

DEFENSE

Cooperation

**Memorandum of Understanding
Between the
UNITED STATES OF AMERICA
and the REPUBLIC OF KOREA**

Signed at Washington and Seoul April 30, 2009



NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966
(80 Stat. 271; 1 U.S.C. 113)—

“ . . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof.”

REPUBLIC OF KOREA

Defense: Cooperation

*Memorandum of understanding signed
at Washington and Seoul April 30, 2009;
Entered into force April 30, 2009.*

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DEPARTMENT OF DEFENSE
OF THE UNITED STATES OF AMERICA
AND
THE MINISTRY OF NATIONAL DEFENSE
OF THE REPUBLIC OF KOREA
CONCERNING
COOPERATION ON
INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)
(Short Title: U.S. - ROK IA/CND MOU)

TABLE OF CONTENTS

PREAMBLE..... 1

ARTICLE I..... 2

DEFINITION OF TERMS 2

ARTICLE II 4

OBJECTIVE AND SCOPE..... 4

ARTICLE III..... 5

MANAGEMENT..... 5

ARTICLE IV..... 9

CHANNELS OF COMMUNICATION AND VISITS 9

ARTICLE V 10

FINANCIAL ARRANGEMENTS..... 10

ARTICLE VI..... 11

CONTRACTUAL ARRANGEMENTS 11

ARTICLE VII..... 12

DISCLOSURE AND USE OF IA/CND INFORMATION 12

ARTICLE VIII..... 14

CONTROLLED UNCLASSIFIED INFORMATION..... 14

ARTICLE IX..... 15

SECURITY 15

ARTICLE X 17

THIRD PARTY TRANSFERS 17

ARTICLE XI..... 18

SETTLEMENT OF DISPUTES..... 18

ARTICLE XII 19

GENERAL PROVISIONS..... 19

ARTICLE XIII..... 20

ENTRY INTO FORCE, AMENDMENT, TERMINATION, AND DURATION 20

SIGNATURE 21

PREAMBLE

The Department of Defense of the United States of America (U.S. DoD) and the Ministry of National Defense of the Republic of Korea (ROK MND), hereinafter referred to as the "Parties":

Recognizing that the Exchange of Notes regarding the General Security of Information Agreement Between The United States of America and Korea, which entered into effect May 1, 1962, as amended May 22, 1974, and September 24, 1987, applies to this MOU;

Having a common interest in defense;

Recognizing the benefits to be obtained from the mutual support in coordinating information assurance and computer network defense matters;

Desiring to improve their conventional defense capabilities through the exchange of Information Assurance/Computer Network Defense (IA/CND) Information and in the planning and execution of combined military operations; and

Recognizing the benefits to the Parties of cooperation in the mutual exchange of information related to cyber defense;

Have agreed as follows:

ARTICLE I

DEFINITION OF TERMS

1.1. The Parties have jointly decided upon the following definitions for terms used in this MOU:

Authorities	Government officials listed in this MOU who are authorized to act on behalf of the Parties in matters pertinent to the implementation of this MOU.
Classified Information	Official information that requires protection in the interests of national security and is so designated by the application of a security classification marking. This information may be in oral, visual, magnetic, or documentary form or in the form of equipment technology.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks. The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems, or their contents, or theft of information. CND protection activity employs IA protection activity. CND response includes alert or threat information, monitoring, analysis, detection activities, and trend and pattern analysis.
Contractor Support Personnel	Persons specifically identified as providing administrative, managerial, scientific, or technical support services to a Party under a support contract.
Controlled Unclassified Information	Unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations. It includes information that has been declassified but remains controlled.
Designated Security Authority	The security authority designated by national authorities to be responsible for the coordination and implementation of national industrial security aspects of this MOU.
Establishments	Government organizations listed in this MOU that provide, or have an interest in, the information to be exchanged through the Project Officers or Executive Agents.

Executive Agents	Government organizations listed in this MOU that are authorized to act on behalf of the Authorities and that have responsibility for implementation, management, and data or information exchange procedures pertinent to this MOU.
Information Assurance/Computer Network Defense Information (IA/CND Information)	Any IA or CND knowledge that can be communicated by any means, regardless of form or type including, but not limited to, scientific, technical, business, or financial knowledge whether or not subject to copyright, patents, or other legal protection.
Information Assurance (IA)	Confidentiality, integrity, availability, authentication, and non-repudiation of information systems or information being handled by the information systems including actions to protect and defend these systems.
Intellectual Property	In accordance with the World Trade Organization Agreement on Trade-related Aspects of Intellectual Property Rights of April 15, 1994, all copyright and related rights, all rights in relation to inventions (including patent rights), all rights in registered and unregistered trademarks (including service marks), registered and unregistered designs, undisclosed information (including trade secrets and know-how), layout designs of integrated circuits, and geographical indications, and any other rights resulting from creative activity in the industrial, scientific, literary, and artistic fields.
Party	A signatory to this MOU represented by its military or civilian personnel. Contractors and Contractor Support Personnel shall not be representatives of a Party under this MOU.
Project Officers	Representatives of Government organizations who are specifically authorized by Authorities to maintain policy oversight of IA and CND activities.
Response	All actions taken to handle incidents reported by or affecting members of the Parties.
Standard Operating Procedure (SOP)	Procedure to share IA/CND Information.
Third Party	A government or entity other than the Governments of the Parties and any person or other entity whose government is not the Government of a Party.

ARTICLE II

OBJECTIVE AND SCOPE

2.1. The objective of this MOU is to conduct information exchanges and related activities among the ROK MND, the U.S. DoD, the U.S. Pacific Command (USPACOM) and U.S. Forces Korea (USFK) in matters of IA and CND. The Parties shall conduct bilateral IA and CND activities and IA/CND Information sharing to contribute to both Parties' common goals of protecting information networks. Actions carried out within the scope of this MOU shall result in enhanced defensive capabilities to:

2.1.1. improve the confidentiality, integrity, and availability of the information and the information systems used to transmit and process information for decision-makers;

2.1.2. enhance the interoperability of U.S. and ROK forces;

2.1.3. improve cyber attack prediction, detection, and response capabilities;

2.1.4. improve interoperability, policy development, configuration management, and standardization of information and information systems to provide for more robust and reliable command and control systems;

2.2. The scope of this MOU shall include:

2.2.1. developing a Standard Operating Procedure (SOP);

2.2.2. identifying technical solutions or administrative documentation required for the continuous exchange of IA/CND Information;

2.2.3. exchanging information in the areas of incident response, investigation, and forensics; and

2.2.4. exchanging information to improve interoperability in the area of security technologies employed and configuration management to facilitate rapid exchanges of IA/CND-related information during periods of peace, crisis, and hostilities.

2.3. Exchanges of information under this MOU shall be on a reciprocal, balanced basis, such that the information provided or exchanged between the Parties, or through the designated Project Officers and Executive Agents, shall be of approximately equivalent value, quantitatively and qualitatively.

2.4. No defense equipment or services may be exchanged or provided under this MOU.

ARTICLE III
MANAGEMENT

3.1. The Parties hereby establish the following Authorities for this MOU, or their equivalents in the event of reorganization:

<u>United States:</u>	Assistant Secretary of Defense (ASD), Networks and Information Integration (NII)
<u>Republic of Korea:</u>	Deputy Minister, Planning and Coordination Office

3.2. The Authorities shall be responsible for:

3.2.1. reviewing, and recommending for approval to the Parties, amendments to this MOU in accordance with Article XIII (Entry into Force, Amendment, Termination, and Duration) of this MOU;

3.2.2. exercising executive-level oversight of efforts provided in this MOU;

3.2.3. resolving issues brought forth by the Project Officers;

3.2.4. designating Project Officer assignments and the list of Establishments; and

3.2.5. employing best efforts to resolve, in consultation with the export control authorities of the Parties, any export control issues raised by the Project Officers in accordance with subparagraph 3.4.8 or raised by a Party's Authority in accordance with paragraph 3.12. of this Article.

