NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

13 May 2015

DOCUMENT
AC/35-D/2003-REV5

SECURITY COMMITTEE

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

Note by the Acting Chairman

1. At Annex is the fifth revision of the Directive on Classified Project and Industrial Security which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies.

2. While this revision reflects approved changes and amendments to all sections, the most significant ones are in the Section "Tendering, Negotiation and Letting of Contracts/Sub-Contracts involving classified Information" with focus on pre-contractual security requirements.

3. In addition, two new Sections have been introduced: "Facility Security Officer" and "Handling of NATO Classified Information in Communication and Information Systems (CIS)". Specific attention should also be paid to activities/scenarios involving NATO RESTRICTED Information.

4. This document has been approved by the Security Committee (SC) in Security Policy Format (SP) under the silence procedure (AC/35-WP(2011)0010-REV11 (SP) refers) and will be subject to periodic review.

5. This document replaces AC/35-D/2003-REV4 which should be destroyed.

(Signed) Marco Criscuolo

Annex: 1
15 appendices

Action officer: Rolf Ultes, NOS/POB, ext. 4680
Original: English

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

TABLE OF CONTENTS

INTRODUCTION 1-5

Scope 1-5

Authority 1-5

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS/SUB-CONTRACTS INVOLVING CLASSIFIED INFORMATION 1-6

Contracts/Sub-contracts in NATO Nations 1-6

General 1-6

Tendering Process 1-6

Access to Information Classified NATO CONFIDENTIAL or above during the Tendering Process 1-6

Access to Information classified NATO RESTRICTED during the Tender Process 1-7

Unsuccessful Bidders 1-7

Negotiations 1-7

Letting 1-8

Contracts involving NATO RESTRICTED Information 1-8

Contracts involving Information classified NATO CONFIDENTIAL or above 1-8

Programme/Project Security Instruction and Security Aspects Letter 1-8

Notification of Contracts 1-9

30. ..... Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR as detailed in Appendix 3 shall notify their NSA/DSA about any such contracts they have been awarded. 1-9

Contracts/Sub-contracts with Contractors in Non-NATO Nations 1-9

Termination of Contracts involving Classified Information 1-10

INDUSTRIAL SECURITY CLEARANCES 1-10

Facility Security Clearances 1-10

Contractor's Personnel performing work on NATO Premises or on other Contractor's Facilities 1-11

Changes to or Revocation of FSC 1-11

FACILITY SECURITY OFFICER 1-11

PERSONNEL SECURITY CLEARANCES 1-13

General Provisions 1-13

Contractual Conditions 1-13

Initiating Personnel Security Clearance Procedures 1-13
Revalidation 1-13
Procedures to be followed when a PSC is suspended or revoked 1-13
Procedures to be followed when a PSC is denied 1-14
PSC of an Employee holding the Nationality/Citizenship of another Nation 1-14
Multiple Nationalities 1-15
Provisional PSC 1-15
Verification 1-15
Security Awareness and Briefings of Individuals 1-15

PROGRAMME/PROJECT SECURITY 1-16
Introduction 1-16
Principles 1-16
Programme/Project Security Instruction 1-16

RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS 1-18
Security Arrangements for the Release of NATO Classified Information to non-NATO Nations and International Organizations 1-18
Procedures to be followed for the Release of NATO Classified Programme/Project Information to non-Programme/Project Participants from NATO Nations 1-18

HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS) 1-18
General 1-18

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs) 1-19
Requirements and Procedures for Visits 1-19

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL 1-20
General 1-20
International Hand Carriage of NATO Classified Material at NC or NS level 1-20
General 1-20
Security Arrangements 1-20
Procedure 1-20
Carriage of Material at the level NC by Commercial Courier Companies 1-21
Transportation of NATO Classified Material NC or NS as Freight 1-22
Transportation of NATO Classified Material NC or NS as Freight by Road 1-22
Transportation of NATO Classified Material NC or NS as Freight by Rail 1-23
Transportation of NATO Classified Material NC or NS as Freight by Sea 1-23

Transportation of NATO Classified Material NC or NS as Freight by Aircraft 1-24

Security Principles applicable to all Forms of Transportation 1-25

Countries presenting special Security Risks 1-25

Customs 1-25

Acknowledgement 1-25

Packaging 1-25

Security Guards and Escorts 1-25

Transportation of Explosives, Propellants or Other Dangerous Substances 1-26

GLOSSARY AND ACRONYMS 1-27

20. ..... Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded. 1-43

E-mail: ivcp@uvns.hr 1-73

The following Appendices to this Directive address the specific procedures, arrangements, and sample documents:

(a)	APPENDIX 1 -	General Responsibilities;
(b)	APPENDIX 2 -	Facility Security Clearance Information Sheet (FSCIS);
(c)	APPENDIX 3 -	Facility and Personnel Security Clearance for Contracts involving NATO RESTRICTED Information - National requirements;
(d)	APPENDIX 4 -	Contract Security Clause for Inclusion in Tenders and Contracts involving NATO RESTRICTED Information;
(e)	APPENDIX 5 -	Security Aspects Letter (SAL);
(f)	APPENDIX 6 -	Project Security Instructions (PSIs) - Structure and Content;
(g)	APPENDIX 7 -	Facilities/Organisations List;
(h)	APPENDIX 8 -	International Visits Control Procedures (IVCPs);
(i)	APPENDIX 9 -	International Visits Processing Times/Lead Times and NU or NR notification requirements;
(j)	APPENDIX 10 -	Security Acknowledgement (in case of Hand Carriage) - Declaration;
(k)	APPENDIX 11 -	Courier Certificate for the International Hand Carriage of classified Documents, Equipment and/or Components;
(l)	APPENDIX 12 -	International Transportation Plan - Transportation Plan for the Movement of Classified Consignments;
(m)	APPENDIX 13 -	Authorisation for Security Guards;
(n)	APPENDIX 14 -	NATO Personnel Security Clearance Certificate (PSCC);
(o)	APPENDIX 15 -	Attestation of a NATO Personnel Security Clearance (APSC).

