DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
CANBERRA

AGREEMENT

BETWEEN

THE GOVERNMENT OF AUSTRALIA

AND

THE GOVERNMENT OF THE REPUBLIC OF KOREA

ON THE PROTECTION OF

CLASSIFIED MILITARY INFORMATION

(Singapore, 31 May 2009)

Not yet in force
[2009] ATNIF 12

The Government of Australia and the Government of the Republic of Korea (hereinafter referred to as "the Parties"),

DESIRING to cooperate in the field of defence on the basis of mutual respect for sovereignty, independence and non-interference in each other's internal affairs, and

WISHING to ensure the reciprocal protection of Classified Military Information exchanged between the Parties under this Agreement,

HAVE AGREED AS FOLLOWS:

ARTICLE 1
PURPOSE

The Parties shall ensure the protection of Classified Military Information transmitted or exchanged between the Parties in the field of defence cooperation. Each Party shall implement its obligations under this Agreement subject to its national laws, regulations and policies.

ARTICLE 2
DEFINITIONS

2.1 For the purposes of this Agreement:

2.1.1 "Classification" means identifying, categorising and assigning a national security classification to information the disclosure of which could have adverse consequences for the Originating Party. The national security classification level assigned to information indicates the minimum level of protection that information must be afforded to safeguard it from loss or compromise.

2.1.2 "Classified Contract" means any contract or subcontract between the Parties or with or between Contractors, which contains, or the performance of which requires access to Classified Military Information of either Party.

2.1.3 "Classified Military Information" means all information and Material of defence interest (including documents, material, equipment, substances, and other items in any form or reproduction or translation of such information or material) which requires protection in the interests of national security and which is assigned a nominated level of national security Classification.

2.1.4 "Contractor" means an individual, organisation or other entity, with the legal capacity to conclude contracts, including a sub-contractor that has entered into a Classified Contract with either of the Parties or with another Contractor.

2.1.5 “Industrial Operations” means all commercial activities which develop, produce and/or manufacture Material and/or information, including Information and Communications Technology, for or on behalf of the defence organisations of either Party.

2.1.6 “Information and Communications Technology" means any communication device or application, including those relating to radio, television, cellular phones, computer and network hardware and software, and satellite systems, as well as the various services and applications associated with them, including video conferencing and distance learning.

2.1. 7 "Material" means anything (whether visible or not) in which information is recorded, embodied, encoded or stored and anything from which information can be derived, regardless of its physical form or composition including, but not limited to, documents, written records, equipment, instruments, machinery, devices, models, sound records, reproductions, representations, maps, computer programs, compilations and electronic data storage.

2.1.8 "Originating Party" means the Party which transmits Classified Military Information to the other Party, and assigns it a national security Classification.

2.1.9 "Personnel Security Clearance" means a certification provided by a National Security Authority of either Party concerning the level of Classified Military Information which a national of the country of that Party is authorised to access.

2.1.10 "Receiving Party" means the Party to which Classified Military Information is transmitted.

2.1.11 “Security Personnel” means personnel of a Party who are appointed by the National Security Authority of that Party to perform the functions of Security Personnel under this Agreement.

2.1.12 "Third Party" means any person or entity other than the Parties (including any Contractor, third country government, and any national or legal entity of a third country) whether or not it is owned, controlled or influenced by a Party.

2.1.13 "Transmitted Classified Military Information" means Classified Military Information which is transferred between the Parties, regardless of whether it is transmitted orally, visually, electronically, in writing, through the handing over of Material or in any other form or manner.

ARTICLE 3
NATIONAL SECURITY AUTHORITY

3.1 Each Party shall nominate its National Security Authority which shall be responsible for the implementation of this Agreement.

3.2 Unless otherwise advised by a Party in writing, the National Security Authorities for the Parties shall be:

3.2.1 For the Government of the Republic of Korea:

Director, Intelligence Force Development and Security
Korean Defense Intelligence Agency
Ministry of National Defense
22, Itaewon-Ro, Yongsan-Gu, Seoul
Republic of Korea

3.2.2 For the Government of Australia:

Head, Defence Security Authority
Department of Defence
Campbell Park Offices
Canberra ACT 2600
AUSTRALIA

3.3 The Parties may, at any time, make changes to their National Security Authority and shall promptly advise the other Party of such change in writing. Such changes shall not require amendment of this Agreement.