3.3. The following Project Officers for this MOU are responsible for the management of this MOU, and shall represent the Authorities.

<u>United States:</u>	Director, International Information Assurance Program, Office of the Assistant Secretary of Defense (OASD), Networks and Information Integration (NII)
<u>Republic of Korea:</u>	Director General, Information Planning Bureau

3.4. Project Officers for this MOU shall be responsible for:

3.4.1. exercising policy oversight of activities under this MOU;

3.4.2. resolving issues brought forth by Executive Agents;

3.4.3. referring to the Authorities issues that cannot be mutually resolved by the Project Officers;

3.4.4. recommending to the Authorities the amendment or termination of this MOU;

3.4.5. establishing and maintaining annual objectives for this MOU, as appropriate;

3.4.6. Monitoring Third Party sales and authorized transfers in accordance with Article X (Third Party Transfers) of this MOU;

3.4.7. providing oversight to the U.S.-ROK Information Assurance/Computer Network Defense Working Group (IA/CND WG) described in paragraph 3.7. of this MOU; and

3.4.8. monitoring export control arrangements required to implement this MOU and, if applicable, referring immediately to the Authorities any export control issues that could adversely affect the implementation of this MOU.

3.5. The Executive Agents for this MOU, who shall act as the designated operational points of contact, and have responsibility for implementation of the MOU and data/information exchange procedures, are:

<u>United States:</u>	USPACOM, through USFK
<u>Republic of Korea:</u>	Information Planning Bureau, MND

3.6. The Executive Agents shall:

3.6.1. exercise day-to-day management of MOU implementation activities and information exchanges;

3.6.2. maintain oversight of the security aspects of this MOU in accordance with Article VII (Disclosure and Use of IA/CND Information), Article VIII (Controlled Unclassified Information), and Article IX (Security) of this MOU; and

3.6.3. establish and co-chair the Information Assurance/Computer Network Defense Working Group (IA/CND WG) described in paragraph 3.7. of this MOU.

3.7. The Authorities, with the Project Officers, shall establish a working group consisting of appropriate representatives to develop and maintain SOPs. The working group is designated as the U.S.-ROK Information Assurance/Computer Network Defense Working Group (U.S.-ROK IA/CND WG). The IA/CND WG shall maintain overall control for IA/CND activities within the scope of this MOU.

3.8. The U.S.-ROK IA/CND WG shall, at a minimum, meet annually and as required to administer and coordinate IA and CND activities. The U.S.-ROK IA/CND WG shall determine the frequency and nature of the IA/CND Information exchanges, and shall establish procedures for rapid exchanges of CND-related information during periods of peace, crisis or hostilities.

3.9. The U.S.-ROK IA/CND WG shall be responsible for:

3.9.1. providing required information to the Project Officers, as requested by the Parties;

3.9.2. reviewing and providing progress reports to the Executive Agents of activities under this MOU;

3.9.3. resolving bilateral IA and CND issues or forwarding to the Project Officers issues that cannot be resolved at their level;

3.9.4. reviewing and forwarding to the Parties recommended amendments to this MOU in accordance with Article XIII (Entry into Force, Amendment, Termination, and Duration) of this MOU;

3.9.5. maintaining oversight of the security aspects of this MOU; and

3.9.6. developing and maintaining the SOP for information exchanges.

3.10. The Establishments for this MOU are:

United States:

1. U.S. Pacific Command (USPACOM)
2. U.S. Forces Korea (USFK)
3. U.S. Strategic Command (USSTRATCOM) and Joint Task Force-Global Network Operations (JTF-GNO)
4. Defense Information Systems Agency (DISA)
5. Defense-wide Information Assurance Program (DIAP)

Republic of Korea:

1. Information Planning Bureau of MND
2. Defense Security Command (DSC)
3. Joint Chiefs of Staff (JCS)
4. Combined Forces Command (CFC)
5. Defense Communication Control Force (DCCF)
6. National Defense Computer Center (NDCC)
7. Headquarters, ROK Army
8. Headquarters, ROK Navy
9. Headquarters, ROK Air Force

3.11. The Establishments may:

3.11.1. provide or receive IA/CND Information to be exchanged through Project Officers or Executive Agents; and

3.11.2. receive IA/CND Information directly from the originating Party with its consent.

3.12. If a Party finds it necessary to exercise a restriction on the retransfer of export-controlled information as set out in paragraph 7.10. of Article VII (Disclosure and Use of IA/CND Information) of this MOU, it shall promptly inform the other Party. If a restriction is then exercised and an affected Party objects, that Party's Authority shall promptly notify the other Party's Authority and they shall immediately consult in order to discuss ways to resolve such issues or mitigate any adverse effects.

ARTICLE IV

CHANNELS OF COMMUNICATION AND VISITS

4.1. IA/CND Information may only be exchanged by those Project Officers, Executive Agents, and U.S. or ROK individuals who are authorized to do so, and are either appointed members of the U.S.-ROK IA/CND WG or are authorized representatives of Establishments. IA/CND Information exchanged between the Parties shall be forwarded via official channels for appropriate dissemination.

4.2. Each Party shall permit visits to its Government facilities, agencies and laboratories, and contractor industrial facilities by employees or Contractor Support Personnel of the other Party provided that the visit is authorized by both Parties and the employees have all necessary and appropriate security clearances and need-to-know.

4.3. All visiting personnel shall be required to comply with security regulations and procedures of the host Party. Any information disclosed or made available to visitors shall be treated as if supplied to the Party sponsoring the visiting personnel, and shall be subject to the provisions of this MOU.

4.4. Requests for visits by personnel of one Party to a facility of the other Party shall be coordinated through official channels, and shall conform with the established visit procedures of the host Party. Requests for visits shall bear the name of this MOU and include a proposed list of topics to be discussed.

4.5. Lists of personnel of each Party required to visit, on a continuing basis, facilities of the other Party shall be submitted through official channels in accordance with recurring visit procedures.

ARTICLE V

FINANCIAL ARRANGEMENTS

5.1. Each Party shall bear the full costs of its participation under this MOU. No funds shall be transferred between the Parties. A Party shall promptly notify the other Party if available funds are not adequate to fulfill its responsibilities under this MOU.

ARTICLE VI

CONTRACTUAL ARRANGEMENTS

6.1. This MOU provides no authority for placing contracts on behalf of the other Party in connection with any IA/CND Information exchanges under this MOU. Furthermore, this MOU creates no responsibility to put in place contracts to implement any IA/CND Information exchanges under this MOU.

6.2. Each Party shall legally bind its contractors to a requirement that the contractor shall not retransfer or otherwise use export-controlled information furnished by the other Party for any purpose other than the purposes authorized under this MOU. The contractor shall also be legally bound not to retransfer the export-controlled information to another contractor or subcontractor unless that contractor or subcontractor has been legally bound to limit use of the information to the purposes authorized under this MOU. Export-controlled information furnished by one Party under this MOU may only be retransferred by another Party to its contractors if the legal arrangements required by this paragraph have been established.