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

1. Industrial security is the application of protective measures and procedures to prevent, detect and recover from loss or compromise of classified information handled by industry in contracts. NATO classified information disseminated to industry, generated as a result of a contract with industry, and contracts involving classified information with industry shall be protected to a standard no less stringent than NATO Security Policy (C-M(2002)49) and supporting Directives.

2. This Directive is published by the Security Committee (SC) pursuant to paragraph 5.7 of Enclosure "B" and in support of Enclosure "G" to the NATO Security Policy (C-M(2002)49).

3. This Directive contains mandatory minimum standards, common procedures and processes in connection with the implementation of industrial security.

Scope

4. This Directive applies to the protection of NATO classified information released or created during all phases of the contracting processes, including licensing, bidding, negotiation, award, performance, and termination. The protection of NATO UNCLASSIFIED information is governed by C-M(2002)60, The Management of Non-Classified Information, and is addressed in this Directive only if required for consistency.

5. The provisions outlined in this Directive are applicable to NATO, NATO Programme/Project Agency/Offices (NPA/NPOs), National Security Authorities (NSA), Designated Security Authorities (DSA), National Security Accreditation Authorities (SAAs) and any other competent national authorities that let contracts involving NATO classified information to Contractors. The following definitions apply:

Contracting Authority:
An organization in NATO or NATO nations including Contractors authorised to tender for, or place a contract with a Contractor or Consultant.

Contractor:
An industrial, commercial or other entity that seeks or agrees to provide goods or services.

Consultant:
An individual who serves either independently or through a Contractor in an advisory capacity. A Consultant expresses views, gives opinions on problems, answers questions as requested or provides advice. The work performed under contract is the provision of advice. Therefore, for the purpose of this Directive, a Consultant is considered the same as a Contractor. Hereafter, referred to as Contractor.

Authority

6. The NSAs/DSAs/SAAs are responsible for the implementation and oversight of security for NATO classified information entrusted to their Contractors. The NSAs/DSAs/SAAs shall ensure that they have the means to make their security requirements binding upon Contractors and that they have the right to inspect and approve the measures taken by Contractors in compliance with this Directive for the protection of NATO classified information.

7. Detailed responsibilities of the NSAs/DSAs, the SC, the NATO Office of Security (NOS), and NPA/NPOs are laid down in Appendix 1. Principle organisations with responsibility for CIS security, e.g. SAAs are addressed in Enclosure "F".

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS/SUB-CONTRACTS INVOLVING CLASSIFIED INFORMATION

Contracts/Sub-contracts in NATO Nations

General

8. All Contractors/Sub-contractors undertaking a NATO contract involving classified information requiring access to, or generation of information classified NATO CONFIDENTIAL (NC) or above shall hold or, in respect of paragraph 11 (b) and (c) below, be able to obtain a Facility Security Clearance (FSC) at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction[1] over the Contractor/Sub-contractor's facility. It is the responsibility of the Contracting Authority to verify with the relevant NSA/DSA of a Contractor/Sub-contractor whether it has been granted an appropriate FSC before any NC or above information is released to it. Where no FSC at the required level exist it is the responsibility of the Contracting Authority to initiate an FSC or upgrade action.

9. A FSC is not required by Enclosure G to C-M(2002)49 for access to, or generation of classified information at level of NATO RESTRICTED (NR). However some NATO nations, as identified in Appendix 3, and as mandated by their national laws and regulations, do require a FSC for Contractor/Sub-contractor under their jurisdiction, for access to classified information at the level of NR.

Tendering Process

Access to Information Classified NATO CONFIDENTIAL or above during the Tendering Process

10. A bidder, not holding an appropriate FSC as required by the potential contract/sub-contract shall not be automatically excluded from the competition during the tendering process, as detailed in the scenarios below.

11. The following identifies the three scenarios that may arise during the tendering process for a contract/sub-contract involving classified information NC or above and details the security requirements:

(a) access to classified information NC or above at the bidder's facility during the tendering process:

- when the contract notice, invitation to tender or request for proposals require bidders to hold or generate at their facility information classified NC or above, the bidder's facility shall hold an FSC at the appropriate level. In such circumstances the Contracting Authority shall obtain an assurance from the relevant NSA/DSA that the bidder has been granted an appropriate FSC;
- the Contracting Authority shall obtain the respective assurance from the responsible NSA/DSA by using the Facility Security Clearance Information Sheet (FSCIS) at Appendix 2.

(b) no access to information classified NC or above during the tendering process:

- when the contract/sub-contract notice, invitation to tender or request for proposal concerns a contract/sub-contract that will involve classified information NC or above but does not require the bidder to hold or originate such information at the tender stage, a bidder not holding an appropriate FSC shall not be excluded from the bidding process, but should be advised in the tender document that an FSC shall be required prior to it being awarded the contract/sub-contract;

[1] Power to exercise authority over a subject matter or a territory/geographic area

- should a bidder without an appropriate FSC be selected to undertake the contract/sub-contract, the Contracting Authority shall initiate action to grant the bidder an FSC at the required level;
- the contract/sub-contract shall not be awarded until the NSA/DSA has provided an assurance that the selected bidder's facility has been granted an FSC at the required level. The Contracting Authority shall initiate the FSC action by using the FSCIS at Appendix 2.

