11 (1978) Nr. 5

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2023 Nr. 102 HERUITGAVE

A. TITEL

Memorandum van overeenstemming tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika over samenwerking inzake defensiematerieel; Washington/'s-Gravenhage, 25 juli/24 augustus 1978

Voor een overzicht van de verdragsgegevens, zie verdragsnummers 000919 en 013810 in de Verdragenbank.

B. TEKST

In overeenstemming met artikel VI van het Memorandum van overeenstemming is op 13 maart 2006 te Washington een Akkoord tot stand gekomen tot vervanging van Bijlage V bij het onderhavige Memorandum van overeenstemming. De tekst van het Akkoord luidt als volgt:

Security Implementing Arrangement for Operations between the Minister of Defence of the Kingdom of the Netherlands and the Department of Defense of the United States

1. Purpose

a) The following procedures have been developed by the Department of Defense of the United States (DoD) and the Minister of Defence of the Kingdom of the Netherlands (MODNL), hereinafter referred to as "the Participants"; to implement the provisions of the General Security Agreement (GSA) between the Government of the United States and the Government of the Kingdom of the Netherlands, entered into on August 18, 1960, as amended, and replaces the Security Procedures for Industrial Operations between the Ministry of Defence of the Kingdom of the Netherlands and the Department of Defense of the United States, dated April 9, 1982. That Agreement provides for the safeguarding of all classified information exchanged between the Governments. This Implementing Arrangement (hereinafter referred to as "Arrangement") will apply to those cases in which contracts, subcontracts, pre-contract negotiations or other government approved Arrangements involving classified information of the Participants, are placed or entered into by or on behalf of the MODNL in the United States (U.S.) or by or on behalf of the DoD in the Kingdom of the Netherlands (NL).
b) Within the framework of their national legislation, each Participant will take all appropriate measures to ensure the protection of classified information or materiel provided pursuant to this Arrangement.
c) "The U.S. DoD hereby designates the Director, International Security Programs Directorate, Office of the Deputy Under Secretary of Defense (Technology Security Policy and Counterproliferation) as its Designated Security Authority (DSA) to provide policy oversight concerning the provisions of this Arrangement. For the NL MOD the DSA is the Director of the Defence Intelligence and Security Service (DDISS).

2. Definitions

The definitions of the GSA are outdated; The following definitions will therefore be used for the purpose of this Arrangement:

Classified Contract: A contract that requires, or will require, access to classified information by a contractor or by its employees in the performance of a contract.

Classified Information: Official information which has been determined to require, in the interests of national security of the owning or releasing government, protection against unauthorized disclosure and which has

been so designated by the appropriate classification authority. This embraces classified information in any form, be it oral, visual, electronic, documentary or in the form of materiel.

Cognizant Security Office (CSO): The Government office or offices designated to administer industrial security in a Contractor's facility on behalf of the DSA.

Contract: A legally enforceable Arrangement to provide goods or services.

Contractor: An individual or a commercial or other entity that agrees to provide goods or services.

Designated Government Representative (DGR): A person appointed to represent the sending or receiving Participant in making or authorizing a government-to-government transfer of classified information.

Designated Security Authority (DSA): The government authority responsible for the security of classified information covered by this Arrangement.

Document: Any letter, note, minute, report, memorandum, message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, typewriter ribbon, diskette, magnetic tape, or any other form of recorded information.

Facility Security Clearance Assurance (FSCA): A certification provided by a Participant's DSA or CSO for a contractor facility under its territorial jurisdiction which indicates that the facility is security cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard classified information. The FSCA also signifies that classified information CONFIDENTIAL or above will be protected by the contractor on which the FSCA is provided in accordance with the provisions of this Arrangement and that compliance will be monitored and enforced by the responsible DSA or CSO. **NOTE:** A FSCA is not required for a contractor to carry out contracts that require the receipt or production of classified information at the DEPARTEMENTAAL-VERTROUWELIJK (Departmental Confidential) level.

Government-to-government transfer: The principle that classified information and materiel CONFIDENTIAL and above will be transferred through official government-to-government channels or through other channels as may be jointly decided, in writing, by the Participants.