ARTICLE 4
MARKING CLASSIFIED MILITARY INFORMATION

4.1 The Originating Party shall assign and mark all Classified Military Information that can be physically marked with one of the national security Classifications specified in paragraph 5 of this Article before transmission.

4.2 The Receiving Party shall ensure that Transmitted Classified Military Information, and anything incorporating Classified Military Information, received from the Originating Party is assigned and marked if physically possible with a national security Classification no lower than the corresponding Classification specified by the Originating Party.

4.3 Any Material produced by one Party that contains the Transmitted Classified Military Information of the other Party shall be marked KOREA/AUSTRALIA or AUSTRALIA/KOREA followed by the appropriate national security Classification.

4.4 For Classified Military Information where a marking is not physically possible, the Originating Party shall inform the Receiving Party in writing of the national security Classification.

4.5 The corresponding national security Classifications of the Parties are as follows:

In Korea:		In Australia:
군사 Ⅱ급 비밀	to be protected as	SECRET
군사 Ⅲ급 비밀	to be protected as	CONFIDENTIAL
군사대외비	to be protected as	RESTRICTED

ARTICLE 5
PROTECTION AND USE OF CLASSIFIED MILITARY INFORMATION

5.1 The Parties shall apply the following rules for the protection and use of Transmitted Classified Military Information:

5.1.1 the Originating Party may specify in writing any limitations not included in Article 6 (Access to Classified Military Information) on the use, disclosure, release and access to Transmitted Classified Military Information by the Receiving Party and the Receiving Party shall comply with any such limitations on the use, disclosure, release and access to Transmitted Classified Military Information which has been specified by the Originating Party;

5.1.2 the Receiving Party shall not downgrade the national security Classification of the Transmitted Classified Military Information without the prior written consent of the Originating Party;

5.1.3 the Originating Party shall inform the Receiving Party in writing of any change in the national security Classification of Transmitted Classified Military Information;

5.1.4 the Receiving Party shall accord all Transmitted Classified Military Information a standard of physical and legal protection not less than that which it accords its own information of a corresponding national security Classification;

5.1.5 unless otherwise mutually determined by the Parties in writing, the Receiving Party shall not disclose, release or provide access to Transmitted Classified Military Information to any Third Party without the prior written consent of the Originating Party;

5.1.6 the Receiving Party shall take all appropriate steps legally available to it to keep Transmitted Classified Military Information free from unauthorised disclosure; and

5.1.7 the Receiving Party shall not permit Transmitted Classified Military Information to be used for any purpose other than that for which it is provided without the prior written consent of the Originating Party.

5.2 When Transmitted Classified Military Information is no longer required for the purpose for which it was provided, the Receiving Party shall:

5.2.1 return the Classified Military Information to the Originating Party; or

5.2.2 destroy the Classified Military Information in accordance with the procedures of the Receiving Party for the destruction of such information and confirm in writing to the Originating Party the destruction of the Classified Military Information.

5.3 The Parties may mutually determine in writing such additional requirements for security protection as they consider appropriate for the purpose of facilitating the transmission and protection of Transmitted Classified Military Information.

ARTICLE 6
ACCESS TO CLASSIFIED MILITARY INFORMATION

6.1 Access to Transmitted Classified Military Information shall be limited, subject to the provisions of this Agreement, to those personnel of a Party who:

6.1.1 are nationals of the country of either Party, unless the Originating Party has given its prior written consent otherwise;

6.1.2 require access to Classified Military Information for the performance of their official duties; and

6.1.3 have been given a Personnel Security Clearance to the appropriate level in accordance with the Receiving Party's laws, regulations and policies.

6.2 The Parties acknowledge the special status of elected parliamentary representatives and shall continue to apply their current practices governing access to Classified Military Information to them on a need-to-know basis.

ARTICLE 7
TRANSMISSION, PROCESSING AND STORAGE OF CLASSIFIED MILITARY INFORMATION

7.1 Classified Military Information shall be transmitted in accordance with the national laws, regulations and procedures of the Originating Party and the provisions in this Agreement.