(c) access to information classified NC or above at the premises of the contracting authorities during the tendering process:

- shall only be granted to individuals who are in the possession of an appropriate Personnel Security Clearance (PSC). An assurance of the PSC of individuals requiring access on the premises of the Contracting Authority shall be provided in the form of a PSC Certificate or a Request for Visit by the appropriate NSA/DSA;
- should a bidder without an appropriate FSC be selected to undertake the contract/sub-contract, the Contracting Authority shall request the relevant NSA/DSA to initiate action to grant the bidder an FSC at the required level;
- the contract/sub-contract shall not be awarded until the NSA/DSA has provided an assurance that the selected bidder's facility has been granted an FSC at the required level. The Contracting Authority shall request the responsible NSA/DSA to initiate the FSC action by using the FSCIS at Appendix 2.

12. Should the NSA/DSA determine that a bidder is ineligible for the required level of FSC the Contracting Authority shall not award the contract.

Access to Information classified NATO RESTRICTED during the Tender Process

13. When the contract notice, invitation to tender or request for proposals require bidders to hold or generate NR information, the contract notice, the invitation to tender or request for proposal shall include a copy of the "Contract Security Clause for Inclusion in Tenders and Contracts Involving NR Information" at Appendix 4. This will inform the bidder on the minimum measures required for the protection of NR classified information.

Unsuccessful Bidders

14. Unsuccessful bidders having been provided NATO classified information in connection with a tender shall be required to return the classified information to the Contracting Authority within 15 working days of receipt of notification of their unsuccessful tender. All individuals having accessed NATO classified information shall be reminded of their responsibility for its protection and of not disclosing such information further.

Negotiations

15. Following the tendering process and at the start of the negotiations for contracts involving NC or above with preferred bidders, if not already confirmed, an assurance shall be obtained that the potential Contractor(s) hold(s) an FSC at the required level. If the Contracting Authority is a NATO civil and military body the request shall be forwarded to the NSA/DSA of the nation with jurisdiction over the potential Contractor(s). If the Contracting Authority is in a NATO nation, the request shall be forwarded to its responsible NSA/DSA. The Contracting Authority shall ensure that all Contractors are required to follow the same approval process when negotiating a sub-contract.

16. In case the potential Contractor does not hold the required FSC, the responsible NSA/DSA shall be requested to initiate the clearance procedure accordingly. For such purposes the FSCIS at Appendix 2 shall be used.

17. The Contracting Authority shall also provide information regarding the classification level to the responsible NSA/DSA and the nature of services or supplies requiring access or potential access to NATO classified information in order to allow the responsible NSA/DSA to ensure the necessary security arrangements have been implemented.

Letting

18. Contracting authorities will not normally award a contract involving classified information NC or above before having obtained assurance that the Contractor's facility holds an FSC at the required level. Exceptionally and after consulting with the relevant NSA/DSA, the Contracting Authority may allow the Contractor to commence work on the NR parts of the contract provided the contractual arrangement includes a clause stating that the contract shall be terminated in case the Contractor cannot be granted the required FSC.

Contracts involving NATO RESTRICTED Information

19. Contracts involving classified information at the level of NR shall include a "Contract Security Clause for Tenders and Contracts Involving NR Information" detailing, as a minimum, the provisions specified in Appendix 4. Such contracts shall also include a Security Aspects Letter (SAL) (see Appendix 5) identifying the specific NR aspects of the contract requiring protection.

20. The requirements in contracts for the protection of NR information may be more stringent than that detailed in Appendix 4 and, if required by national laws and regulations, NSAs/DSAs will be responsible for ensuring compliance of Contractors/Sub-contractors being under their jurisdiction with applicable security provisions for the protection of NR information and should conduct verification visits on Contractor's facilities located in their nation. In all other cases it is the responsibility of the Contracting Authority to ensure that the required security provisions of Appendix 4 and the SAL, as applicable, are implemented. Any incident, which has or may lead to NR information being lost or compromised, shall immediately be reported by the SO to the Contracting Authority, which shall inform the competent NATO body or the Contractor's NSA/DSA, as applicable.

Contracts involving Information classified NATO CONFIDENTIAL or above

21. Contracts/sub-contracts involving access to information classified NC or above shall include an article/paragraph, which requires the Contractor/Sub-contractor to protect any such classified information no less stringently than applicable NATO security regulations as implemented by its competent NSA/DSA, and comply with any relevant national security laws and regulations and any additional instructions given by the responsible NSA/DSA. Contract specific NATO security requirements shall be given either in a Programme Security Instruction (PSI) (see Appendix 6) or in a SAL, as appropriate.

Performance of Contracts within Class II Security Areas

22. In accordance with AC/35-D/2001, Directive on Physical Security, unescorted access to Class II Security Areas shall only be granted to individuals who are security cleared. For all other individuals, provisions shall be made for escorts or equivalent controls to prevent unauthorised access to NATO classified information. If escort arrangements or equivalent controls are not feasible, the requirement for individuals to hold an appropriate PSC when the execution of the contract starts shall be clearly stated in the invitation to bid.

Programme/Project Security Instruction and Security Aspects Letter

23. For all programmes involving classified information NC or above managed by an NPA/NPO, the programme security office shall produce a PSI (see Appendix 6) in collaboration with and subject to approval by the NSA/DSA of the NATO nation(s) participating in the programme. PSIs may be produced for other activities if considered necessary by the appropriate security authorities. Security classifications shall be addressed in the Security

Classification Guide (SCG). If considered appropriate by the NPA/NPO and programme participants a PSI may also be produced for programmes involving only classified information at the NR level.