ARTICLE VII

DISCLOSURE AND USE OF IA/CND INFORMATION

- 7.1. Only information related to IA and CND shall be provided or exchanged under this MOU.
- 7.2. Relevant information within the scope of this MOU may be provided or exchanged bilaterally between the Parties according to the disclosure policies of the originating Party.
- 7.3. Information shall be provided or exchanged only when it may be done in accordance with the following provisions:
 - 7.3.1. Information may be made available only if the rights of holders of Intellectual Property rights are not infringed; and
 - 7.3.2. Disclosure must be consistent with the respective national laws, regulations, and policies of the originating Party.
- 7.4. All IA/CND information that is subject to Intellectual Property rights shall be identified and marked, and it shall be handled as Controlled Unclassified Information or as Classified Information, depending on its security classification.
- 7.5. IA/CND information that is exchanged under this MOU shall be disclosed to Third Parties by the receiving Party only in accordance with Article X (Third Party Transfers) of this MOU.
- 7.6. This MOU does not alter the Parties' policies or procedures regarding the exchanges of intelligence or intelligence-related information, nor does it provide authority for exchanges of intelligence information beyond that of existing Government instructions and notices governing exchange of intelligence information.
- 7.7. IA/CND Information provided by the Parties under this MOU may be used by the other Party solely for information, evaluation, and planning purposes consistent with Article II (Objective and Scope) of this MOU. IA/CND Information shall not be used by the receiving Party for any purpose other than the purpose for which it was furnished without the specific prior written consent of the furnishing Party, specifying the authorized use of the IA/CND Information. The receiving Party shall not disclose IA/CND Information exchanged under this MOU to contractors or any other persons, other than its Contractor Support Personnel, without the specific written consent of the furnishing Party. IA/CND Information that is exchanged under this MOU shall only be disclosed to Third Parties by the receiving Party in accordance with Article X (Third Party Transfers) of this MOU.

7.8. The receiving Party shall ensure that Contract Support Personnel, contractors, or any other persons to whom it discloses IA/CND Information received under this MOU are placed under a legally binding obligation to comply with the provisions of this MOU.

7.9. No transfer of ownership of IA/CND Information shall take place under this MOU. IA/CND Information shall remain the property of the originating Party or its contractors.

7.10. Transfer of IA/CND Information shall be consistent with the furnishing Party's applicable export control laws and regulations. Unless otherwise restricted by duly authorized officials of the furnishing Party at the time of transfer to another Party, all export-controlled information furnished by that Party to another Party may be retransferred to the other Party's Contractor Support Personnel subject to the requirements of paragraph 6.2. of Article VI (Contractual Arrangements) of this MOU. Export-controlled information may be furnished by Contractor Support Personnel of one Party to the Contractor Support Personnel of the other Party pursuant to this MOU, subject to the conditions established in licenses or other approvals issued by the Government of the Party furnishing the information in accordance with its applicable export control laws and regulations.

7.11. Each Party shall notify the other Party of any Intellectual Property infringement claims made in its territory as a result of the exchange of information pursuant to this MOU. Insofar as possible, the other Party shall provide information available to it that may assist in defending the claim. Each Party shall be responsible for handling all Intellectual Property infringement claims made in its territory, and shall consult with the other Party during the handling, and prior to any settlement, of such claims.

7.12. No export-controlled information shall be provided or exchanged by either Party, except as otherwise provided in this MOU.

ARTICLE VIII

CONTROLLED UNCLASSIFIED INFORMATION

8.1. Except as otherwise provided in this MOU or as authorized in writing by the furnishing Party, Controlled Unclassified Information provided or generated pursuant to this MOU shall be controlled as follows:

8.1.1. Such information shall be used only for the purposes specified in Article VII (Disclosure and Use of IA/CND Information) of this MOU;

8.1.2. Access to Controlled Unclassified Information shall be limited to personnel whose access is necessary for the permitted use under subparagraph 8.1.1. of this Article, and shall be subject to the provisions of Article X (Third Party Transfers) of this MOU; and

8.1.3. Each Party shall take all lawful steps, which may include national classification, available to it to keep Controlled Unclassified Information free from further disclosure (including requests under any legislative provisions), except as provided in subparagraph 8.1.2. of this Article, unless the originating Party consents to such disclosure. In the event of unauthorized disclosure, or if it becomes probable that the information may have to be further disclosed under any legislative provision, immediate notification shall be given to the originating Party.

8.2. To assist in providing the appropriate controls, the originating Party shall ensure that Controlled Unclassified Information is appropriately marked to indicate its "in confidence" nature. The Parties shall decide, in advance and in writing, on the markings to be placed on the Controlled Unclassified Information.

8.3. Prior to authorizing the release of Controlled Unclassified Information to contractors, the Parties shall ensure the contractors are legally bound to control Controlled Unclassified Information in accordance with the provisions of this Article.

ARTICLE IX

SECURITY

9.1. All Classified Information provided pursuant to this MOU shall be used, stored, handled, transmitted, and safeguarded in accordance with the Exchange of Notes regarding the General Security of Information Agreement Between the United States of America and Korea, which entered into effect May 1, 1962, as amended May 22, 1974, and September 24, 1987.

9.2. Classified Information shall be transferred only through official Government-to-Government channels or through channels approved by the Designated Security Authorities of the Parties. Such Classified Information shall bear the level of classification, denote the country of origin and the provisions of release, and the fact that the Classified Information relates to this MOU.

9.3. Each Party shall take all appropriate lawful steps available to it to ensure that Classified Information provided or generated pursuant to this MOU is protected from further disclosure except as provided by paragraph 9.6. of this Article, unless the other Party consents to such disclosure. Accordingly, each Party shall ensure that:

9.3.1. The recipient Party shall not release the Classified Information to any Third Party without the prior written consent of the originating Party in accordance with the procedures set forth in Article X (Third Party Transfers) of this MOU.

9.3.2. The recipient Party shall not use the Classified Information for other than the purposes provided for in this MOU.

9.3.3. The recipient Party shall comply with any distribution and access restrictions on Classified Information that is provided under this MOU.

9.4. Each Party shall undertake to maintain the security classifications assigned to Classified Information by the originating Party and shall afford to such Classified Information the same degree of security protection provided by the originating Party.

9.5. Each Party shall ensure that access to the Classified Information is limited to those persons who possess the requisite security clearances and have a specific need for access to such Classified Information.

9.6. The Parties shall investigate all cases in which it is known or when there are grounds for suspecting that Classified Information provided pursuant to this MOU has been lost or disclosed to unauthorized persons. Each Party shall also promptly and fully inform the other Party of the details of any such occurrence, the final results of the investigation, and corrective action taken to preclude recurrence.

9.7. For any facility wherein Classified Information is to be used, the responsible Party or Establishment shall approve the appointment of a person or persons to exercise effectively the responsibilities for safeguarding at such facility the Classified Information pertaining to this MOU. These officials shall be responsible for limiting access to Classified Information involved in this MOU to those persons who have been properly approved for access and have a need-to-know.

9.8 Information provided or generated pursuant to this MOU may be classified as high as SECRET. The existence of this MOU is UNCLASSIFIED, and the contents are UNCLASSIFIED.

ARTICLE X

THIRD PARTY TRANSFERS

10.1. The Parties shall not sell, transfer title to, disclose, or transfer possession of IA/CND Information received under this MOU to any Third Party without the prior written consent of the Government of the Party that provided the IA/CND Information under this MOU. Such consent shall not be given unless the Government of the intended recipient confirms in writing to the other Party that it shall:

10.1.1. Not retransfer, or permit the further retransfer of, IA/CND Information provided.

10.1.2. Use, or permit the use of, IA/CND Information provided only for the purposes specified by the Parties.

10.2. The providing Party's Government shall be solely responsible for authorizing such transfers and approving the purpose of such transfers and, as applicable, specifying the method and provisions for implementing such transfers.