7.2 Classified Military Information shall be transmitted through diplomatic channels. If, in the opinion of the Originating Party, the use of diplomatic channels would be impractical or unduly delay receipt of Classified Military Information, transmissions may be undertaken by authorised personnel who possess the requisite Personnel Security Clearance and are furnished with a courier certificate issued by the

Originating Party, or through other channels mutually determined by the National Security Authorities.

7.3 All Information and Communications Technology networks, systems and infrastructure used to process, transmit and/or store Classified Military Information in an electronic format shall be protected in accordance with methods and standards mutually recognised and settled upon by the National Security Authorities of the Parties.

7.4 The Receiving Party shall acknowledge receipt of Classified Military Information in writing.

7.5 The Originating Party reserves the right to refuse to transmit any of its Classified Military Information.

ARTICLE 8
CLASSIFIED CONTRACTS

8.1 Classified Contracts shall be concluded and implemented in accordance with this Agreement and the relevant laws, regulations and policies of the Party in whose territory the Classified Contract is made.

8.2 The National Security Authorities of the Parties shall be responsible for the administration of the security aspects of Classified Military Information of Classified Contracts.

8.3 The National Security Authorities may mutually determine arrangements to effect this Article between the Parties and Contractors.

ARTICLE 9
PROTECTION OF INTELLECTUAL PROPERTY AND OTHER RIGHTS

Nothing in this Agreement diminishes or limits any existing or acquired intellectual property rights associated with Classified Military Information to which either Party or any Third Party may be entitled.

ARTICLE 10
EXCHANGE OF SECURITY STANDARDS

Each Party shall provide to the other, upon request, information regarding its national security standards, procedures and practices for the protection of Classified Military Information, including those national security standards, practices and procedures which relate to its Industrial Operations. Each Party shall inform the other Party in writing of any changes to its national security standards, procedures and practices that affect the manner in which Transmitted Classified Military Information is protected.

ARTICLE 11
VISITS – GENERAL PRINCIPLES

11.1 Visits by personnel of a Party requiring access to Classified Military Information held by the other Party or requiring access to restricted areas or facilities where Classified Military Information is held shall be undertaken only with the prior written approval of the host Party. Approval for such visits shall be granted only to personnel specified in Article 6.

11.2 Requests for such visits shall be submitted in writing by the National Security Authority of the visiting Party, through diplomatic channels to the National Security Authority of the host Party. Unless otherwise mutually determined, such requests shall be made at least three (3) weeks prior to the date of the requested visit.

11.3 Such requests shall contain the following information:

11.3.1 the purpose of the proposed visit;

11.3.2 the proposed date and duration of the visit;

11.3.3 the names of the organisations or facilities to be visited;

11.3.4 the identification and telephone number of a Government official of the visiting Party who can provide additional information concerning the visit;

11.3.5 the identification and telephone number of a contact at the organisations or facilities to be visited;

11.3.6 the following personal details of the personnel who shall undertake the visit:

11.3.6.1 full name;

11.3.6.2 date and place of birth;

11.3.6.3 citizenship and passport number;

11.3.6.4 the official titles of the visiting personnel and the names of the organisations he/she represents; and

11.3.6.5 the Personnel Security Clearance held, the date of its issue and the period of its validity.

11.4 Nothing in paragraph 11.2 of this Article shall restrict the right of either Party to permit visiting personnel of the other Party to have access to Classified Military Information or entry to controlled areas or any other establishments at any time during an approved visit should the host Party wish to grant such access or entry.

ARTICLE 12
VISITS BY SECURITY PERSONNEL

12.1 Each Party shall permit Security Personnel of the other Party to visit organisations, facilities and controlled areas within the territory of the host Party

where Classified Military Information is stored, when mutually convenient and in accordance with the procedures set out in Article 11:

12.1.1 to obtain access to Transmitted Classified Military Information; or

12.1.2 to confer with the National Security Authority of the host Party regarding its national security standards, procedures and practices applied for the protection of Classified Military Information.

12.2 Each Party shall assist the Security Personnel of the visiting Party in the exercise of their functions under paragraph 1 of this Article.

ARTICLE 13
COMPLIANCE AND SECURITY INSPECTIONS

13.1 Each Party shall ensure that facilities, establishments and other organisations that handle or store Transmitted Classified Military Information protect such information in accordance with the provisions of this Agreement.