24. Contracts which do not require a PSI shall include as a minimum an SAL. In that case security classifications shall be addressed in a Security Classification Checklist.

25. The PSI and/or SAL shall be made binding for all participants.

Notification of Contracts

26. NATO contracting authorities shall notify, via their respective security officers, the NSA/DSA of the nation with jurisdiction over the Contractor about any contracts involving classified information at the level of NC or above, to include details on the nature of services or supplies or work to be performed by the Contractor, the security classification, the nature and volume of classified information to be furnished to or to be generated by the Contractor as well as any other relevant security aspects.

27. Each NPA/NPO shall develop and maintain an up-to-date list of facilities and involved organisations. The list shall be in the format at Appendix 7 and be available to all NSAs/DSAs and NATO civil and military bodies upon request. The list consists of:

(a) the prime Contractors that hold contracts involving classified information NC or above connected with the NATO project/programme;

(b) all government departments or agencies known to be involved in the project/programme; and

(c) any civil or military body involved, when applicable.

28. Each NPA/NPO shall also be responsible for requiring that each prime Contractor maintains a similar list for any Sub-contractors, by project, with access to information classified NC or above.

29. Other contracting authorities awarding a NATO classified prime contract involving classified information at the level of NC or above, shall provide their NSA/DSA with a copy of the security provisions of the contract and the PSI/SAL. That NSA/DSA shall provide copies of the security provisions and PSI/SAL to the NSA/DSA of the country with jurisdiction over the Contractor so that security oversight of the classified information can be maintained.

30. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR as detailed in Appendix 3 shall notify their NSA/DSA about any such contracts they have been awarded.

Contracts/Sub-contracts with Contractors in Non-NATO Nations

31. The letting of the contract involving NATO classified information to Contractors in non-NATO nations constitutes a release of information and has to be in accordance with the established procedures as referenced in paragraph 91.

32. Contracts/sub-contracts with Contractors/Sub-contractors in non-NATO nations which involve NATO classified information require the existence of a bilateral Security Agreement/Arrangement between NATO and the non-NATO nation whose NSA/DSA has jurisdiction over the Contractors/Sub-contractors. It is the responsibility of that NSA/DSA to ensure their Contractors/Sub-contractors provide the required level of protection for the contract involving NATO classified information.

33. If there is no bilateral Security Agreement/Arrangement between NATO and the non-NATO nation, a bilateral Security Agreement/Arrangement between

a contracting/sponsoring NATO Nation and the non-NATO Nation is required. The NATO Nation shall provide a written Security Assurance signed by a representative duly mandated by the Non-NATO recipient, to NATO. The Security Assurance shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement/Arrangement for the protection of the NATO nation's classified information of an equivalent classification.

34. If the NATO Nation which has concluded the Security Agreement/Arrangement with the Non-NATO Nation does not have the jurisdiction over the Contracting Authority, the NSA/DSA of the NATO Nation with jurisdiction over the Contracting Authority must be provided with the Security Assurance as detailed in paragraph 33 above and a copy of the Security Agreement/Arrangement. The written consent of the NATO Nation with jurisdiction over the Contracting Authority is required otherwise the contract shall not be placed.

35. Placing contracts/sub-contracts involving classified NATO information shall follow the procedures as established in paragraphs 8 to 30 above.

Termination of Contracts involving Classified Information

36. Upon termination of a contract/sub-contract involving classified information, and where classified information has been provided to or generated by the Contractor/Sub-contractor during the performance of the contract, the classified information shall be returned to the Contracting Authority unless the Contracting Authority has agreed in writing that the classified information can be destroyed in accordance with the national laws and regulations or retained by the Contractor/Sub-contractor, e.g. for purposes of follow-on services or supplies. Disposition instructions shall be included in any contracts involving access to NC and higher.

INDUSTRIAL SECURITY CLEARANCES

Facility Security Clearances

37. The NSA/DSA of each NATO nation is responsible for granting an appropriate FSC for Contractor's facilities under their jurisdiction and which are involved in NATO contracts involving classified information at NC or above level, in accordance with national laws and regulations. Prior to granting an FSC, an assessment shall be made on the following mandatory minimum requirements:

(a) of the integrity and probity of the company which is to be entrusted with NATO classified information at the level of NC or above;

(b) of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other individuals as per national laws and regulations who may, by virtue of their association, position or employment, be required to have access to NATO classified information or supervise a NATO contract involving classified information, to ensure that they have the requisite level of PSC;

(c) of the foreign ownership, control and influence aspects (such as corporate structure) to ensure that these aspects are adequately addressed and where necessary mitigated; and

(d) of the security arrangements provided for the protection of NATO classified information to ensure that they comply with the requirements of NATO Security Policy and its supporting directives.

38. An FSC is an administrative determination by which an NSA/DSA formally recognizes the capacity or reliability of Contractor's facilities to manage, generate or have access to classified information up to a certain level. Depending on the contract requirements and, subject to national laws and regulations, there may be different types of FSCs, as determined by the NSA/DSA and are conveyed in the NATO FSCIS.