Materiel: Any document product or substance on or in which information may be recorded or embodied. Materiel will encompass everything regardless of its physical character or makeup including documents, writing, hardware, equipment, machinery, apparatus, devices, models, photographs, recordings, reproductions, notes, sketches, plans, prototypes, designs, configurations, maps and letters, as well as all other products, substances or materiel from which information can be derived.

Need to know: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Participant: In the NL Participant refers to the Ministry of Defence (including the Chief of Defence Staff, the Navy, Army, Air Force and Military Police Departments, the Defence Interservice Command and other Defence Agencies). In the U.S. Participant refers to the Department of Defense, Department of Defense agencies and the Departments of the Army, Navy, and Air Force.

Personnel Security Clearance Assurance (PSCA):

a) In the case of an individual who is employed by a government agency or contractor facility under the jurisdiction of a DSA or CSO, a certification provided by that DSA or CSO concerning the level of personnel security clearance held by the individual.
b) In the case of an individual who is a citizen of the country of one Participant but is to be employed by the other Participant or its contractors, a statement provided by the DSA or CSO of the individual's country of citizenship concerning the individual's eligibility for a personnel security clearance at a level specified by the requesting Participant.

Receiving Participant: The Participant to which classified information is transferred.

Sending Participant: The Participant that transfers classified information to the receiving Participant.

3. Restrictions on use and disclosure of exchanged classified information

a) Unless express prior written consent is given to the contrary, the receiving Participant will not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by the sending Participant.

b) The receiving Participant will not pass or disclose to a government official, contractor; contractor's employee or to any other person holding the citizenship of any third country, or to any international organization, any classified information CONFIDENTIAL or above, supplied under the provisions of the General Security Agreement and/or this Arrangement, nor publicly disclose any classified information without the prior written consent of the sending Participant.
c) Nothing in this Arrangement will be taken as an authority for, or to govern the release, use, exchange or disclosure of information in which intellectual property rights exist, until the specific written authorization of the owner of these rights has first been obtained. The sending Participant will advise the requesting Participant of any intellectual property rights attached to any classified information provided to or exchanged with the receiving participant.

4. Protection of classified information

Upon receipt of classified information furnished under this Arrangement, the receiving Participant will carry out to afford the information a degree of security protection at least equivalent to that afforded to the information by the sending Participant. The receiving Participant will be responsible for information so received while it is within the territorial jurisdiction of its government and while it is possessed by or furnished to persons authorized to visit abroad pursuant to this Arrangement. In the NL, the DDISS of the MOD is the CSO and the DSA. In the U.S., the Defense Security Service (DSS) is the CSO. These organizations will assume responsibility for ensuring the administration of security measures for contracts involving classified information CONFIDENTIAL or above awarded to industry for performance in their respective countries. NL DEPARTEMENTAAL-VERTROUWELIJK will be protected in the U.S. in accordance with the provisions of Appendix A.

a) Access. Access to classified information CONFIDENTIAL or above will be limited to those persons who have a need to know and have been security cleared by either of the Participants in accordance with its national laws and regulations to the level at least equal to the classification of the information to be accessed.
b) Inspection/security review. The CSOs, as identified above, will ensure that periodic industrial security inspections/security reviews are made of each contractor facility that is located and incorporated to do business within their country and engaged in the performance of, or in negotiations for, a classified contract.
c) Security costs. Costs incurred in conducting security inspections/security reviews will be borne by the Participant rendering the service. Costs incurred by either of the two Participants through implementation of other security measures, including costs incurred through the use of the diplomatic courier service or any other authorized official courier service, will not be reimbursed. There will be provisions in classified contracts for security costs to be incurred under the contract, such as special costs for packing, transport and the like, which will be borne by the Participant for whom the service is required under the contract. If, subsequent to the date of the contract, the security classification or security requirements under the contract are changed, and the security costs or time required for delivery under the contract are thereby increased or decreased, the contract price, delivery schedule, or both, and any other provisions of the contract that may be affected will be subject to an equitable adjustment by reason of such increased or decreased costs. Such equitable adjustments will be accomplished under the appropriate provisions in the contract governing changes.
d) Security clearances. Clearances of contractor facilities and individuals that will possess or be authorized access to classified information CONFIDENTIAL or above in connection with a classified contract or potential classified contract will be processed according to the pertinent regulations of the country having responsibility for administering security measures for the classified contract.
e) Orientation. The CSOs will ensure that contractors or subcontractors having access to classified information are furnished instructions setting forth their responsibility to protect the information in accordance with applicable national laws and regulations commensurate with the provisions of this Arrangement.