13.2 Each Party shall ensure that within its territory necessary security inspections are carried out, and appropriate security regulations and procedures shall be complied with in order to protect Transmitted Classified Military Information.

ARTICLE 14
LOSS OR COMPROMISE OF CLASSIFIED MILITARY INFORMATION

14.1 Should Classified Military Information provided by the Originating Party be lost or compromised while in the possession of the Receiving Party, the Receiving Party shall immediately inform the Originating Party. The Receiving Party shall also immediately inform the Originating Party of any suspected loss or compromise of Transmitted Classified Military Information. The Receiving Party shall immediately investigate the circumstances of such loss or compromise, or suspected loss or compromise, and shall promptly inform the Originating Party of the findings of the investigation and corrective action taken or to be taken.

14.2 The Receiving Party, if necessary, may request the Originating Party to send personnel to provide assistance in connection with specific investigations to assess the damage caused by the loss or compromise. Such requests shall be considered favourably.

14.3 Any security incident relating to Transmitted Classified Military Information shall be dealt with in accordance with the policies and laws of the Party in whose territory the security incident occurred which are in force at the time of the security incident.

ARTICLE 15
COSTS

Each Party shall be responsible for its own costs incurred in implementing this Agreement.

ARTICLE 16
SETTLEMENT OF DISPUTES

Disputes arising from the interpretation or application of this Agreement shall be settled by consultation and negotiation between the Parties and shall not be referred to any third party.

ARTICLE 17
ENTRY INTO FORCE, REVIEW, AMENDMENT, DURATION AND TERMINATION

17.1 This Agreement shall enter into force when the Parties have notified each other in writing that their respective requirements for entry into force have been satisfied. The date of entry into force of the Agreement shall be the date of the last notification.

17.2 This Agreement may be terminated at any time by mutual consent in writing or by either Party giving the other written notice of its intention to terminate, which shall take effect six (6) months after notification.

17.3 This Agreement may be reviewed at the request of either Party and amended by mutual written consent of the Parties. Such amendments shall enter into force when the Parties have notified each other in writing that their respective domestic requirements for the entry into force of the amendment have been satisfied.

17.4 The existing responsibilities and obligations related to the protection and use of Transmitted Classified Military Information and the understanding stated in Article 16 shall continue to apply notwithstanding the termination of this Agreement.

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

Done in duplicate in Singapore on 31 May 2009
in the Korean and English languages, both texts being equally authentic.

For the Government of Australia	For the Government of the Republic of Korea
The Hon. Joel Fitzgibbon	Mr Lee Sang Hee
Minister for Defence	Minister of National Defense

호주 정부와 대한민국 정부 간의
군사비밀정보의 보호에 대한 협정

호주 정부와 대한민국 정부(이하 “ 당사자들” 이라 한다)는

다른 국가의 주권, 독립 및 내정 불간섭 원칙에 따라 국방 분야에서 협력하길 원하며

이 협정에 따라 당사자 간에 교환되는 군사비밀정보의 상호 보호를 보장하기를 희망하며

다음과 같이 합의하였다.

제 1 조

협정의 목적

당사자들은 국방 협력분야에서 당사자들 간에 상호 전송되거나 교환된 군사비밀정보의 보호를 보장한다. 각 당사자는 이 협정에 따라 각 당사자의 의무를 자국의 국내법, 규칙 및 정책에 따라 이행한다.

제 2 조

용어의 정의

2.1 이 협정의 목적상:

2.1.1 “ 비밀분류”란 공개될 경우에 제공 당사자에게 불이익을 초래할 수 있는 정보를 식별, 분류하고 국가보안등급을 지정하는 것을 의미한다. 정보에 부여하는 국가보안등급은 해당 정보가 분실 또는 손상을 입지 않도록 보호하는 데 필요한 최소한의 보호수준을 의미한다.

2.1.2 “ 비밀계약” 이란 당사자 간, 당사자와 계약자 간 또는 계약자 간에 체결한 계약 또는 하도급 계약으로, 어느 한쪽 당사자의 군사비밀정보를 포함하거나 그 계약의 이행이 군사비밀정보에의 접근을 필요로 하는 계약을 의미한다.