39. The following minimum criteria shall be applied by the NSA/DSA in issuing all categories of FSCs:

(a) that the company must establish security processes which covers all appropriate security requirements for the protection of information classified at NC or above in accordance with NATO security regulations;

(b) that the personnel security status of personnel (both management and employees) who are required to have access to information classified at NC or above is confirmed in accordance with NATO personnel security clearance requirements;

(c) that the NSA/DSA has the means to ensure that the industrial security requirements are binding upon industry and that it has the right to inspect and approve the measures taken in industry for the protection of information classified at NC and above; and

(d) that the company shall appoint a Facility Security Officer (FSO) responsible for security who is in a position to report to the NSA/DSA.

40. In granting an FSC, NSAs/DSAs shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted (e.g. a transfer of the controlling interests in the company or facility, a realignment of the business associations, the replacement of any of its principal officers or directors, a change in the facility's physical location, an alteration to the premises it occupies, or a variation in its security procedures).

41. The NSAs/DSAs shall evaluate the extent to which the circumstances described above represent a threat to the security of NATO classified information that may be entrusted to that company or facility. If it is determined that there is a threat, the NSAs/DSAs will take appropriate steps to negate or mitigate the threat prior to issuing or maintaining the FSC.

42. The responsible NSA/DSA shall confirm the level of the FSC granted to, or initiate facility clearance action for a company, when requested, in the FSCIS format (Appendix 2).

43. The NSA/DSA may specify additional security measures to be taken for the protection of NATO classified information in each company/facility in its nation in order to qualify for an FSC.

Contractor's Personnel performing work on NATO Premises or on other Contractor's Facilities

44. Contractor/Sub-contractor's personnel, including freelance consultants and interpreters, or any other type of freelance personnel or self-employed service providers who carry out works on NATO premises or Contractor's facilities in connection with a classified NATO programme/project or any other type of NATO contract requiring access to information classified NC or above shall hold a PSC at the requisite level and, if required by national laws and regulations, an appropriate FSC.

Changes to or Revocation of FSC

45. Should an NSA/DSA change or withdraw an FSC that it has issued, the NSA/DSA shall at once notify any other NSA/DSA and/or NPA/NPO to which it has provided a clearance notification. The contractual arrangement shall include a clause allowing for the termination of the contract in case of the revocation of the required FSC.

FACILITY SECURITY OFFICER

46. A FSO shall be in place for a Contractor/Sub-contractor to be granted an FSC. The FSO will be responsible for the overall protection of NATO classified information and obliged to ensure the effective implementation of security requirements and procedures within the facility involved in any contract/sub-contract requiring access to NATO classified information.

47. The FSO shall, in accordance with national laws and regulations, serve as the main point of contact between the Contractor/Sub-contractor and the Contracting Authority or relevant NSA/DSA for all security related aspects. When appointing the FSO, the following requirements apply:

(a) the FSO shall be:
- a citizen of the nation where the facility is located, or a citizen of a NATO nation *(for contracts involving classified information NC and above);*
- an employee of the Contractor/Sub-contractor;
- granted a PSC at the appropriate level;
- a part of the facility's management, or reporting directly to one of the members of the management in order to exercise security authority;

(b) the FSO shall undertake appropriate briefing and/or training regarding protective security and threat awareness;

(c) the responsible NSA/DSA should endeavour to create and maintain a close cooperation with the FSO.

48. The FSO is responsible for the following tasks:

(a) establishing and maintaining a system of procedures and measures for the protection of NATO classified information. These measures must ensure that all security requirements specified for personnel security, physical security, security of information and CIS security (CISS) are adhered to and are in place throughout the lifetime of the classified project/contract;

(b) reporting to the responsible NSA/DSA any circumstances that may have an impact on the status of the FSC (e.g. changes in the ownership or key management personnel, changes in personnel who are involved in the classified project, changes to physical security, security of information and CISS, etc.), or PSCs (e.g. changes to or other circumstances which necessitate revalidation or which may adversely affect the individual's loyalty, reliability and trustworthiness, etc);

(c) reporting to the responsible NSA/DSA any suspected espionage, sabotage or subversive activities at the facility, including any indication of loss, compromise or suspected compromise of NATO classified information and any other security risks concerning NATO classified information;

(d) providing initial security briefings to new employees, and to all cleared persons before they are given access to NATO classified information. Providing periodic security training and security awareness programs for all personnel as required and conduct debriefings with individuals who are terminating employment on their continuing responsibilities concerning the safeguarding of NATO classified information they have accessed;

(e) conducting periodic security spot-checks or inventories as required of their facility;

(f) initiating a preliminary enquiry to ascertain the circumstances of any security violation, submit an initial investigation report of the security incident and final report including the corrective actions taken to the responsible NSA/DSA;

(g) cooperating in security inspections and investigations undertaken by the responsible NSA/DSA for assessing the protection of NATO classified information and assist in personnel security investigations of current or former employees; complying with any procedure that is, or may be, established by the NSA/DSA regarding the safeguarding and release of NATO classified information related to the contract/sub-contract.

PERSONNEL SECURITY CLEARANCES

General Provisions

49. All individuals (e.g. Contractors/Sub-contractor's personnel, including freelance consultants, interpreters, or any other type of freelance personnel or self-employed service providers) who require access to, or whose duties or functions may afford access to information classified NC or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know. Typical categories of personnel being subject to the security clearance procedure, in relation to the issuing of an FSC, are:

(a) owners of companies, members of supervisory boards and members of management's boards who may be subject to the personnel security clearance process in accordance with requirements in national laws and regulations;

(b) FSOs, CIS Security staff, registry staff, couriers and subject matter experts of a company may be subject to the personnel security clearance process as required for the fulfilment of the contract involving NATO classified information.

50. A PSC is not required for access to NR information; individuals shall have a need-to-know, shall be briefed about their responsibilities for the protection of NR information and shall acknowledge in writing that they fully understand their responsibilities.