ARTICLE XI

SETTLEMENT OF DISPUTES

11.1. Disputes between the Parties arising under or relating to this MOU shall be resolved only by consultation between the Parties and shall not be referred to a national court, to an international tribunal, or to any other person or entity for settlement.

ARTICLE XII

GENERAL PROVISIONS

12.1. The activities carried out under this MOU shall be carried out in accordance with the Parties' respective national laws and regulations, including their export control laws and regulations. The obligations of the Parties shall be subject to the availability of funds for such purposes.

12.2. This MOU does not replace, amend, or terminate any existing bilateral information exchanges or cooperative programs.

12.3. The Parties have mutually determined that this MOU creates binding obligations within each Party's responsibilities under international law.

ARTICLE XIII

ENTRY INTO FORCE, AMENDMENT, TERMINATION, AND DURATION

13.1. This MOU, which consists of a Preamble and thirteen Articles, shall enter into force upon signature by both Parties and shall remain in force for fifteen (15) years. The Parties shall consult no later than one year prior to the expiration of this MOU to decide whether to extend its duration.

13.2. This MOU may be amended or extended upon the mutual written agreement of the Parties, which shall be signed by both Parties' Project Officers with the consent of both Parties' Authorities in accordance with subparagraph 3.2.1. of Article III (Management) of this MOU.

13.3. This MOU may be terminated at any time upon the written agreement of the Parties. In the event both Parties agree to terminate this MOU, the Parties shall consult prior to the date of termination to ensure termination on the most economical and equitable terms.

13.4. Either Party may terminate this MOU upon 90 days written notification of its intent to terminate to the other Party. Such notification shall be the subject of immediate consultation by the LAWG to decide upon the appropriate course of action to conclude the activities under this MOU. In the event of such termination, the terminating Party shall continue participation, financial or otherwise, up to this effective date of termination.

13.5. The respective rights and responsibilities of the Parties regarding Article VII (Disclosure and Use of IA/CND Information), Article VIII (Controlled Unclassified Information), Article IX (Security), and Article X (Third Party Transfers) of this MOU shall continue notwithstanding termination or expiration of this MOU.

IN WITNESS WHEREOF, the undersigned, being duly authorized, have signed this Memorandum of Understanding concerning cooperation on Information Assurance (IA) and Computer Network Defense (CND).

DONE, in duplicate, in the English and Korean languages, both texts being equally authentic.

For the Department of Defense of the United States of America

For the Ministry of National Defense of the Republic of Korea


Signature


Signature

John G. Grimes

Woo, Joo Ha

Name

Name

Assistant Secretary of Defense
Networks and Information Integration

Deputy Minister
Planning and Coordination Office

Title

Title

April 30, 2009
Date

2009 4 30
Date

Washington, DC
Location

Seoul, Korea
Location

대한민국 국방부와

미 합중국 국방부간

정보보증/컴퓨터네트워크방어 협력에 대한

양해각서

(소제: 한·미 정보보증/컴퓨터네트워크방어 양해각서)

목 차

● 서론.....	1
● 제 1 조	
용어 정의	2
● 제 2 조	
목표 및 범위.....	4
● 제 3 조	
관리.....	5
● 제 4 조	
의사소통 및 방문 창구	9
● 제 5 조	
재무 약정.....	10
● 제 6 조	
계약 관련 약정.....	11
● 제 7 조	
정보보증/컴퓨터네트워크방어 정보의 공개 및 이용.....	12
● 제 8 조	
통제된 평문	14
● 제 9 조	
보안.....	15
● 제 10 조	
제 3 자 이전.....	17
● 제 11 조	
분쟁 해결	18
● 제 12 조	
일반적인 조항	19
● 제 13 조	
발효, 개정, 종료 및 유효기간	20
● 서 명	21

서 문

대한민국 국방부와 미합중국 국방부(이하 '양 당사자' 라 칭함)는

1962년 5월 1일 발효되고 1974년 5월 22일, 1987년 9월 24일 개정된
대한민국 정부와 미합중국 정부간의 일반적인 정보 보안 협정이 이 각서에 적용됨을 인
식하며;

국방분야에 공통 관심사를 가지며;

정보보증과 컴퓨터네트워크방어 사안을 조율함에 있어서 상호 협력을 통해 얻어지는
이익을 인식하고 있고;

정보보증/컴퓨터네트워크방어 정보의 교환을 통하여 또한 연합군사작전의 계획과 수행
에 있어서 기존의 국방능력 향상을 원하고;

사이버 방어와 관련된 정보의 상호교환에 있어서 양당사자의 협력에 따른 이익을 인식
하며;

다음과 같이 합의하였다.

제 1 조

용어 정의

양 당사자는 본 양해각서에 사용된 아래 용어의 정의를 공동으로 결정하였다.

Authorities (당국자)	양 당사자를 대신하여 본 양해각서의 이행과 관련된 임무수행 권한을 부여받은 본 각서에 명시된 정부인사
Classified Information (비문)	국가 안보를 위하여 보호가 필요하고 지정된 보안 등급 표시가 명시되어 있는 공식정보. 이 정보는 구두, 시각, 자기, 문서 형태 혹은 장비 기술의 형태로도 될 수 있다.
Computer Network Defense (CND) (컴퓨터네트워크방어)	정보 시스템과 컴퓨터네트워크에서 일어나는 인가되지 않은 행위에 대한 방어, 감시, 분석, 탐지 및 대응을 위해 취해진 조치. 인가되지 않은 행위란 컴퓨터네트워크와 정보체계 또는 그 내용에 대한 교란, 거부, 성능 저하, 파괴, 약탈 및 접근과 정보의 절도를 포함한다. 컴퓨터네트워크 방어 보호 활동은 정보보중 보호 활동을 이용한다. 컴퓨터네트워크방어 대응은 경보 또는 위협정보, 감시, 분석, 침입 탐지, 경향 및 패턴 분석을 포함한다.
Contractor Support Personnel (계약자 지원인원)	지원 계약에 따라 당사자에게 행정, 관리, 과학 또는 기술 지원용역을 제공하도록 구체적으로 식별된 인원들
Controlled Unclassified Information (통제된 평문)	해당 국가법규에 의해 정보의 접근 및 배포선이 제한된 비밀이 아닌 정보. 이에는 비밀문서 목록에서 제외되었지만 여전히 통제 받고 있는 정보가 포함된다.
Designated Security Authority (지정보안당국자)	이 양해각서의 국가산업 보안측면의 협력과 이행에 대해 책임을 지도록 국가당국자에 의해 지정된 보안권한자
Establishments (관계기관)	관리담당관이나 집행대행기관을 통해 교환될 정보를 제공하거나 이에 관심이 있는 본 양해각서에 명시된 정부 기관들
Executive Agents (집행 대행기관)	본 각서에 명시된, 당국자를 대행하도록 인가를 받고 본 각서와 관련된 이행, 관리 및 자료 또는 정보 교환 절차에 대해 책임을 지는 정부기관