2.1.3 “ 군사비밀정보” 란 국가안보를 위해 보호하여야 하며 국가보안등급을 부여받은 국방과 관련된 모든 정보 및 자료(서류, 자료, 장비, 물품, 그 외의 모든 형태의 품목 또는 이러한 정보와 자료의 복제본이나 번역본을 포함한다)를 의미한다.

2.1.4 “ 계약자” 란 계약을 체결할 수 있는 법적 권한을 보유한 개인, 기관 또는 그 외의 주체를 의미하며, 당사자 중 어느 한쪽 또는 다른 계약자와 비밀계약을 체결한 하도급 계약자를 포함한다.

2.1.5 “ 산업적 운용” 이란 각 당사자의 국방당국을 위해 또는 대신하여 자료 및/또는 정보통신기술을 포함한 정보를 개발, 생산 및/또는 제조하는 모든 상업행위를 의미한다.

2.1.6 “ 정보통신기술” 이란 라디오, 텔레비전, 휴대폰, 컴퓨터, 하드웨어 및 소프트웨어 네트워크, 위성장치와 관련된 모든 통신장치 및 응용체계를 의미하며, 이들과 제휴된 다양한 서비스와 응용체계 및 화상회의와 원격교육을 포함한다.

2.1.7 “ 자료”란 물리적 형태나 구성을 불문하고 가시성과 무관하게 서류, 기록, 장비, 기구, 기계, 장치, 모형, 녹음, 복제, 표현물, 지도, 컴퓨터 프로그램, 편집물, 편집물 및 전자정보기억장치 등을 포함하지만 이에 한정되지 않고, 정보를 기록 · 구체화 또는 저장하고 도출할 수 있는 모든 것을 의미한다.

2.1.8 “ 제공 당사자”란 군사비밀정보를 다른 당사자에게 전송하고 국가보안등급을 부여하는 자를 의미한다.

2.1.9 “ 보안허가”란 양 당사자의 국가보안당국이 그 국가의 국민이 접근하도록 허가된 군사비밀정보의 등급에 대해 발급하는 인가를 의미한다.

2.1.10 “ 접수 당사자”란 군사비밀정보가 전송되는 당사자를 의미한다.

2.1.11 “ 보안직원”이란 국가보안당국으로부터 이 협정에 따라 보안직원으로서의 기능을 수행하도록 임명된 당사자의 직원을 의미한다.

2.1.12 “ 제 3 자”란 어느 한 당사자가 소유하거나 통제하거나 영향력을 행사하는지의 여부와 무관하게 계약자, 제 3 국 정부 및 제 3 국의 모든 국가 또는 법적 실체를 포함하여 당사자를 제외한 그 어떤 개인이나 주체를 의미한다.

2.1.13 “ 제공된 군사비밀정보” 란 구두, 영상, 전자, 서면, 자료를 통한 양도 및 그 밖의 그 어떤 형태나 방식으로든 당사자 간에 전송된 군사비밀정보를 의미한다.

제 3 조

국가보안당국

3.1 각 당사자는 이 협정의 이행을 책임지는 국가보안당국을 지정한다.

3.2 별도로 서면으로 통지하지 않는 한, 각 당사자의 국가보안당국은 다음과 같다.

3.2.1 대한민국 정부측: 국방부 정보본부 전력발전보안부장

대한민국 서울 용산구 이태원로 22 가

3.2.2 호주 정부측: 국방부 국방안보본부장

캠벨파크 오피스, 캔버라 ACT 2600 호주

3.3 당사자들은 언제든지 국가보안당국을 변경할 수 있고 다른 쪽 당사자에게 신속히 서면으로 변경사항을 통보해야 한다. 그런 변경은 이 협정의 개정을 요구하지 않는다.

제 4 조

군사비밀정보의 표시

4.1 제공 당사자는 물리적으로 표시가 가능한 모든 군사비밀정보를 제공하기 전에 이 조 제 5 항에 명시된 국가보안등급 중 하나를 부여하고 표시한다.

4.2 접수 당사자는 제공 당사자로부터 접수한 군사비밀정보 및 군사비밀정보를 포함한 모든 것에 대해 제공 당사자가 표시한 국가보안등급보다 낮지 않은 비밀등급이 부여되고 물리적으로 가능할 경우 표시되도록 보장한다.