5. Transfers of classified information

a) Classified information CONFIDENTIAL and above will normally be transferred between the Participants through DGRs using government-to-government channels. Government-to-government channels are official government channels (e.g. diplomatic courier service, military courier or military postal service). Other channels that may be established, if jointly decided in writing by the Participants, will ensure that government accountability and control is maintained from the point of origin to the ultimate destination. The CSO for each classified contract will approve the procedures, or inform the contractor of the channels of transmission to be used, and identify the DGR. Materiel will be prepared for transmission in accordance with the national security laws and regulations of the sending Participant.
b) Classified information CONFIDENTIAL and above that is to be transferred electronically will be transmitted using secure means that have been approved by each Participant's communications security authorities.
c) Classified information at the NL DEPARTEMENTAAL-VERTROUWELIJK level will be transmitted in the U.S. in accordance with the provisions of Appendix A.

d) Classified information at the NL DEPARTEMENTAAL-VERTROUWELIJK level may be transmitted or accessed electronically via a public network like the Internet, using government or commercial encryption devices jointly accepted by the Participants' security authorities. International telephone conversations, video conferencing or facsimile transmissions containing NL DEPARTEMENTAAL-VERTROUWELIJK information may be in clear text if an approved encryption system is not available.

6. Public release of information

Public release by a contractor or subcontractor of any classified information CONFIDENTIAL or above pertaining to a classified contract will in the NL be governed by the *Algemene Beveiligingseisen voor Defensieopdrachten* (ABDO 2002 and its subsequent amendments) and in the U.S. by the *National Industrial Security Program Operating Manual* (NISPOM), DoD 5220.22-M. In the case of a NL facility with a U.S. classified contract, initial prior review and approval will be governed by the ABDO 2002 with final approval by the appropriate U.S. authority. In the case of an U.S. facility with a NL classified contract, initial prior review and approval will be governed by the NISPOM with final approval by DDISS.

7. Marking

a) The sending Participant will ensure that documents containing classified information are marked with the appropriate classification markings and pre-fixed with the country of origin/ownership prior to transfer to the receiving Participant. Upon receipt, the information will, if required, be marked with the equivalent security classification, as detailed below. If such information subsequently is included in other documents, those documents will be marked to identify the sending Participant and the applicable classification.

Table of Equivalent Security Classification Categories

The Netherlands	*United States*
STG. ZEER GEHEIM	TOP SECRET
STG. GEHEIM	SECRET
STG. CONFIDENTIEEL	CONFIDENTIAL
DEPARTEMENTAAL-VERTROUWELIJK	No equivalent (See Appendix A)

b) Classified information produced or reproduced by a receiving Participant will be marked with the assigned classification markings of both countries as provided above. The markings will be applied in the manner prescribed in the regulations of the country in which the information is produced or reproduced.

8. Contracts

When a Participant proposes to place, or authorizes a contractor in its country to place, a contract involving classified information CONFIDENTIAL or above with a contractor in the country of the other Participant, the Participant that is to place or authorize the contractor to place such contract will request a FSCA as defined in paragraph 2, where appropriate, from the CSO of the other country. The FSCA will provide governmental assurance that the security conduct by the cleared contractor will be in accordance with the applicable national security laws or regulations and be monitored by its CSO.

a) Security Requirements paragraph
   1. The responsible authority of the Participant in the process of negotiating a classified contract to be performed within the other country, and every contractor in receipt of a classified contract or in the process of negotiating a classified subcontract to be performed within the other country, will incorporate in the contract, request for proposal or subcontract document, appropriate security paragraphs. For such activity involving classified information CONFIDENTIAL or above the security provisions attached at Appendix B will be used.
   2. A copy of the relevant portions of the contract, request for proposal or subcontract, including the security requirements paragraph, will be furnished promptly through appropriate channels to the CSO where the contract is placed to enable them to furnish security supervision over the contract.
   3. Contracts placed with U.S. contractors involving classified information at the NL DEPARTEMENTAAL-VERTROUWELIJK level will identify the measures to be applied for the protection of the NL DEPARTEMENTAAL-VERTROUWELIJK information.

