classification and, where necessary, an appropriate indication to identify such information as CMI. Such information may be in oral, visual, electronic, magnetic, or documentary form, or in the form of equipment or technology;

(b) "Originating Party" means the Party that provides CMI;

(c) "Receiving Party" means the Party that receives CMI provided by the Originating Party;

(d) "Competent Authorities" means agencies of a Party which are designated by the Party as authorities responsible for the protection of defense-related information. Each Party shall notify the other Party, through the diplomatic channel, of its Competent Authorities; and

(e) "Personnel Security Clearance" means an eligibility for handling securely CMI granted to individuals in accordance with each Party's appropriate procedures.

ARTICLE 3
NATIONAL LAWS AND REGULATIONS

Each Party shall notify the other Party of its national laws and regulations in force related to the protection of CMI, upon request, and of any changes to them that would affect the protection of CMI under this Agreement.

ARTICLE 4
SECURITY CLASSIFICATION AND MARKING OF CMI

1. CMI shall be marked with one of the following security classifications:

(a) in relation to the Government of Japan, Gokuhi 極秘, Tokutei Himitsu 特定秘密, or Hi 秘; and

(b) in relation to the Government of the Republic of Korea, GUNSA II-KUP BI MIL 군사Ⅱ급비밀 or GUNSA III-KUP BI MIL 군사Ⅲ급비밀.

2. The Receiving Party shall mark all provided CMI with the name of the Originating Party and the corresponding security classification of the Receiving Party as follows:

Japan	The Republic of Korea	Note: Equivalent in English
Gokuhi 極秘/ Tokutei Himitsu 特定秘密	GUNSA II-KUP BI MIL 군사Ⅱ급 비밀	SECRET
Hi 秘	GUNSA III-KUP BI MIL 군사Ⅲ급 비밀	CONFIDENTIAL

3. Documents or media produced by the Receiving Party that contain CMI provided by the Originating Party shall be marked with the appropriate security classification and shall bear an indication that the documents or media contain CMI provided by the Originating Party.

ARTICLE 5
SUPPLEMENTAL IMPLEMENTING ARRANGEMENT

Supplemental implementing arrangements under this Agreement may be made by the Competent Authorities of the Parties.

ARTICLE 6
PRINCIPLES OF PROTECTING CMI

In order to protect provided CMI, the Parties shall ensure that:

(a) the Receiving Party shall not release the CMI to any government, person, firm, institution, organization, or other entity of a third country without the prior written approval of the Originating Party;

(b) the Receiving Party, subject to its national laws and regulations in force, shall take appropriate measures to provide to the CMI a degree of protection substantially equivalent to that afforded by the Originating Party;

(c) the Receiving Party shall not use the CMI for any other purpose than that for which it was provided, without the prior written approval of the Originating Party;

(d) the Receiving Party shall observe intellectual property rights such as patents, copyrights, or trade secrets applicable to the CMI, subject to its national laws and regulations in force;

(e) each governmental facility that handles the CMI shall maintain a registry of individuals who have Personnel Security Clearances and are authorized to have access to such information;

(f) procedures for identification, location, inventory, and control of the CMI shall be established by each Party to manage the dissemination of and access to the CMI;

(g) the Originating Party shall promptly notify, in writing, the Receiving Party of any changes in the security classification of the CMI which was previously provided to the Receiving Party. The Receiving Party shall alter the security classification of the CMI in accordance with the Originating Party's notification; and

(h) when the CMI is no longer required for the purpose for which it was provided, the Receiving Party shall, as appropriate, either:

(i) return the CMI to the Originating Party; or

(ii) destroy the CMI in accordance with Article 13 and subject to its national laws and regulations in force.

ARTICLE 7
PERSONNEL ACCESS TO CMI

1. No government official shall be entitled to access to provided CMI solely by virtue of rank, appointment, or a Personnel Security Clearance.

2. Access to provided CMI shall be granted only to those government officials whose official duties require such access and who have been granted a Personnel Security Clearance subject to the national laws and regulations in force of the Receiving Party.