4.3 다른 쪽 당사자로부터 접수된 군사비밀정보가 포함된 자료를 생산한 어느 한쪽 당사자의 자료는 Korea/Australia 또는 Australia/Korea 로 표기되며 적절한 국가보안등급이 뒤에 명기된다.

4.4 제공 당사자는 국가보안등급을 물리적으로 표시하기 어려운 군사비밀정보에 대해서는 국가보안등급을 접수 당사자에게 서면으로 알려준다.

4.5 당사자의 상응하는 국가보안등급은 다음과 같다.

한국	호주
군사 2 급 비밀	SECRET
군사 3 급 비밀	CONFIDENTIAL
군사 대외비	RESTRICTED

제 5 조

군사비밀정보의 보호와 이용

5.1 당사자는 상호 제공된 군사비밀정보의 보호와 이용을 위하여 다음 원칙을 적용한다:

5.1.1 제공 당사자는 군사비밀정보의 사용, 공개, 유출 및 접근에 대해 군사비밀정보의 접근을 다루는 제 6 조에 포함되지 않은 제한을

서면으로 규정할 수 있으며, 접수 당사자는 제공 당사자가 규정한 군사비밀정보의 사용, 공개, 유출 및 접근에 대한 제한을 준수해야 한다.

5.1.2 접수 당사자는 제공 당사자의 사전 서면 동의 없이는 제공된 군사비밀정보의 비밀등급을 하향 조정하여서는 안 된다.

5.1.3 제공 당사자는 제공된 군사비밀정보의 국가보안등급을 변경할 경우 그 변경내용을 접수 당사자에게 서면으로 통지한다.

5.1.4 접수 당사자는 제공된 군사비밀정보에 대하여 자국의 상응하는 국가보안등급에 해당되는 군사비밀정보에 적용되는 기준보다 낮지 않은 물리적 및 법적 보호기준을 적용한다.

5.1.5 사전에 당사자간 서면으로 합의하지 않은 한, 접수 당사자는 제공 당사자의 사전 서면 허락이 없이 그 어떤 제 3 자에게도 군사비밀정보를 공개, 유출 또는 제공해서는 안 된다.

5.1.6 접수 당사자는 제공된 군사비밀정보를 허가되지 않은 공개로부터 보호하기 위해 법적으로 허용되는 모든 적절한 조치를 취해야 한다.

5.1.7 접수 당사자는 제공 당사자의 사전 서면 허락이 없는 한, 제공된 군사비밀정보가 애초에 제공된 목적 외의 용도로 사용되는 것을 허락해서는 안 된다.

5.2 제공된 군사비밀정보가 애초에 제공된 목적에 비추어 더 이상 필요하지 않을 경우 접수 당사자는 다음과 같은 조치를 취한다:

5.2.1 군사비밀정보를 제공 당사자에게 반환한다. 또는

5.2.2 군사비밀정보를 접수 당사자의 그런 정보를 파기하는 절차에 합치하도록 파기하며, 군사비밀정보를 파기한 사실을 제공 당사자에게 서면으로 확인한다.

5.3 당사자들은 제공된 군사비밀정보의 전송 및 보호를 원활하게 하는 목적하에 적절하다고 생각된다면 보안 보호를 위한 추가적인 요건을 서면으로 상호 결정할 수 있다.

제 6 조

군사비밀정보에의 접근

6.1 제공된 군사비밀정보에 대한 접근은 이 협정의 규정에 따라 양 당사자의 다음에 모두 해당되는 자로 제한된다:

6.1.1 제공 당사자가 사전에 다르게 서면 동의하지 않는 한, 각 당사자의 국민

6.1.2 공무수행을 위하여 군사비밀정보에 접근해야 하는 자, 및

6.1.3 접수 당사자의 법, 규칙과 정책에 따른 적절한 수준의 보안허가를 받은 자

6.2 당사자들은 선출된 의회의 대표들의 특수한 지위를 인정하고, 알 필요가 있는 경우 그들의 군사비밀정보의 접근에 대한 현재 관행을 지속적으로 적용한다.

제 7 조

군사비밀정보의 전송, 처리 및 저장

7.1 군사비밀정보의 전송은 제공 당사자의 국내법, 규칙 및 절차와 이 협정의 조항에 근거하여 이루어져야 한다.