c) Security classification guidance.
   The appropriate authority (see 8.a. (1) above) of the contracting government will furnish the contractor or subcontractor with the security classification guidance pertaining to each classified aspect related to the contract. In the case of the NL, this guidance will be set forth in a Security Classification Guide and in the U.S., by way of a Contract Security Classification Specification (DD Form 254). The guidance must identify that classified information which is furnished by the contracting Participant in connection with the contract, or which is generated pursuant to the classified contract, is assigned a proper security classification. Two copies of the written security classification guidance and of the security portions of the clas-

sified contract, or request for proposal, or subcontract containing the security requirements paragraph will be submitted to the CSO of the Participant which is responsible for administering security measures. The addresses of the CSOs are:

The Netherlands
Director of Defence Intelligence and Security Service (DDISS)
Attention: Head Industrial Security Office
Ministry of Defence
P.O. Box 20701
2500 ES The Hague
NETHERLANDS

United States
Defense Security Service
Attention: Deputy Director for Industrial Security
Department of Defense
1340 Braddock Place
Alexandria, Virginia 22314-1651
UNITED STATES OF AMERICA

c) Subcontracts.
Unless specifically prohibited in the classified contract, a contractor may subcontract within its own country in accordance with the security procedures prescribed in its country for classified subcontracts, and within' the country of the contracting Participant under the procedures established by this Arrangement for placing a classified prime contract in that country, in accordance with the paragraphs set out in Appendix B to this Arrangement.

d) Foreign ownership, control, or influence.
Firms that are determined by national security authorities to be under financial, administrative, policy or management control of nationals or other entities of a third Participant country may participate in a contract or subcontract requiring access to classified information provided by the other Participant only when enforceable measures are in effect to ensure that nationals or other entities of third participant countries will not have access to classified information that is provided to or that is generated therefrom. If enforceable measures are not in effect to preclude access by nationals or other entities of third participant countries, the permission of the originating Participant will be obtained prior to permitting such access.

e) Corporate Governance.
The MODNL approves to oversee implementation of board resolutions entered into by NL entities in connection with DoD Special Security Arrangements (SSAs). The MOD also approves to assist the DoD in addressing alleged violations of the provisions of a DoD SSA by a NL company. These approvals are predicated on the understanding that the DoD will oversee compliance with board resolutions/ arrangements entered into by U.S. entities in connection with requirements with the MOD governing foreign ownership, control or influence of NL entities holding NL security clearances, and that DoD will assist the MOD in addressing violations of these provisions by U.S. entities.

9. Visits

Requests for approval of visits will be submitted using the procedures in Appendix C. Approval for visits will be granted only to persons possessing security clearances at least at the level of the information to which access will be given. Authorization for visitors to have access to classified information will be limited to those who have a need to know. Visits to contractor facilities that only involve access to, or the exchange of information at the unclassified or DEPARTEMENTAAL-VERTROUWELIJK levels do not require the approval of the Participants and may be arranged directly between the sending and receiving facilities.

10. Security assurances related to national security clearances of facilities or individuals of the other country

a) Each Participant will provide a FSCA or PSCA for facilities or individuals in its country when requested by the other Participant.

b) When requested, the Participant receiving the request will determine the security clearance status of the facility or individual that is the subject of the inquiry and forward a FSCA or PSCA if the facility or individual is already cleared. If the facility or individual does not have a security clearance, or the facility or individual has a clearance that is at a lower security level than that requested, notification will be sent to the requesting Participant that the FSCA or PSCA cannot be issued without further consultation. In such cases, further steps may be initiated to conduct inquiries that are necessary to meet the requirement.

c) If the Participant receiving the request determines that a facility located and incorporated to do business in its country is ineligible for a security clearance, the requesting Participant will be notified.

d) If either Participant learns of any adverse information about a facility or an individual for whom it has furnished a FSCA or PSCA, it will notify the other Participant of the nature of the information and the action it intends to take, or has taken. Either Participant may request a review of any FSCA or PSCA that has been furnished by the other Participant, provided that the request is accompanied by a rationale. The requesting Participant will be notified of the results of the review and any subsequent action.

e) If either Participant invalidates, suspends or takes action to revoke a personnel or facility security clearance, the Participant that requested the PSCA or FSCA will be notified and given the reasons for such an action.
f) If requested by the other Participant, each Participant will cooperate in reviews and investigations concerning security clearances.