Information Assurance/Computer Network Defense Information(IA/CND Information) (정보보증/컴퓨터네트워크방어 정보)	저작권, 특허, 혹은 기타 법적 보호 여부와 상관 없이 과학, 기술, 사업 및 재무 지식을 포함하나, 이에 국한되지 않으며, 형식이나 종류에 상관 없이 어떤 수단이든지 간에 전달될 수 있는 모든 정보보증/컴퓨터네트워크방어 지식
Information Assurance (IA) (정보보증)	정보체계 또는 정보체계에 의해 처리되는 정보의 기밀성, 무결성, 가용성, 인증 및 부인방지를 보장함으로써 정보 및 정보체계를 보호하고 방어하는 활동
Intellectual Property (지적재산)	1994년 4월 15일 체결된 지적재산권의 무역 관련 측면에 관한 세계무역기구(WTO) 합의에 따라, 모든 저작권 및 관련 권리, 발명과 관련된 모든 권리(특허권 포함), 등록 혹은 미등록 상표(서비스 마크 포함)에 관한 모든 권리, 등록 혹은 미등록 의장, 공개된 정보(기업 비밀 및 노하우 포함), 통합 회로 설계도, 지리적 표시, 그리고 산업, 과학, 문학, 예술 분야의 창조적 활동에서 비롯된 모든 기타 권리
Party (당사자)	군인 또는 민간인이 대표한 이 양해각서의 서명권자. 계약자 및 계약자 지원 인원은 이 양해각서 당사자의 대표자가 될 수 없다.
Project Officers (관리담당관)	정보보증/컴퓨터네트워크방어 활동에 대한 정책감독을 유지하도록 당국자로부터 특별히 인가받은 정부기관의 대표자
Response (대응)	양당사자에 의해 보고되거나 양당사자에게 영향을 주는 사건들의 처리를 위해 취해지는 모든 활동
Standard Operating Procedure (SOP) (예규)	정보보증/컴퓨터네트워크방어 정보의 공유 절차
Third Party (제 3자)	양 당사자 정부 이외의 정부 또는 기관, 그리고 소속 정부가 당사자의 정부가 아닌 어느 개인 또는 기타 기관

제 2 조

목표 및 범위

- 2.1. 본 양해각서의 목표는 정보보증과 컴퓨터통신망 방어의 사안에 있어서 대한민국 국방부, 미국방부, 미태평양사령부 및 주한미군간 정보 교환 및 관련 활동을 수행하는데 있다. 양 당사자는 양 당사자의 공통 목표인 정보망의 보호에 기여하기 위해 쌍방 정보보증/컴퓨터 네트워크방어 활동 및 정보보증/컴퓨터네트워크방어 정보 공유를 수행한다. 본 각서의 범위 안에서 수행된 행동들은 아래의 측면에서 방어 능력을 증가시킨다.
 - 2.1.1. 의사 결정자를 위한 정보의 전송과 처리에 사용되는 정보와 정보체계의 기밀성, 무결성, 가용성을 향상시킨다.
 - 2.1.2. 한국군과 미군의 상호운용성을 향상시킨다.
 - 2.1.3. 사이버 공격의 예측, 탐지 및 대응능력을 향상시킨다.
 - 2.1.4. 보다 견고하고 신뢰할 수 있는 지휘 통제체계를 제공하기 위해서 정보 및 정보체계의 상호 운용성, 정책 개발, 형상관리 및 정보와 정보체계의 표준화를 향상시킨다.
- 2.2. 이 양해각서의 범위는 다음을 포함한다.
 - 2.2.1. 예규(SOP) 개발;
 - 2.2.2. 정보보증/컴퓨터네트워크방어 정보의 지속적인 교환을 위해 필요한 기술적인 해결책 또는 행정 문서화할 내용 식별.
 - 2.2.3. 사건 대응, 조사 및 수사 분야에서 정보 교환
 - 2.2.4. 평시, 위기 및 전시에 정보보증/컴퓨터네트워크방어 관련 정보의 신속한 교환을 촉진시키기 위하여, 사용된 보안 기술 및 형상 관리 분야에서의 상호운용성 개선을 위한 정보 교환
- 2.3. 본 양해각서에 의거한 정보교환은 호혜적이고 균형이 잡혀야 하는 바, 당사자 간에, 또는 지정된 관리담당관 및 집행대행기관을 통해 제공되거나 교환된 정보들은 대략적으로 양적/질적인 측면에서 동등한 가치를 지녀야 한다.
- 2.4. 어떤 방어 장비나 서비스도 본 양해각서에 의거해 교환되거나 제공되지 않는다.

제 3 조

관 리

- 3.1. 양 당사자는 이로서 다음과 같이 본 양해각서를 위한 당국자를 임명하고, 조직개편시 이에 상응하는 직책을 임명한다.

한국측: 국방부 기획조정실장
미국측: 국방부 네트워크/ 정보 통합(NII) 차관보

- 3.2. 당국자들은 다음과 같은 책임이 있다.

- 3.2.1. 이 양해각서 제 13 조(발효, 개정, 종료 및 유효기간)에 따라 본 양해각서 개정을 검토하고, 또한 당사자의 승인을 받기 위해 건의함.
- 3.2.2. 본 양해각서에 명시된 노력에 대한 집행간부급 감독을 집행함.
- 3.2.3. 관리담당관들에 의해 제기된 문제들을 해결함.
- 3.2.4. 관리담당관 임무 및 관계기관 목록을 지정함.
- 3.2.5. 양 당사자의 유출통제 책임자와 협의하여, 소단락 제 3.4.8 항에 의거한 관리담당관이 제기하거나 또는 본 조항의 단락 제 3.12 항에 의거한 어느 한쪽 당사자가 제기한 일체의 유출통제 문제를 해결하기위해 최선의 노력을 경주함.

- 3.3. 이 양해각서의 다음의 관리담당관들은 이 양해각서의 관리 책임을 지고 각 당국자를 대표한다.

한국측: 정보화기획관
미국측: 국제 정보보증 프로그램 국장, 국방부 NII 차관보실

- 3.4. 양해각서의 관리담당관은 다음과 같은 사항을 담당한다.

- 3.4.1. 본 양해각서하의 활동에 대한 정책 감독을 실행.
- 3.4.2. 집행 대행기관에 의해 제기된 문제들을 해결.
- 3.4.3. 관리담당관에 의해 해결될 수 없는 문제들을 당국자에게 회부.
- 3.4.4. 이 양해각서의 개정 또는 종료를 당국자에게 건의.

- 3.4.5. 본 양해각서를 위해 연간 목표를 적절히 수립하고 유지.
 - 3.4.6. 이 양해각서의 제 10 조(제 3 자 이전)에 의거한 제 3 자 판매 및 인가된 이전을 감시.
 - 3.4.7. 이 양해각서의 3.7 조항에서 설명된 한·미 정보보증/컴퓨터네트워크방어 실무단을 감독.
 - 3.4.8. 이 양해각서의 이행에 있어 요구되는 유출통제를 감시하고, 가능할 경우, 이 양해각서의 이행에 불리하게 영향을 줄 수 있는 유출통제 문제를 즉시 당국자에게 회부.
- 3.5. 지정된 운용상 연락창구 역할을 하며 본 양해각서의 이행 및 자료/정보 교환 절차의 책임이 있는 본 양해각서의 집행 대행기관은:

<u>한국측:</u>	국방부 정보화기획관실
<u>미국측:</u>	미 태평양사령부 (주한미군사령부가 대행)