7.2 군사비밀정보는 외교채널을 통하여 전송되어야 한다. 만일 제공 당사자가 외교채널을 통한 군사비밀정보 전송이 비실용적이고 군사비밀정보의 수령을 과도하게 지연한다고 판단할 경우, 필요한 보안허가를 보유하고 제공 당사자가 발행한 전령인증서를 소지한 자를 통하거나 국가보안당국이 상호 합의한 여타 다른 채널을 통해 군사비밀정보를 전송할 수 있다.

7.3 전자적 형태의 군사비밀정보를 처리, 전송 및/또는 저장할 때 사용하는 모든 정보통신기술네트워크, 시스템 및 기반체계는 양 국가보안당국이 상호 인정하고 결정한 방법과 기준에 의해 보호되어야 한다.

7.4 접수 당사자는 군사비밀정보의 수령을 서면으로 알린다.

7.5 제공 당사자는 군사비밀정보의 전송을 거부할 수 있는 권한을 가진다.

제 8 조

비밀계약

8.1 비밀계약은 이 협정과 비밀계약이 체결되는 당사자의 관련 법, 규칙 및 정책에 따라 체결되고 이행되어야 한다.

8.2 당사자들의 국가보안당국은 비밀계약에 포함된 군사비밀정보의 보안 문제에 대한 관리에 대해 책임을 진다.

8.3 국가보안당국은 당사자와 계약자 간 이 조항을 적용하기 위해 상호 약정을 할 수 있다.

제 9 조

지적재산권 보호

이 협정의 어떠한 조항도 당사자 또는 제 3 자에게 소유권이 있는 군사비밀정보와 관련된 지적재산권을 축소하거나 제한하지 않는다.

제 10 조

보안기준의 공유

각 당사자는 다른 당사자에게 그의 요청에 따라 산업적 운용과 관련된 군사비밀정보 보호를 위한 자국의 보안기준, 절차 및 군사비밀정보의 보호 관련 관행에 대한 정보를 제공한다. 각 당사자는 전송된 군사비밀정보가 보호되는 방식에 영향을 미치는 자국의 국가보안기준, 절차 및 관행에 대한 변경사항을 서면으로 통보한다.

제 11 조

방문– 일반원칙

11.1 다른 쪽 당사자가 보유한 군사비밀정보에의 접근을 요하는 어느 한쪽 당사자의 인사의 방문 또는 군사비밀정보가 저장되는 제한 구역 또는 시설에의 접근을 요하는 경우 접수 당사자의 사전 서면 승인 하에 이행되어야 한다. 이런 방문의 승인은 제 6 조에 규정된 인사에게만 수여될 수 있다.

11.2 이런 방문의 요청은 방문하는 당사자의 국가보안당국이 외교채널을 통해 방문자를 접수하는 당사자의 국가보안당국에게 서면으로 제출한다. 상호 다르게 합의하지 않는 한, 그러한 요청은 최소한 방문 예정 날짜보다 3 주 전에 해야 한다.

11.3 방문 신청서에는 다음 사항이 포함되어야 한다:

11.3.1 제안한 방문의 목적

11.3.2 제안한 방문의 날짜와 기간

11.3.3 방문하려는 기관 또는 시설의 이름

11.3.4 방문에 대해 추가 정보를 줄 수 있는 방문 당사자의 정부 공무원의 개인정보 및 연락처

11.3.5 방문하고자 하는 조직 또는 시설 담당자의 개인정보 및 전화번호

11.3.6 방문예정자의 다음과 같은 상세 신상정보

11.3.6.1 성명

11.3.6.2 생년월일 및 출생지

11.3.6.3 국적 및 여권번호

11.3.6.4 방문자의 공식직함 및 그들의 대표하는 기관명

11.3.6.5 보안허가 발급일 및 유효기간

11.4 방문자를 접수하는 당사자가 허가된 방문기간 중 그러한 접근 또는 출입을 허가하려고 할 경우, 이 조 제 2 항의 어떠한 내용도 다른 당사자의 인사가 군사비밀정보에 대한 접근을 갖거나 접근제한구역 또는 그 어떤 다른 시설에 들어가는 것을 허락하는 양 당사자의 권리를 제한하지 않는다.