51. Personnel security is addressed further at Enclosure "C" to the NATO Security Policy (C-M(2002)49) and in the supporting Directive on Personnel Security (AC/35-D/2000).

Contractual Conditions

52. Before letting a sub-contract involving information classified NC or above the Contractor shall contact its responsible NSA/DSA to ensure that Sub-contractor's facility and personnel requiring access to NATO information classified NC or above fulfil the requirements of this Directive.

Initiating Personnel Security Clearance Procedures

53. The FSO shall request each individual requiring access to NATO classified information NC and above to complete the respective national PSC questionnaire and forward the completed form to his/her responsible NSA/DSA.

Revalidation

54. The FSO is responsible to ensure the timely processing of a request for revalidation of the employee's PSC with the responsible NSA/DSA.

55. If a NATO PSC is not revalidated within the life of the clearance, a period of a further 12 months may be allowed for the revalidation to be completed, provided that the responsible NSA/DSA has commenced the action necessary to revalidate the clearance.

56. If, at the end of this additional 12-month period, the revalidation has still not been completed, the individual shall not have access to NATO classified information NC and above.

Procedures to be followed when a PSC is suspended or revoked

57. If the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor learns adverse information about an individual who is a national of another NATO nation, it shall immediately inform the NSA/DSA of the individual's country of citizenship in order to determine whether the individual shall continue to hold a PSC.

58. In the case where the NSA/DSA of the country of citizenship of an individual who is employed in another NATO nation decides to suspend or revoke the individual's security clearance, it shall immediately inform the NSA/DSA of the nation of origin of the facility that requested the PSC.

59. If an employee's security clearance has been suspended or revoked, the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor shall inform the facility where the individual is employed and vice versa. Other NSAs/DSAs to whom clearance verification has been provided shall be notified of the suspension or revocation.

60. On receiving the information that a PSC has been suspended or revoked, the FSO of the facility/Security Officer of the NATO civil and military body, which employs the individual, shall ensure that the individual is denied access to classified information NC or above and debriefed.

Procedures to be followed when a PSC is denied

61. The NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor shall inform the facility where the individual is employed of the denial of a PSC. If other NSAs/DSAs have been involved in the PSC process they shall also be notified of the denial of the issuing of the clearance.

62. Should the NSA/DSA of a parent nation of an individual decide not to grant a PSC it will immediately inform the NSA/DSA of the nation which has jurisdiction over the facility that requested the PSC.

63. Equally, should the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor that requested the PSC decides not to grant it, it will immediately inform the NSA/DSA of the individual's country of citizenship.

64. On receiving the information that a PSC has been denied, the facility/NATO body which employs the individual shall ensure that they are not involved in classified work at the level of NC or above.

PSC of an Employee holding the Nationality/Citizenship of another Nation

65. If a PSC is required for a Contractor's/Sub-contractor's employee whose nationality/citizenship is that of another NATO nation, the NSA/DSA of the nation which has jurisdiction over the Contractor shall obtain a PSC or assurance from the employee's country of nationality/citizenship.

66. As an alternative, having the character of subsidiarity, the NSA/DSA of the nation which has jurisdiction over the Contractor may, where permitted by national laws and regulations, grant a PSC to an employee holding the nationality/citizenship of another NATO nation provided that:

(a) the employee has resided in the Contractor's country for at least 5 consecutive years;

(b) the NSA/DSA of the nation which has jurisdiction over the Contractor have checked their appropriate records to ensure that there is no adverse information;

(c) the material and information concerned with the contract is not at the COSMIC TOP SECRET (CTS) level; and

(d) an assurance is requested from the NSA/DSA of the employee's country of citizenship that there is no adverse information in respect to the individual that would prevent the granting of a NATO PSC by the parent nation.

67. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO classified information up to and including NATO SECRET (NS), it is the responsibility of the NSA/DSA of the nation which has jurisdiction over the hiring facility to

determine the suitability of the individual for accessing NATO classified information in accordance with the Directive on Personnel Security.

Multiple Nationalities

68. For individuals holding multiple nationalities, where appropriate, the host nation granting the PSC should obtain assurances on the individuals' suitability to be granted a PSC from the other nations, subject to the host nation's security policy.

Provisional PSC

69. The NSA/DSA may issue a provisional PSC in accordance with its national laws and regulations. The period of validity of such a PSC and its level shall be determined and notified by the issuing NSA/DSA.

70. In exceptional cases, where the attainment of major operational objectives would otherwise be seriously impaired, and it is not possible to obtain the clearance in time by prioritising a particular request, access may be permitted following the procedures set out in the Directive on Personnel Security(AC/35-D/2000). However, such access may be permitted only with the prior approval of the originator, be limited only for citizens of NATO nations, and in connection with contracts requiring access to classified information not higher than NS.

Verification

71. The verification that the individual has a valid PSC may either be in the form of request for visit (RFV) (Appendix B to Attachment 1 of Appendix 8), in the form of the NATO Personnel Security Clearance Certificate (PSCC) (Appendix 14) or in the form of an Attestation of NATO Personnel Security Clearance (APSC) (Appendix 15).

Security Awareness and Briefings of Individuals

72. All individuals employed in positions where they have access to NATO classified information, shall be briefed on security procedures and their security obligations. All individuals having access to NATO classified information shall acknowledge that they fully understand their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the FSO.

73. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

74. All individuals who cease to be employed in duties requiring access to NATO classified information shall be made aware of, and acknowledge, their responsibilities for the continued safeguarding of NATO classified information.

