

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

THIS DOCUMENT IS CERTIFIED TO BE A TRUE COPY

CERTIFIED BY: Mr. Mark Hall, Office of the Assistant Secretary of Defense (Networks and Information Integration), Director, Information Assurance Policy and Strategy, GS-15

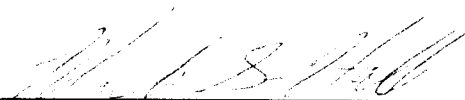


TABLE OF CONTENTS

PREAMBLE..... 3

ARTICLE I..... 4

DEFINITION OF TERMS 4

ARTICLE II..... 6

OBJECTIVE AND SCOPE..... 6

ARTICLE III..... 7

MANAGEMENT..... 7

ARTICLE IV..... 11

CHANNELS OF COMMUNICATION AND VISITS 11

ARTICLE V 12

FINANCIAL ARRANGEMENTS..... 12

ARTICLE VI..... 13

CONTRACTUAL ARRANGEMENTS 13

ARTICLE VII 14

DISCLOSURE AND USE OF IA/CND INFORMATION 14

ARTICLE VIII..... 16

CONTROLLED UNCLASSIFIED INFORMATION..... 16

ARTICLE IX..... 17

SECURITY 17

ARTICLE X 19

THIRD PARTY TRANSFERS 19

ARTICLE XI..... 20

SETTLEMENT OF DISPUTES..... 20

ARTICLE XII 21

GENERAL PROVISIONS..... 21

ARTICLE XIII..... 22

ENTRY INTO FORCE, AMENDMENT, TERMINATION, AND DURATION 222

PREAMBLE

The Department of Defense of the United States of America (U.S. DoD) and the Federal Ministry of Defense of the Federal Republic of Germany (MOD), hereinafter referred to as the "Parties":

On the basis of the Memorandum of Understanding (MOU) between the Parties to the North Atlantic Treaty Organization regarding the Status of their Forces, dated June 19, 1951 (hereinafter referred to as "NATO SOFA");

Recognizing the General Security Agreement between the Governments of the United States of America and the Federal Republic of Germany, which entered into force on December 23, 1960, as amended (Security MOU) applies to this MOU;

Recognizing the Operating Procedures for Implementation of the General Security Agreement, dated December 23, 1960, between the Governments of the Federal Republic of Germany and the United States of America, with Particular Reference to Industrial Security, dated March 10, 1970, as amended September 16, 1991;

Recognizing Appendix G to the Operating Procedures for Implementation of the General Security Agreement, dated December 23, 1960, between the Governments of the Federal Republic of Germany and the United States of America, with Particular reference to a Reciprocal Industrial Security Agreement, which entered into effect September 11, 1980, and amended March 24, 1982;

Recognizing the Agreement between the Government of the United States of America and the Government of the Federal Republic of Germany to Facilitate Interchange of Patent Rights and Technical Information for Defense Purposes, which entered into force on January 4, 1956, and was operative retroactively from December 27, 1955; and

Recognizing the Agreement regarding Procedures for the Reciprocal Filing of Classified Patent Applications in the United States and the Federal Republic of Germany, which entered into force on May 26, 1959, as amended May 28, 1964, applies to this Agreement.

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 Information (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.
Competent Authority	An authority identified by the National Security Authority (NSA) of a Party that is authorized to carry out personnel security clearances in order to give their nationals access to Classified Information and/or is responsible for the protection of Classified Information and who will be communicated to the other Party for the purposes of this MOU whenever necessary.
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 between the MOD and the U.S. DoD, including U.S. European Command (USEUCOM), 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 German Federal Armed 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); and

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

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 personnel, 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:

United States: Assistant Secretary of Defense (ASD), Networks and Information Integration (NII)

Germany: Information Technology – Director Modernization Directorate II

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 the Project Officers and updating the list of Establishments; and

3.2.4. 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.

United States: Director, Information Assurance Policy and Strategy, Office of the Assistant Secretary of Defense (OASD), Networks and Information Integration (NII)

Germany: Branch Chief Modernization Directorate II / IT 3

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. - Germany Information Assurance Working Group (IAWG) described in paragraph 3.7. of this Article; 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 functional points of contact, and have responsibility for implementation of the MOU and data/information exchange procedures, are:

United States: U.S. European Command (USEUCOM)

Germany: Federal Office of the Bundeswehr for Information Management and Information Technology (IT-AmtBw)

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 Working Group (IAWG) described in paragraph 3.7. of this Article.

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. - Germany Information Assurance Working Group (U.S. - Germany IAWG). The IAWG shall maintain overall control for IA/CND activities within the scope of this MOU.

3.8. The U.S. - Germany IAWG shall, at a minimum, meet annually and as required to administer and coordinate IA and CND activities. The U.S. - Germany IAWG 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 crisis or hostilities.

3.9. The U.S. - Germany IAWG 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 Parties 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. European Command (USEUCOM)
- 2. U.S. Strategic Command (USSTRATCOM) and Joint Task Force-Global Network Operation (JTF-GNO)
- 3. Defense Information Systems Agency (DISA)
- 4. Defense-wide Information Assurance Program (DIAP)

Germany:

- 1. Federal Ministry of Defence (BMVg)
- 2. Federal Office of the Bundeswehr for Information Management and Information Technology (IT-AmtBw)
- 3. Bundeswehr Centre for Information Technology (IT-ZentrumBw)

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 Project 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 Germany individuals who are authorized to do so, and are either appointed members of the U.S. - Germany IAWG or are authorized representatives of Establishments. IA/CND Information exchanged between the Parties shall be forwarded via Government-to-Government 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. 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 IC/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 former 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 marked, used, stored, handled, transmitted, and safeguarded in accordance with the Security MOU and procedures as referred to in the Preamble, the provisions of this MOU, and with the Parties' national security laws and regulations.

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 that IA/CND Information under this MOU. Furthermore, neither Party shall permit any such sale, disclosure, or transfer, including by the owner of the IA/CND Information, without the prior written consent of the Government of the other Party. 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, the equipment or 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. Any existing Agreements, Memoranda of Understanding, and Arrangements between the Parties of the Competent Authorities on the protection of Classified Information shall be unaffected by the present MOU.

12.3. The Parties have mutually determined that this MOU creates legally binding obligations 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.

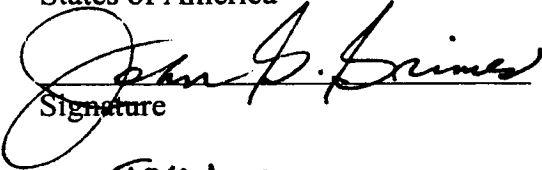
13.4. Either Party may terminate this MOU upon 90 days written notification of its intent to terminate to the other Party. Such notification shall be the subject of immediate consultation by the IAWG to decide upon the appropriate course of action to conclude the activities under this MOU. In the event 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 MOU concerning Cooperation on Information Assurance (IA) and Computer Network Defense (CND).

DONE, in two originals, in the English language.

For the Department of Defense of the United States of America


Signature

JOHN G. GRIMES
Name

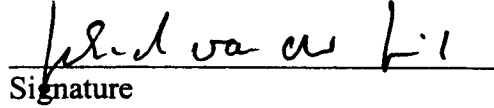
Assistant Secretary of Defense, Networks and Information Integration

Title

16 May 2008
Date

Washington, DC
Location

For the Federal Ministry of Defence of the Federal Republic of Germany


Signature

Gerhard van der Giel
Name

IT-Director Modernization Directorate II

Title

26 Mei 2008
Date

Berlin
Location