제 12 조

보안요원의 방문

12.1 각 당사자는 상호 편리하고 제 11 조에 규정된 절차에 따라 접수 당사자의 영토내에 있으며 군사비밀정보가 저장된 기관, 시설 및 통제된 구역에 다른 당사자의 보안요원의 방문을 아래의 경우 허용한다.

12.1.1 제공된 군사비밀정보에의 접근을 얻기 위해 또는

12.1.2 군사비밀정보의 보호에 적용되는 보안기준, 절차 및 관행에 관해 접수 당사자의 국가보안당국과의 협의를 위해

12.2 각 당사자는 방문 당사자의 보안요원으로 하여금 이 조 제 1 항에 명시된 임무를 수행할 수 있도록 지원한다.

제 13 조

보안규정 준수 및 보안점검

13.1 각 당사자는 제공된 군사비밀정보를 취급하거나 보관하는 자국 내 시설, 조직 및 그 밖의 기관이 이 협정에 따라 군사비밀정보를 보호하도록 보장한다.

13.2 각 당사자는 제공된 군사비밀정보를 보호하기 위하여, 자국 내에서 필요한 보안점검이 실시되고 적절한 보안규정과 절차가 준수되도록 보장한다.

제 14 조

군사비밀정보의 분실 또는 손상

14.1 제공 당사자가 제공한 군사비밀정보가 접수 당사자가 소유하는 동안 분실되거나 손상된 경우 접수 당사자는 바로 제공 당사자에게 그 사실을 알린다. 접수 당사자는 제공 당사자에게 분실이나 손상이 의심될 경우 그

사실도 즉시 통보한다. 접수 당사자는 그런 분실과 손상 또는 의심되는 분실과 손상의 상황에 대한 조사를 즉시 개시하며, 그 조사의 결과 및 이미 취해진 또는 향후 취해질 시정조치에 대해 바로 제공 당사자에게 알린다.

14.2 접수 당사자는 필요 시 제공당사자에게 분실 또는 손상으로 발생한 손해 평가를 위한 구체적인 조사를 위해 필요한 인력의 지원을 제공토록 요청할 수 있다. 그런 요청은 호의적으로 고려되어야 한다.

14.3 제공된 군사비밀정보에 관한 그 어떤 보안사고 시 사건이 발생한 당사자 국가의 당시 효력 있는 군사비밀정보 보안규정 위반에 관한 법률이나 정책에 따라 처리한다.

제 15 조

비 용

각 당사자는 이 협정의 이행 시 발생하는 비용을 각자 부담한다.

제 16 조

분쟁의 해결

이 협정의 해석 또는 적용과 관련하여 분쟁이 발생하는 때에는 당사자 간의 협의와 협상에 의하여 해결되어야 하며 제 3 자에게 의뢰하지 않는다.

제 17 조

발효, 검토, 수정, 기간 및 종료

17.1 이 협정은 협정의 발효를 위해 필요한 각 당사국의 국내절차가 완료되었다는 양 당사국의 서면통지서가 교환된 날 발효된다. 이 협정의 발효일자는 마지막 통지의 날이다.

17.2 이 협정은 아무 때나 상호 합의하에 또는 어느 한쪽 당사자의 서면 통지를 통해 종료될 수 있으며 통지한 시점으로부터 6 개월이 경과한 후에 발효한다.

17.3 이 협정은 어느 한쪽의 요청에 따라 검토될 수 있으며, 당사자 간 서면 합의에 의하여 수정할 수 있다. 이 협정을 수정하는 경우, 양 당사자가 상호 서면으로 각자의 국내절차 요건이 충족되었음을 통지할 때 발효한다.

17.4 제공된 군사비밀정보의 보호와 사용에 대한 이미 존재하는 책임과 의무 및 제 16 조의 합의는 이 협정의 종료와 무관하게 계속 적용된다.

이상의 증거로 아래 서명자는 그들 각자의 정부로부터 정당하게 권한을 위임받아 이 협정에 서명하였다.

년 월 일 에서 동등하게 정본이 한국어, 영어로 2 부씩 작성되었다.

호주 정부를 대표하여 대한민국 정부를 대표하여