3. The Parties shall ensure that the determination on the granting to a government official of a Personnel Security Clearance is consistent with the interests of national security and based upon all available information indicating whether the government official is trustworthy and reliable in the handling of provided CMI.

4. Appropriate procedures shall be implemented by the Parties to ensure that the criteria referred to in the preceding paragraph have been met, subject to the national laws and regulations in force of each Party, with respect to any government official to be granted access to provided CMI.

5. Before a representative of one Party provides CMI to a representative of the other Party, the Receiving Party shall provide to the Originating Party an assurance that:

(a) the representative possesses the necessary level of Personnel Security Clearance;

(b) the representative requires access for official purposes; and

(c) the Receiving Party, subject to its national laws and regulations in force, shall take appropriate measures to provide to the CMI a degree of protection substantially equivalent to that afforded by the Originating Party.

ARTICLE 8
VISIT

Authorizations for visits by representatives of one Party to facilities of the other Party where access to CMI is required shall be limited to those necessary for official purposes. Authorization to visit a facility that is located in the territory of the country of one Party shall be granted only by the Party. The visited Party shall be responsible for advising the facility of the proposed visit, the topic, the scope, and highest level of CMI that may be furnished to the visitor. Requests for visits by representatives of the Parties shall be submitted by the relevant Competent Authority of the visiting Party to the relevant Competent Authority of the visited Party.

ARTICLE 9
TRANSMISSION OF CMI

CMI shall be transmitted between the Parties through Government-to-Government channels. Upon such transfer, the Receiving Party shall assume responsibility for custody, control, and security of the CMI.

ARTICLE 10
SECURITY OF FACILITY

Each Party shall be responsible for the security of all governmental facilities where provided CMI is kept and shall assure that for each such facility qualified government officials are appointed who shall have the responsibility and authority for the control and protection of the CMI.

ARTICLE 11
STORAGE

The Parties shall store provided CMI in a manner that ensures access only by those individuals who have been authorized access pursuant to Articles 7 and 16.

ARTICLE 12
SECURITY REQUIREMENTS DURING TRANSMISSION OF CMI

The minimum requirements for the security of CMI during transmission shall be as follows:

(a) Classified documents and media

(i) Documents and media containing CMI shall be transmitted in double, sealed envelopes with the innermost envelope bearing only the security classification of the documents or media and the organizational address of the intended receiving Competent Authority and the outer envelope bearing the organizational address of the receiving Competent Authority, the organizational address of the originating Competent Authority, and the registry number, if applicable.

(ii) No indication of the security classification of the enclosed documents or media shall be made on the outer envelope. The sealed envelope shall then be transmitted according to the prescribed regulations and procedures of the Originating Party.

(iii) Receipts shall be prepared for packages containing classified documents or media that are transmitted between the Parties and a receipt for the enclosed documents or media shall be signed by the final receiving Competent Authority and returned to the originating Competent Authority.

(b) Classified equipment

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

(ii) Classified equipment that must be stored temporarily awaiting shipment shall be placed in a storage area that provides protection commensurate with the level of security classification of the equipment. Only authorized personnel shall have access to the storage area.

(iii) Receipts shall be obtained on every occasion when classified equipment changes hands en route.

(iv) Receipts shall be signed by the final receiving Competent Authority and returned to the originating Competent Authority.

(c) Electronic transmissions

CMI transmitted by electronic means shall be protected during transmission using encryption appropriate for the level of security classification of the CMI. Information systems processing, storing, or conveying CMI shall receive security accreditation by the appropriate authority of the Party employing the system.

ARTICLE 13
DESTRUCTION

1. The Parties shall destroy classified documents and media by burning, shredding, pulping, or other means preventing reconstruction in whole or in part of provided CMI.

2. The Parties shall destroy classified equipment beyond recognition or modify it so as to preclude reconstruction in whole or in part of provided CMI.

ARTICLE 14
REPRODUCTION

When the Parties reproduce classified documents or media, they shall also reproduce all original security markings thereon. The Parties shall place such reproduced classified documents or media under the same controls as the original classified documents or media. The Parties shall limit the number of copies to that required for official purposes.