3.6. 집행 대행기관은

- 3.6.1. 양해각서 이행 활동과 정보 교환 등의 일상 관리업무를 수행한다.
 - 3.6.2. 이 양해각서의 제 7 장(정보보증/컴퓨터네트워크방어 정보의 공개 및 이용), 제 8 장(통제된 평문)과 제 9 장(보안)에 따라서 이 양해각서의 보안 측면을 감독한다.
 - 3.6.3. 이 양해각서의 제 3.7 조항에 명시된 정보보증/컴퓨터네트워크방어 실무단을 구성하고 공동 의장직을 수행한다.
- 3.7. 당국자는, 관리담당관과 함께, 예규의 개발과 유지를 위하여 적절한 대표자로 구성된 실무단을 구성한다. 이 실무단은 한·미 정보보증/컴퓨터네트워크방어 실무단으로 지정된다. 한·미 정보보증/컴퓨터네트워크방어 실무단은 본 양해각서의 적용범위 내의 정보보증/컴퓨터네트워크방어 활동의 전반적 통제를 유지한다.
- 3.8. 한·미 정보보증/컴퓨터네트워크방어 실무단은 최소한 연 1 회 또는 필요시에 만나서 정보보증과 컴퓨터네트워크방어 활동들을 관리하고 조율한다. 한·미 정보보증/컴퓨터네트워크방어 실무단은 정보보증/컴퓨터네트워크방어 정보교환의 빈도와 성격을 결정한다. 그리고 평시, 위기 또는 전시에 컴퓨터네트워크방어 관련 정보의 신속한 교환을 위한 절차를 수립한다.
- 3.9. 한·미 정보보증/컴퓨터네트워크방어 실무단은 다음 사항을 책임진다.
- 3.9.1. 당사자가 요청하는 대로, 요구된 정보를 관리담당관에게 제공한다.
 - 3.9.2. 본 양해각서에 의한 활동의 진행보고서를 검토하고 집행 대행기관에 제공한다.

3.9.3. 양당사자의 정보보증/컴퓨터네트워크방어 문제들을 해결하고, 실무단에서 해결할 수 없는 문제들은 관리담당관에게 전달한다.

3.9.4. 이 양해각서의 제 13 조(발효, 개정, 종료 및 유효기간)에 따라서 본 양해각서의 개정 권고안을 검토하고 당사자에게 전달한다.

3.9.5. 이 양해각서의 보안 측면의 감독을 유지한다, 그리고

3.9.6. 정보 교환을 위한 예규를 발전시키고 유지한다.

3.10. 본 양해각서 관계기관은:

한국측:

1. 국방부 정보화기획관실
2. 기무사령부
3. 합동참모본부
4. 연합사령부
5. 국군지휘통신사령부
6. 국방부 전산정보관리소
7. 육군본부
8. 해군본부
9. 공군본부

미국측:

1. 미 태평양사령부 (USPACOM)
2. 주한미군 (USFK)
3. 미 전략사령부 (USSTRATCOM)와
범세계 네트워크작전 합동기동부대 (JTF-GNO)
4. 미 국방부 정보체계국 (DISA)
5. 국방 정보보증 사업(DIAP)

3.11. 관계 기관은

3.11.1. 관리담당관이나 집행대행기관을 통하여 교환될 정보보증/컴퓨터네트워크방어 정보를 제공하거나 받을 수 있다. 그리고

3.11.2. 정보 제공 당사자의 동의가 있을 시, 정보보증/컴퓨터네트워크방어 정보를 직접 제공받을 수 있다.

3.12. 본 양해각서의 제 7 조 (정보보증/컴퓨터네트워크방어 정보의 공개 및 이용) 의 7.10 항에 명시된 바 당사자가 유출통제된 정보의 재이전을 제한할 필요가 있다고 판단되면, 다른 당사자에게 즉시 이를 통보해야 한다. 만약 제한이 가해지고 그로 인해 영향을 받는 당사자가 반대하면, 그 당사자의 당국자는 상대 당사자의 당국자에게 바로 통보하고, 양 당국자들은 이러한 문제를 해결하거나 일체의 역효과를 최소화하기 위한 방법을 토의하기 위해 즉각 협의해야 한다.

제 4 조

의사소통 및 방문 창구

00

- 4.1. 본 양해각서에 명시된 관리담당관, 집행대행기관 및 인가를 받고, 한·미 정보보증/컴퓨터네트워크방어 실무단의 지명된 구성원이거나 또는 관계기관의 대표자인 한국측 또는 미측의 개인들만이 정보보증/컴퓨터네트워크방어 정보 교환을 수행할 수 있다. 당사자들 간에 교환된 정보보증/컴퓨터네트워크방어 정보는 적절한 배포를 위하여 공식적인 경로를 이용하여 전달되어야 한다.
- 4.2. 각 당사자는 상대측 당사자의 직원 또는 계약업체 지원인원이 정부 시설, 산하 기관과 연구소 및 계약업체 산업설비 방문을 허락한다. 단 이 방문은 양 당사자들간에 의해 승인받아야 하며 해당 직원은 필수 및 적절한 모든 보안통행허가와 필지사항(need-to-know)을 확보해야 한다.
- 4.3. 모든 방문 인원은 수용측 당사자가 요구하는 보안절차와 규정을 준수해야 한다. 방문자에게 공개되거나 제공된 모든 정보는 방문자의 신원을 보증하는 측 당사자에게 제공된 것으로 간주되며 본 양해각서 조항의 적용을 받아야 한다.
- 4.4. 어느 일방의 당사자측 직원에 의한 상대측 당사자의 시설에 대한 방문 요청은 공식 경로를 통해 조율되며, 수용측 당사자의 정해진 방문 절차를 순응해야 한다. 방문 요청은 본 양해각서 이름하에, 논의주제 제안목록을 포함한다.
- 4.5. 상대측 당사자의 시설을 계속하여 방문해야 하는 각 당사자 측의 인원목록은 되풀이되는 방문의 관련절차에 따라 공식경로를 통해 제출된다.

제 5 조

재무 약정

- 5.1. 각 당사자는 본 양해각서에 의거, 자기측 참여에 대한 모든 비용을 부담한다. 어떠한 자금도 양 당사자들간에 이전될 수 없다. 각 당사자는 본 양해각서에 의한 책임을 이행하는데 가용 자금이 충분하지 않을 경우 반드시 상대측 당사자에게 신속히 통보해야 한다.

제 6 조

계약 관련 약정

- 6.1. ⁰⁰ 본 양해각서는 본 양해각서에 의한 일체의 정보보증/컴퓨터네트워크방어 정보교환과 관련하여 상대측 당사자를 대신하여 계약을 체결할 권한을 부여하지 않는다. 더욱이, 본 양해각서는 이 양해각서하에서 일체의 정보보증/컴퓨터네트워크방어 정보 교환을 이행하기 위한 계약을 체결할 책임을 발생시키지 않는다.
- 6.2. 각 당사자는 이 양해각서에 의거 인가된 목적 이외의 다른 목적을 위해 당사자의 계약자가 상대측 당사자에 의해 제공된 유출통제된 정보를 재이전하거나 달리 사용하지 못하도록 하는 요구조건에 각측 계약자를 법적으로 강제해야 한다.
계약자는 또다른 계약자 또는 하도급 계약자가 유출통제된 정보를 본 양해각서에 의거 인가된 목적으로 제한하여 사용하도록 법적으로 강제되어있지 않는 한, 유출통제된 정보를 또다른 계약자 또는 하도급 계약자에게 재이전하지 못하도록 법적으로 강제되어야 한다. 본 양해각서에 의거 어느 일방의 당사자에 의해 제공된 유출통제된 정보는 이 조항이 요구하는 법적 약정이 수립되었을 경우에만 또다른 당사자에 의해 그의 계약자들에게 재이전 될 수 있다.