75. Additional guidance can be obtained from Guidelines on Security Education and Awareness AC/35-D/1029.

PROGRAMME/PROJECT SECURITY

Introduction

76. Where established, the NPA/NPO is responsible for managing project security for major NATO programmes/projects or procurement activities. The security risks related to the operational, technological, political and commercial sensitivities of the project must be considered, and although these risks are managed on their behalf by the NPA/NPO, individual programme participants (the security stakeholders) must be made aware of the security risks.

77. At the start of a programme/project it is important to define the process required to ensure effective management of security throughout the activity, primarily by identifying and recording the relevant security sensitivities and identifying the appropriate protection in a PSI. All participants are responsible for the implementation of the PSI. It is also important to ensure that the security requirements for the programme/project are kept up to date during the entire life of the programme/project.

78. The allocation of a NATO classification indicates the required level of protective security to be provided to material or information associated with the NATO programme/project and the expected impact or damage as a consequence of loss or compromise associated with programme material and information. However, the classification alone does not prevent the release of information to other trusted nations, subject to an appropriate release process. Although material generated under the programme/project shall receive a NATO classification it should be recognised that the release authority remains with the programme/project participants, even for releases to other NATO nations.

Principles

79. Security measures are established to deter, detect and prevent the compromise of information and protect its confidentiality, integrity and availability. Within project security, it is important to recognise that such security measures are not only required for the technological aspects of the material, but also aspects such as how the material is to be used, where it will be used, details of the acquisition programme (e.g. prices, dates, quantities, etc.), and consideration of the need for associated specific information/data (e.g. mission plans, intelligence data libraries) or material (e.g. specific radios for interoperability). When considering the security risks to the programme/project, attention needs to be given to any operational, technological, commercial and political risks. Programme/project security must be the result of a team effort involving program management, and support personnel from disciplines such as technical, intelligence, security, and foreign disclosure.

80. Following determination of the threats and vulnerabilities associated with the programme/project, security is achieved by:

(a) classification of information. The classification markings applied are appropriate to the state of development of the programme/project. The preparation of a SCG requires collaboration amongst the programme/project technical staff and security professionals. The SCG is one of the most important tools in preparing the other programme/project related security documents;

(b) need-to-know. This principle is to be adhered to by all personnel involved in the programme/project; and

(c) the applicable security protection of a programme/project should be reviewed regularly or at each programme/project approvals milestone to ensure consistency and effectiveness.

Programme/Project Security Instruction

81. For all programmes/projects managed by NPA/NPO involving information classified NC or above, a PSI shall be developed utilising the template at Appendix 6. The purpose of the PSI is to supplement the security policies and requirements detailed in C-M(2002)49, and its supporting

Directives. It must establish specific security procedures associated with the NATO programme/project concerned and assign responsibilities for the implementation of security measures concerning classified information generated and exchanged under the development, production and follow-on support of the NATO programme/project. If considered appropriate by the NPA/NPO and programme participants a PSI may also be produced for programmes involving only classified information at the NR level.

82. The PSI also may include marking and handling instructions for unclassified information.

83. The PSI shall be developed by the NPA/NPO in conjunction with the NSAs/DSAs and technical staff of the programme participating NATO nations. It shall include an SCG which must identify the security sensitivities and security classification of the aspects related to the programme.

84. The PSI shall apply to all military and civilian establishments and as described below to Contractors/Sub-contractors and their personnel involved in the programme/project. Prime Contractors participating in the programme/project shall be provided with the complete PSI, which shall be made binding through appropriate contractual language. For Sub-contractors the complete PSI shall be provided if appropriate or alternatively only the relevant provisions of the PSI shall be provided and made binding through appropriate contractual language.

85. The following general principles shall be observed in connection with the security classification requirements of NATO contracts involving classified information (prime and sub):

(a) the assignment of security classifications to background information shall be the responsibility of the originator of the classified information; the classification of foreground information is a mutual responsibility of the participants in the programme/project;

(b) security classifications shall be applied only to those aspects of a programme/project that must be protected, and the level of such classifications must be strictly related to the degree of protection required;

(c) the classification of a compilation of information from more than one source shall be co-ordinated among the sources to determine the appropriate NATO security classification;

(d) information shall be declassified or downgraded as soon as appropriate; and

(e) the originator will approve any change of the classification level of background information. Changes to the classification of foreground information shall be co-ordinated among the participants.

86. The responsibility for applying a security classification to elements of a programme/project dealing with a product wherein all elements are clearly defined and their classification pre-determined, rests with the NPA/NPO of the contract, acting in collaboration with the NSAs/DSAs of the participating NATO nations.

87. The programme/project SCG should be developed in close co-operation with industry participating in the programme/project. A “Security Classification Board” may be established to assist in the preparation of classification guidance. Such Boards should be comprised of appropriate representatives of the NSAs/DSAs of the participating nations and the NPA/NPO, and advised by the participating prime Contractor(s).

88. The initial assessment that information should be classified, which was not previously identified for classification in a programme/project, may be made by the Contractor having system design responsibility. In such case, the Contractor shall recommend that the NPA/NPO take appropriate classification action. However, the decision to classify information ultimately is

the responsibility of the participating NSAs/DSAs or other designated classification authority. These decisions will be codified in the programme/project SCG.

89. In the absence of clearly defined classification guidance, any participant in the programme/project may forward a classification proposal to the responsible NPA/NPO regarding interim classification. The NPA/NPO shall review the proposed classification guidance, consult with the NSAs/DSAs, and, if agreed, update the programme/project SCG.