ARTICLE 15
TRANSLATION

The Parties shall ensure that all translations of provided CMI are done by individuals with Personnel Security Clearances pursuant to Articles 7 and 16. The Parties shall keep the number of copies to a minimum and control the distribution. Such translations shall bear an appropriate security classification and a suitable notation in the language into which it is translated indicating that the document or media contains CMI of the Originating Party.

ARTICLE 16
RELEASE OF CMI TO CONTRACTORS

Prior to the release to a contractor (including a subcontractor, whenever the term is used herein) of any CMI received from the Originating Party, the Receiving Party shall take appropriate measures, subject to its national laws and regulations in force, to ensure that:

(a) no individual is entitled to access to the CMI solely by virtue of rank, appointment, or a Personnel Security Clearance;

(b) the contractor and the contractor's facilities have the capability to protect the CMI;

(c) all individuals whose official duties require access to the CMI have Personnel Security Clearances;

(d) a Personnel Security Clearance is determined in the same manner as provided for in Article 7;

(e) appropriate procedures are implemented to provide assurance that the criteria referred to in paragraph 3 of Article 7 have been met with respect to any individual granted access to the CMI;

(f) all individuals having access to the CMI are informed of their responsibilities to protect it;

(g) initial and periodic security inspections are carried out by the Receiving Party at each contractor facility where the CMI is stored or accessed to ensure that it is protected as required in this Agreement;

(h) access to the CMI is limited to those persons whose official duties require such access;

(i) a registry of individuals who have Personnel Security Clearances and are authorized to have access to the CMI is maintained at each facility;

(j) qualified individuals are appointed who shall have the responsibility and authority for the control and protection of the CMI;

(k) the CMI is stored in the same manner as provided for in Article 11;

(l) the CMI is transmitted in the same manner as provided for in Articles 9 and 12;

(m) classified documents and media and classified equipment are destroyed in the same manner as provided for in Article 13;

(n) classified documents and media are reproduced and placed under control in the same manner as provided for in Article 14; and

(o) translation of the CMI is done and copies are treated in the same manner as provided for in Article 15.

ARTICLE 17
LOSS AND COMPROMISE

The Originating Party shall be informed immediately of all losses or compromises as well as possible losses or compromises of its CMI and the Receiving Party shall initiate an investigation to determine the circumstances. The results of the investigation and information regarding measures taken to prevent recurrence shall be forwarded to the Originating Party by the Receiving Party.

ARTICLE 18
VISITS BY SECURITY REPRESENTATIVES

Implementation of the foregoing security requirements can be advanced through reciprocal visits by security representatives of the Parties. Accordingly, security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss security procedures and observe their implementation in the interest of achieving reasonable comparability of their respective security systems on mutually agreed venues and in a mutually satisfactory manner. Each Party shall assist the security representatives in determining whether CMI provided by the other Party is being adequately protected.

ARTICLE 19
COSTS

Each Party shall bear its own costs incurred in implementing this Agreement, subject to its national laws and regulations in force and within the limit of the budgetary appropriations of the Party.

ARTICLE 20
DISPUTE SETTLEMENT

1. Any disputes concerning the interpretation or application of this Agreement shall be settled only by consultation between the Parties.

2. During the settlement of disputes under paragraph 1, the Parties shall continue to protect provided CMI pursuant to this Agreement.

ARTICLE 21
ENTRY INTO FORCE, AMENDMENT, DURATION AND TERMINATION

1. This Agreement shall enter into force on the latter of the dates of the written notifications through the diplomatic channel by which the Parties confirm that their respective legal requirements for its entry into force have been fulfilled.

2. This Agreement may be amended at any time by mutual written consent of the Parties.

3. This Agreement shall remain in force for a period of one year and shall be automatically extended annually thereafter unless either Party notifies the other in writing through the diplomatic channel ninety days in advance of its intention to terminate the Agreement.

4. Notwithstanding the termination of this Agreement, all CMI provided pursuant to this Agreement shall continue to be protected in accordance with the provisions of this Agreement.

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

DONE at Seoul on 23 November, 2016, in duplicate, in the English language.

FOR THE GOVERNMENT OF JAPAN

FOR THE GOVERNMENT OF THE REPUBLIC OF KOREA