제 7 조

정보보증/컴퓨터네트워크방어 정보의 공개 및 이용

- 7.1. 본 양해각서 하에서는 정보보증 및 컴퓨터네트워크방어에 관련된 정보만이 제공되거나 교환된다.
- 7.2. 본 양해각서의 범위내의 관련 정보는 정보제공측 당사자의 공개 정책에 의거 양 당사자 간 쌍방 교환 및 제공이 가능하다.
- 7.3. 정보는 오로지 아래 조항에 의거한 경우에만 제공이나 교환된다:
 - 7.3.1. 정보는 지적 재산권자의 권리가 침해되지 않는 경우에만 이용가능해진다.
 - 7.3.2. 공개는 제공측 당사자의 국가법, 규정 및 정책과 일관성이 있어야 한다.
- 7.4. 지적 재산권의 적용을 받는 모든 정보보증/컴퓨터네트워크방어 정보는 해당 보안등급에 따라 표시되어야하고, 통제된 평문 혹은 비문으로 취급한다.
- 7.5. 본 양해각서에 의거하여 교환된 정보보증/컴퓨터네트워크방어 정보는 본 양해각서의 제 10 조(제 3 자 이전)에 의해서만 정보수령측 당사자에 의해 제 3 자에게 공개된다.
- 7.6. 본 양해각서는 양 당사자의 첩보 또는 첩보와 관련된 정책 또는 정보교환 절차를 변경하지 않으며, 첩보정보 교환 관련 기존 정부 지침 및 고지의 권한을 넘어서는 첩보정보교환 권한을 제공하지 않는다.
- 7.7. 본 양해각서에 의거하여 양 당사자에 의해 제공된 정보보증/컴퓨터네트워크방어는 본 양해각서 제 2 조(목표 및 범위)와 일관된 정보, 평가 및 기획 목적으로만 상대측 당사자에 의해 사용될 수 있다. 정보보증/컴퓨터네트워크방어 정보의 인가된 사용을 명시한 제공측 당사자의 구체적인 사전서명 동의가 없으면, 정보 수령측 당사자는 정보보증/컴퓨터네트워크방어 정보를 그 정보가 제공된 용도외의 다른 어떤 용도로도 사용할 수 없다. 정보수령 당사자는 제공측 당사자로부터 구체적 서면동의를 받지 않은 이상, 본 양해각서에 따라 교환되는 정보보증/컴퓨터네트워크방어 정보를 계약자 지원 인원을 제외한 계약자나 다른 어떤 인원에게 공개할 수 없다. 이 양해각서에 의해 교환된 정보보증/컴퓨터네트워크방어 정보는 오로지 이 양해각서 제 10 조(제 3 자 이전)에 의거하여 수령측 당사자에 의해 제 3 자에게 공개되어야 한다.
- 7.8. 정보수령측 당사자는 본 양해각서에 의거하여 제공받은 정보보증/컴퓨터네트워크방어 정보 공개 대상인 계약자 지원 인원 및 계약자, 또는 어떠한 다른 개인이, 본 양해각서 조항에 순응하도록 하는 법적 강제력이 있는 의무사항에 적용을 받도록 한다.

- 7.9. 본 양해각서에 의거하여, 정보보중/컴퓨터네트워크방어 정보 소유권의 이전은 허락되지 않는다. 정보보중/컴퓨터네트워크방어 정보의 소유권은 원 소유 당사자 혹은 원 소유 당사자의 계약자에게 있다.
- 7.10. ① 정보보중/컴퓨터네트워크방어 정보의 이전은 정보 제공측 당사자의 적용가능한 유출통제 법률 및 규정에 따라야 한다. 또다른 당사자에게로의 이전시점에서 제공측 당사자의 적법하게 인가된 담당관에 의해 달리 제한되지 않는 한, 제공측 당사자가 다른 당사자에게 제공하는 모든 유출통제된 정보는 본 교환각서 제 6 조(계약관련 약정) 6.2. 항의 요구 조건에 따라 또다른 당사자의 계약자 지원 인원에게 재이전될 수 있다. 유출통제된 정보는 이 양해각서에 의거, 한 당사자의 계약자 지원 인원에게 상대측 당사자의 계약자 지원 인원에게 제공될 수 있다. 단, 이는 정보제공측 당사자 정부가 적용 가능한 유출 통제 관련 법률 및 규정에 따라 발한 면허 또는 기타 승인에 명시된 조건에 따른다.
- 7.11. 각 당사자는 본 양해각서에 따른 정보교환으로 인한 자기 영토내에서 제기된 일체의 지적 재산권 침해 청구를 상대측 당사자에게 통지할 의무가 있다. 가능한 한, 상대측 당사자는 해당 청구를 변호하는데 도움될 수 있는 자기측에 이용가능한 정보를 제공해야 한다. 각 당사자는 각자의 영토내에서 발생한 모든 지적 재산권 침해 청구에 대해 그러한 청구 처리과정 및 일체의 타결 전에 상대 당사자와 협의해야 한다.
- 7.12. 이 양해각서에 달리 명시되어 있지 않는 한, 어느 일방의 당사자에 의해서도 유출통제된 정보가 제공되거나 교환될수 없다.

제 8 조

통제된 평문

- 8.1. 이 양해각서에 달리 명시되어 있거나 정보제공측 당사자에 의해 서면으로 허가된 경우를 제외하고 이 양해각서에 따라 제공되거나 생성된 통제된 평문은 아래와 같이 통제된다.
 - 8.1.1. 이러한 정보는 제 7 조(정보보증/컴퓨터네트워크방어 정보의 공개 및 이용)에서 명시된 목적에 대해서만 사용이 가능하다.
 - 8.1.2. 통제된 평문에 대한 접근은 이 조의 소단락 제 8.1.1.항에 의해 허용된, 접근이 필요한 인원들로 제한하며, 본 양해각서의 제 10 조(제 3 자 이전)의 조항에 따른다.
 - 8.1.3. 각 당사자는 이 조의 8.1.2.항에 명시된 바를 제외하고는, 추가적 정보공개에 대해 정보제공 당사자가 동의하지 않는 한, 통제된 평문을 그러한 공개로부터 보호하기 위하여 가용한 모든 적법한 조치를 취해야 한다. 이러한 조치는 국가차원의 비밀등급을 포함 할 수도 있다. 허가되지 않은 공개가 발생할 경우이거나 어떠한 법률 조항하에서 정보가 추가적으로 공개되어야 할 가능성이 있다면, 즉각적으로 정보 제공당사자에게 통보되어야 한다.
- 8.2. 적절한 통제를 하는데 도움을 주기 위해, 정보제공 당사자는 통제된 평문에 해당 정보의 '비밀' 성격이 나타나도록 적절히 표시해야 한다. 양 당사자는 통제된 평문 상에 취해질 표식에 관해 미리 서면으로 결정해야 한다.
- 8.3. 통제된 평문을 계약자에게 공개하는 것을 허가하기 전에, 양 당사자는 계약자들이 이 양해각서의 조항에 의거 통제된 평문을 통제하도록 법적으로 강제되도록 해야 한다.