11. Loss or compromise

a) In the event of the loss or possible loss of classified information CONFIDENTIAL or above, or suspicion that such classified information has been compromised, the receiving Participant will immediately inform the sending Participant.
b) The receiving Participant will carry out an Immediate investigation with assistance from the sending Participant, if required, in accordance with the laws and regulations in the country of the receiving Participant. The receiving Participant will inform the sending Participant about the circumstances and outcome of the investigation as soon as possible and the measures adopted to preclude recurrence of the incident.

12. Disputes

This Arrangement does not create any rights or obligations under international law, nor will it be enforceable by either party under international law. Furthermore, the Participants jointly decide that they will not attempt to enforce the terms of this Arrangement in any domestic, third party, or international court or tribunal. Any disputes or disagreements with regard to interpretation of this Arrangement will be resolved jointly through mutual discussion, cooperation and decision or by separate agreement by both Participants.

13. Effective date

This Arrangement to the 1960 General Security Agreement supersedes the Security Procedures for Industrial Operations between the Ministry of Defence of the Kingdom of the Netherlands and the Department of Defense of the United States (Industrial Security Annex) dated 9 April 1982, as amended on 23 April 1988, and becomes effective upon the date of the last signature.

14. Amendment

The provisions of the Arrangement may be amended with the mutual consent in writing of both Participants.

15. Termination/review

a) This Arrangement will remain in effect until termination of the 1960 General Security Agreement or until this Arrangement is terminated by either Participant, giving the other Participant six months written notification of its intent to terminate the Arrangement. This Arrangement may also be terminated at any time upon written consent of both Participants. Both Participants will remain responsible after termination for the safeguarding of all classified information exchanged under the provisions of the 1960 General Security Agreement and this Arrangement and any contracts entered into, or generated therefrom, in accordance with national laws and regulations.
b) This Arrangement will be reviewed jointly by the Participants no later than ten years after its effective date.
c) Any classified information that is exchanged under the cover of this Arrangement will be safeguarded, even though its transfer may occur following notice by either of the Participants to terminate.
d) In the event of termination, solutions to any outstanding problems will be sought by consultation between the two Participants.

Appendix A

Procedures for handling departementaal-vertrouwelijk information within the United States

1. NL-documents or materiel bearing the classification "DEPARTEMENTAAL-VERTROUWELIJK" will be handled in the U.S. as U.S. UNCLASSIFIED information that is exempt from public release under one or more U.S. laws. These laws include the Freedom of Information Act (FOIA) and Title 10 U.S.C. Section 130(c), "Nondisclosure of Information: Certain Sensitive Information of Foreign Governments and International Organizations." Documents or materiel so marked will be stored in locked containers affording the appropriate protection or closed spaces or areas that shall prevent access by unauthorized personnel.

2. DEPARTEMENTAAL-VERTROUWELIJK documents shall be handled in a manner that will preclude open publication, access or use for other than official government purposes of the United States. It shall be exempt from public release under the applicable U.S. Freedom of Information laws unless the NL Government has granted prior written approval.
3. Before any communications and information system is allowed to store, process or forward DEPARTEMENTAAL-VERTROUWELIJK information, it must be given security approval, known as accreditation. An accreditation is defined as a formal statement by appropriate authority confirming that the use of a system meets the appropriate security requirement and does not present an unacceptable risk: For stand alone desktop PCs and laptop systems utilized in DoD establishments the system registration document together with the security operating procedures fulfils the role of the required accreditation. For contractors, guidance on the use of information technology systems will be incorporated within the restricted conditions requirements paragraph in the contract.
4. DEPARTEMENTAAL-VERTROUWELIJK documents shall be transmitted by first class mail within the United States in one secure cover. Transmission outside the United States will be in two secure covers; the inner cover marked "DEPARTEMENTAAL-VERTROUWELIJK". Such transmissions will be by traceable means such as one of the means authorized for United States classified information, international airmail or commercial courier.
5. Otherwise unclassified U.S. documents originated by a U.S. Government agency which contain information that the NL has classified DEPARTEMENTAAL-VERTROUWELIJK shall bear on the cover and the first page the marking: "DEPARTEMENTAAL-VERTROUWELIJK" – exempt from Public Disclosure under Title 10 U.S.C., Section 130(c)." The DEPARTEMENTAAL-VERTROUWELIJK information shall be identified in the documents.
6. DEPARTEMENTAAL-VERTROUWELIJK information may be transmitted-or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Participants' government security authorities. International telephone conversations, video conferencing or facsimile transmissions containing NL DEPARTEMENTAAL-VERTROUWELIJK information may be in clear text, if an approved encryption system is not available. Telephone conversations, video conferencing or facsimile transmissions within the United States may be in clear text.