제 9 조

보 안

- 9.1. ⁰⁰ 본 양해각서에 의거하여 제공된 모든 비문은 1962년 5월 1일 발효되고, 1974년 5월 22일, 1987년 9월 24일 개정된 대한민국과 미합중국간의 일반적인 정보보안 협정에 관한 교환각서에 의거하여 이용, 저장, 처리, 전송 및 보호된다.
- 9.2. 비문은 오로지 정부 대 정부 공식 창구 혹은 양 당사자의 지정보안당국자를 통해서만 전송되어야 한다. 그러한 비문은 보안등급 수준, 정보 제공국, 공개 조항 및 본 양해각서와 관련된 비문이라는 표시가 되어 있어야 한다.
- 9.3. 이 조의 9.6. 조항에서 명시되지 않았거나, 더이상의 공개에 대한 다른 당사자의 동의를 얻지 않았다면, 본 양해각서에 의거하여 제공되거나 생성된 비문은 더 이상 공개되지 않도록 각 당사자는 가용한 모든 적절한 적법조치를 취해야 한다.
 - 9.3.1. 정보수령측 당사자는 본 각서 제 10장(제 3자에 대한 제공)의 절차에 따라 정보 제공측 당사자의 사전 서면동의 없이 비문을 그 어떠한 제 3자에게도 공개하지 않는다.
 - 9.3.2. 정보수령측 당사자는 본 양해각서에 명시된 목적 이외에는 비문을 이용하지 아니한다.
 - 9.3.3. 정보수령측 당사자는 본 양해각서에 명시된 대로 비문의 배포 및 접근에 관한 모든 제한을 따른다.
- 9.4. 각 당사자는 정보제공측 당사자가 정한 비문 별 보안 등급을 유지할 의무가 있고 그 비문에 대해 정보제공측 당사자가 실행하고 있는 것과 같은 보안 등급의 보호를 해야 한다.
- 9.5. 각 당사자는 해당 필수 보안허가 및 해당 비문에 접근하기위한 구체적인 필요가 있는 자로 그 비문에 대한 접근을 제한해야 한다.
- 9.6. 양 당사자는 본 양해각서에 의거하여 제공된 비문이 유실 또는 비인가자에게 공개되었다고 밝혀지거나 그와 같이 의심할 근거가 있는 모든 경우를 조사해야 한다. 각 당사자는 그러한 상황이 발생하게 된 모든 세부사항, 최종 조사결과 및 이러한 상황의 재발방지를 위한 시정 조치를 상대측 당사자에게 신속히 그리고 충실히 알려야 한다.

- 9.7. 비문을 다루는 모든 시설에 대해, 책임당사자 또는 관계기관은, 본 양해각서 관련 비문을 그러한 시설에서 보호하는 책임을 효과적으로 수행할 수 있도록 담당자 일인 혹은 다수의 임명을 승인한다. 임명된 담당자는 본 양해각서와 관련된 비문에 대한 접근을 적절히 승인받고 알 필요가 있는 자로 제한할 책임이 있다.
- 9.8. 본 양해각서에 의거하여 제공되거나 생성된 정보는 “군사 2급비밀” 까지 분류 될 수 있다. 본 양해각서의 실재는 “평문” 이며 그 내용도 “평문” 이다.

제 10 조

제 3 자 이 전

- 10.1. 양 당사자는 본 양해각서에 의거 제공받은 정보보증/컴퓨터네트워크방어 정보를 제공측 당사자 정부의 사전 서면동의 없이는 어떠한 제 3 자에게도 판매하거나 권리양도하거나 공개, 또는 소유이전할 수 없다. 그러한 동의는 의도된 수령측 정부가 다음과 같은 사항들을 상대측 당사자에게 서면으로 확인해 주기 전까지는 이루어질 수 없다.
 - 10.1.1. 정보수령측 당사자는 제공된 정보보증/컴퓨터네트워크방어 정보를 재이전하지 않으며, 또는 그 이상의 재이전을 허가하지 않는다.
 - 10.1.2. 정보수령측 당사자는 양 당사자가 명시한 목적으로만 제공된 정보보증/컴퓨터네트워크방어 정보를 사용 및 사용허가 한다.
- 10.2. 정보제공측 당사자의 정부는 제 3 자에 대한 정보 이전 허가 및 이전 목적 승인과, 적용가능한 경우, 제 3 자 이전을 이행하는데 필요한 방법 및 조항 명시에 대해서 전적으로 책임을 져야 한다.

제 11 조

분쟁 해결

- 11.1. 본 양해각서 하에서 또는 본 양해각서와 관련하여 발생한 당사자간의 분쟁은 당사자간의 협의에 의해서만 해결되어야 하며, 조정을 위해 해당국의 법정, 국제 법정 또는 어떠한 다른 개인이나 기관에게도 회부되지 않는다.

제 12 조

일반적인 조항

- 12.1. 본 양해각서 하에서 행해지는 모든 활동들은 각 당사자의 유출통제법 및 규정을 포함한 각자의 국가법 및 규정에 따라 실행된다. 당사자의 의무사항은 그러한 목적을 위한 자금의 가용여부에 따른다.
- 12.2. 본 양해각서는 어떠한 기존의 쌍무 정보교환 또는 협력사업도 대체, 개정 또는 종료하지 않는다.
- 12.3. 양 당사자들은 본 양해각서가 국제법하에 각 당사자의 책임내에서 구속력이 있는 의무임을 상호간에 결의하였다.

제 13 조

발효, 개정, 종료 및 유효기간

- 13.1. 서문 및 13 개 조항으로 구성된 본 양해각서는 양 당사자에 의해 서명된 후 즉시 효력을 가지며 향후 15 년간 효력을 가진다. 양 당사자는 늦어도 본 양해각서의 만기일 1 년 전에 그 유효기간을 연장할 것인지 협의해야 한다.
- 13.2. 본 양해각서는 양 당사자의 상호서면합의 즉시 개정 혹은 연장될 수 있는 바, 동 합의는 본 양해각서의 제 3 조(관리)의 소단락 3.2.1.에 따른 양 당사자 당국자의 동의를 얻어 양 당사자의 관리담당관에 의해 서명된다.
- 13.3. 본 양해각서는 양 당사자의 서면합의를 통해 언제든지 종료될 수 있다. 양 당사자가 본 각서를 종료하기로 합의한 경우, 양 당사자는 종료일자에 앞서 가장 경제적이고 형평성에 맞게 종료될 수 있도록 협의해야한다.
- 13.4. 어느 일방 당사자도 상대측 당사자에게 종료 의사를 종료 90 일 전에 서면 통보함으로써 본 양해각서를 종료할 수 있다. 그러한 통보는 정보보증/컴퓨터네트워크방어 실무단의 긴급협의사항이 되며, 정보보증/컴퓨터네트워크방어 실무단은 본 양해각서에 따라 수행 하던 활동들을 종결하기 위한 적절한 행동방침을 결정한다. 이러한 종료가 실행될 시, 종료수행측 당사자는 종료 발효일자까지 계속해서 재무적 또는 기타 사안에 참여한다.
- 13.5. 본 양해각서의 제 7 조(정보보증/컴퓨터네트워크방어 정보의 공개 및 이용), 제 8 조(통제된 평문), 제 9 조(보안) 및 제 10 조(제 3 자 이전)에 관한 양 당사자의 각 권리 및 책임은 본 양해각서의 종료 또는 기간의 만료에도 불구하고 계속 효력을 갖는다.

이상을 증거로, 정당한 권한을 위임받아, 아래 서명자는 정보보증 및 컴퓨터네트워크방어 협력에 관한 양해각서에 서명하였다.

본 양해각서는 한글과 영어로 각각 2 부가 작성되었으며, 양 문본은 동등하게 정본이다.

대한민국 국방부를 대표하여


서명

우 주 하

성명

기획조정실장

직책

2009. 4. 30
일시

SEOUL, KOREA
장소

미합중국 국방부를 대표하여


서명

John G. Grimes

성명

네트워크/정보통합(NII) 차관보

직책

April 30, 2009
일시

WASHINGTON, DC
장소