Appendix B

Security requirements paragraph for inclusion in classified contracts involving classified information confidential or above

The provisions of this paragraph are based upon the Security Implementing Arrangement for Operations between the Ministry of Defence of the Netherlands and the Department of Defense of the United States, and shall apply to the extent that this contract involves access to or the possession of information or materiel to which a security classification has been assigned by the Government that originated the information (hereafter called originating government).

1. All classified information and materiel furnished or generated pursuant to this contract shall be protected as follows:
   a) The recipient shall not release the information or materiel to a third country government, person, or firm without the prior approval of the originating government.
   b) The recipient shall afford the information and materiel a degree of protection at least equivalent to that afforded it by the originating government as indicated in the table of Equivalent Security Classification Categories below. Information received shall be marked with the originator's level of classification and denote the country of origin.
   c. The recipient shall not use the information and materiel for other than the purpose for which it was furnished without the prior written consent of the originating Participant.

Table of Equivalent Security Classification Categories

The Netherlands	*United States*
STG. ZEER GEHEIM	TOP SECRET
STG. GEHEIM	SECRET
STG. CONFIDENTIEEL	CONFIDENTIAL
DEPARTEMENTAAL-VERTROUWELIJK	No equivalent (See Appendix A)

2. Classified information and materiel furnished or generated pursuant to this contract shall be transferred through government-to-government channels or other channels jointly decided, in writing, by the governments of the United States and the Netherlands. Access to classified information and materiel CONFIDENTIAL or above shall be granted only to persons who have a security clearance at least equal to the classification level of the information and an official need for access to the information in order to perform on the contract.
3. Classified information and materiel furnished under this contract shall be remarked by the recipient with its government's equivalent security classification marking.

4. Classified information and materiel generated under this contract shall be assigned a security classification as specified by the Contract Security Classification Specifications/Security Aspects Letter (SAL) provided with this contract.
5. All cases in which it is known or there is reason to believe that classified information or materiel furnished or generated pursuant to this contract has been subject to a security breach, compromised, lost, or disclosed to unauthorized persons shall be reported promptly and fully by the contractor to its government's security authorities.
6. Classified information and materiel furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:
   a) A potential contractor or subcontractor which is located in the U.S or NL has been approved for access to classified information and materiel at the requisite level by U.S. or the NL security authorities as appropriate;
   b) If located in a third country, prior written consent is obtained from the U.S. or NL government; whichever is the originating government.
7. The recipient contractor shall insert terms that substantially conform to the language of these provisions, including this paragraph, in all subcontracts under this contract that involve access to classified information furnished or generated under this contract.
8. Upon completion of the contract, all classified information or materiel furnished or generated pursuant to the contract shall either be destroyed by the contractor in accordance with national rules and regulations or, if requested, returned to the government that furnished the information.

Appendix C

Visits

1. This appendix describes procedures to be used in the visit request process. Visits to the Netherlands and the United States that involve access to, or the exchange of, classified information CONFIDENTIAL or above require the prior approval of both Participants using the procedures in this appendix.
2. The offices listed below have been designated by each Participant to process visit requests that are received from the other Participant. The listed offices are hereafter referred to as Central Visit Offices or CVOs.

   The Netherlands:

   a) Visits to and from industries
      Netherlands Industrial Visit Control Office (NIVCO)
      P.O. Box 20010
      2500 EA The Hague
      Netherlands
   b) Visits to and from military establishments
      Ministry of Defence
      Defence Intelligence and Security Service
      Industrial Security Office
      Section Visit Requests
      P.O. Box 20701
      2500 ES The Hague
      Netherlands

   United States:

   Department of the Army
   Office of the Deputy Chief of Staff for Intelligence, G-2
   Attn: Foreign Liaison Directorate (DAMI-CHS)
   Washington, DC 20310-1040
   United States of America
   Department of the Navy
   Navy International Programs Office
   Foreign Disclosure Policy Control Division (Navy IPO- 10)
   Washington, DC 20350-5000
   United States of America
   Department of the Air Force
   Office of the Deputy Under Secretary of the Air Force (International Affairs)
   Foreign Disclosure & Technology Transfer Division (SAF/IAPD) 1010 Air Force Pentagon
   Washington, DC 20330-1010
   United States of America
   Defense Intelligence Agency
   Foreign Liaison Staff (DIA/PO-FL)
   Washington, DC 20301-6111
   United States of America
   (The Defense Intelligence Agency processes visits to the Office of the Secretary of Defense (OSD), the OSD Staff, Department of Defense Agencies, and the Joint Staff, and their contractors.)

3. Requests for approval of visits shall include the following information:
   a) Requesting facility. Provide the full name and postal address (include city, state, country, and postal zone) and the telephone and telefax numbers of the facility.
   b) Government agency or industrial facility to be visited. Provide the full name, title, and visit (street) address (include city, state, country, and postal zone) including telephone and telefax number, E-mail address and name of the person with whom the meeting will take place (point of contact).
   c) Dates of visit. Provide the actual date or period (date-to-date) of the visit by day-month year.
   d) Type of visit. Specify whether the visit is a government initiative or commercial initiative and whether the visit is being initiated by the requesting facility or the facility to be visited. Government initiative will be specified only if the visit is in support of an authorized government program, which must be fully described in subparagraph g., below.
   e) Subject to be discussed/justification. Give a concise description of the issues or subjects to be discussed and the reason for the visit. Do not use unexplained abbreviations. In the case of a request for recurring visits, this item should state recurring visits as the first words in the data element (e.g. recurring visits to discuss...) or in the case of an amendment (amendment to visit ID number....).
   f) Anticipated level of classified information to be involved. Indicate TOP SECRET, SECRET, CONFIDENTIAL, as applicable, and country of origin of the information.
   g) Pertinence of visit. Specify the full name of the government program, Arrangement, or sales contract (e.g. foreign military sales case), or request for proposal or tender offer, using commonly used or explained abbreviations only.
   h) Particulars of visitor.
      Name – family name, followed by forename in full and middle initial(s))
      Date of birth (day-month-year)
      Place of birth (city, state, and country)
      Security clearance status (e.g. TS, S, C)
      Passport number/identification number
      Nationality
      Position – Indicate he official title or position the visitor holds in the organization (e.g. director, product manager, etc.)
      Contractor/government agency – Provide the name of the industrial facility or government agency that the visitor represents.
   i) Security officer of the requesting contractor/government agency. Provide the name, telephone number of the requesting security officer.
   j) Certification of security clearance. To be completed by the applicable government clearance agency.
   k) Remarks. This item can be used for certain administrative requirements (e.g. proposed itinerary, requests of hotel reservations, and/or transportation). If the visit has been pre-coordinated, the name, telephone and telefax numbers of the knowledgeable person with whom advance Arrangements have been made should be stated.
4. One-time visits: One-time visits may be for a single visit of a short duration (not to exceed 30 days for the U.S. and 30 days for the Netherlands). Requests for approval of one-time visits will be submitted via government to government channels. Unforeseen circumstances may occur that require individuals to carry out urgent visits which, due to the urgency, do not permit the usual visit notification lead times to be processed. In such circumstances visit applications will be critically reviewed and must be fully documented and justified by the sending Participant. Such emergency visits will be arranged only in exceptional circumstances when:
   a) The proposed visit is related to an official government request for proposal/request for tender offer (e.g. submission of, or amendment to, a bid or proposal; attendance at pre-contract negotiations or bidder's conference); or,
   c) The visit is to be made in response to the invitation of a host government official or host contractor official and is in connection with an official government project, programme or contract; and,
   d) A programme, project or contract opportunity will be placed in jeopardy if the visit request is not approved.
5. Intermittent recurring visits. Programs that will involve intermittent, recurring visits related to classified contracts that are awarded pursuant to bilateral programs conducted under a government-to-government or agency-to-agency Arrangement or memorandum of understanding, and such visits related to commercial contracts that have been approved by the governments, will be processed as prescribed in subparagraphs (a) or (b) below, as applicable:
   a) Bilateral programs. A list will be developed by each participating contractor facility of those individuals who are participating in the program. The list will be included with a request for visit authorization containing the information described in this Appendix. The requests will be sent through government channels to the Central Visit Offices of the host Participant, as identified in paragraph 2, above. Visit authorizations under this procedure will be valid for the duration of the program and there will be no limit on the number of visitors authorized. The list will be checked annually by the requesting CVO to ensure that there is still a requirement for all visitors to continue to be included. There will be no limit to the number of amendments, which may be submitted to the list but will be confined to the addition and deletion of names. Upon approval, direct Arrangements may be made for visits to the participating contractor facilities and government organizations.

b) Other than bilateral programs. A list will be developed by contractor facilities of those individuals that are involved in a specific contract or subcontract that has been approved by the responsible government authorities. The list will be included with a request for visit authorization containing the information described in paragraph 3. above. The request will be submitted to the CVO identified in paragraph 2, above, for visits to Netherlands and to U.S. contractor facilities and government organizations. Visits by individuals on the approved lists may be arranged directly with the security offices of the Contractor facility or government organization to be visited. Visit authorizations under this procedure will be valid for one year, but may be renewed for periods of up to one year as necessary for performance on the contract or subcontract.

6. Extended visits. An extended visit request should be used when a visitor will be required to remain on a site (industrial or government) for a continuous period of greater than 30 days in the Netherlands, or 30 days in the U.S. The lead-time for a request for an extended visit authorization to the Netherlands is thirty (21) days, and for the U.S. is thirty (21) days. An extended visit authorization can be valid for a period of up to three (3) years in the Netherlands, and for the duration of the program in the U.S. All extended visit authorizations will be validated annually by the requesting CVO to ensure that there continues to be a requirement for the individual to remain at the site. There are limitations on the type of work that can be carried out by an individual on an extended visit authorization.
7. Visits to contractor facilities relating only to unclassified or Netherlands DEPARTEMENTAAL-VERTROUWELIJK information will be arranged directly between the sending and receiving facilities, and the visitor does not require a security clearance.
8. When requested in regard to commercial entities, the authority to visit the facility of the prime contractor will include authorization to have access to or to disclose classified information at the facility of a subcontractor engaged in performance of work in connection with the same prime contract provided the subcontractor is included on the original visit request.
9. It is the responsibility of the host site to ensure that the visitor is not allowed access to information or areas for which they do not have a need to know.
10. Modifications to approved visit requests require the prior concurrence of the receiving Participant. Emergency visit requests may not be modified after approval.

16. Signatures

a) The foregoing represents the understanding between the Minister of Defence of the Kingdom of the Netherlands and the Department of Defense of the United States of America upon the matters referred to therein.
b) This Arrangement is signed in two originals in the English language.

For the Minister of Defence of the Kingdom of the Netherlands

(sd.) Major General B. Dedden

Director of the DISS

Date: 31 January 2006

For the Department of Defense of the United States of America

(sd.) BETH M. MCCORMICK

Deputy Under Secretary of Defense (TSP&NDP)

Date: 13 March 2006

D. PARLEMENT

Het Akkoord behoefde ingevolge artikel 7, onderdeel b, van de Rijkswet goedkeuring en bekendmaking verdragen niet de goedkeuring van de Staten-Generaal.

G. INWERKINGTREDING

De bepalingen van het Akkoord tot vervanging van Bijlage V bij het Memorandum van Overeenstemming zijn op 13 maart 2006 in werking getreden.

Wat betreft het Koninkrijk der Nederlanden, geldt het Akkoord, evenals het Memorandum van overeenstemming, alleen voor Nederland (het Europese deel).

Uitgegeven de *dertigste* augustus 2023.

De Minister van Buitenlandse Zaken,

W.B. HOEKSTRA

trb-2023-102-n1
ISSN 0920 - 2218
's-Gravenhage 2023