90. The PSI and SCG are to be approved by the responsible NSA/DSA and issued and maintained by the NPA/NPO. The PSI and SCG are to be reviewed regularly and amended as necessary in consultation with the programme/project NSAs/DSAs so that any sensitivities relating to the programme are identified and managed to ensure that the most appropriate degree of programme/equipment security is afforded throughout the programme, including during disposal.

RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS

Security Arrangements for the Release of NATO Classified Information to non-NATO Nations and International Organizations

91. Enclosure "E" to C-M(2002)49 NATO Security Policy sets out the principles for authorizing the release of NATO classified information to non-NATO nations and international organizations, and the release authority conditions. AC/35-D/2002 “Directive on Security of Information” addresses the specific procedures and arrangements.

Procedures to be followed for the Release of NATO Classified Programme/Project Information to non-Programme/Project Participants from NATO Nations

92. The release of NATO classified information to non-programme/project participants from NATO nations during the course of a programme/project shall be coordinated by the NPA/NPO and permitted only with the approval of the programme/project participants. These release procedures shall be fully detailed in the PSI.

HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

General

93. Only appropriately security accredited CIS (including stand-alone work stations) shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO classified information.

94. CIS used within national industrial facilities to handle NATO classified information shall be accredited by the respective national Security Accreditation Authorities or their delegated SAAs ensuring that the NATO’s minimum security standards, as described in the policy on Security Within the NATO and its supporting Directives on CIS Security, are met for the handling of NATO classified information.

95. For security accreditation of CIS handling NATO’s classified information, whose components are under different jurisdictional domains (e.g. different SAAs), all SAAs having a legitimate interest in the security of the CIS shall take part in the security accreditation process.

96. The security accreditation of CIS handling NR information may be delegated to Contractors according to national laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate,

the security authority as established in Appendix III of this Directive, with a statement of compliance certifying that the CIS handling NR information has been accredited in compliance with the policy on Security within the NATO and its supporting Directives on CIS Security.

97. Interconnection of industrial facilities' classified CIS to NATO CIS shall be jointly accredited by the respective national and NATO SAAs. The appropriate security arrangements shall be in place to ensure that the SAAs and the different CIS Providers of the interconnected CIS are bound by the requirement to protect NATO information.

98. Where required, the capability for handling NATO classified information in CIS shall be reflected in the Facility Security Clearance Information Sheet (FSCIS – Appendix 2).

99. Enclosure "F" to C-M(2002)49, the "Primary Directive on CIS Security" (AC/35-D/2004), the "INFOSEC Management Directive for CIS" (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO classified information.

100. For further guidance the national Security Accreditation Authority (SAA) shall be consulted.

Security Accreditation Process

101. The security accreditation process shall determine the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and system assets, during the process of establishing the security requirements. The security accreditation process, shall determine that an adequate level of protection has been achieved, and is being maintained. The security accreditation process shall be carried out in accordance with the requirements of the INFOSEC Management Directive for CIS.

Security-related Documentation

102. Security-related documentation shall be established in accordance with the requirements of the INFOSEC Management Directive for CIS and the SAA requirements for a specific CIS. Security-related documentation shall be required throughout the system life cycle, from the planning stage until the disposal stage. The security-related documentation (for example, System-specific Security Requirement Statements (SSRS) and Security Operating Procedures (SecOPs)) shall be developed in an iterative process throughout the system life cycle.

Interconnection of CIS

103. The policy on Security within the North Atlantic Treaty Organisation and its supporting directives on CIS Security require security measures to control the interconnection of CIS handling NATO classified information. The supporting INFOSEC Management Directive for CIS sets out the security accreditation requirements and the supporting CIS Security Technical and Implementation Directives (AC/322 documents) set out the measures to be implemented.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs)

Requirements and Procedures for Visits

104. Procedures for visit requests are formalised in the standard Request for Visit (RFV) procedure as established at Appendix 8. Lead times for the handling of the requests are laid down in Appendix 9.

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

General

105. The international transmission of NATO classified information up to and including NS shall be as set out in the Directive on Security of Information (AC/35-D/2002). Electronic transmission of NATO classified information shall be in accordance with the requirements of Enclosure “F” of NATO Security Policy and its supporting Directives. Information classified at the COSMIC TOP SECRET (CTS) level shall be transmitted by diplomatic pouch or military courier. International hand carriage of CTS is prohibited.

106. Information classified up to and including NS that cannot be transmitted by one of the foregoing methods and relates to contracts, may be transmitted by other means in accordance with the relevant provisions below.

International Hand Carriage of NATO Classified Material at NC or NS level

General

107. When transmission through the channels specified in the Directive on the Security of Information will result in an unacceptable delay that will adversely affect performance of the programme, project, or contract, and when it has been verified that the information is not available at the intended destination, the procedure of personal hand carriage may be permitted, provided the following provisions are complied with:

(a) the courier shall hold a PSC at appropriate level. Commercial courier companies shall not be used except as permitted at paragraph 115 below;

(b) in exceptional circumstances, the NSA/DSA of the dispatching facility may, with the previous agreement of the NSA/DSA of the receiving facility, consider issuing a Courier Certificate to an employee with the appropriate PSC who is assigned to the receiving facility, and to whose NATO nation the release of the classified material relating to the programme/contract has been authorised.

Security Arrangements

108. The hand carriage of NATO classified material will comply with the provisions of Enclosure “E” of NATO Security Policy and the supporting Directive on the Security of Information. In addition, the material must have been authorised by the originating government for release in conjunction with the project, programme or contract.

109. The courier shall be briefed by the FSO before departure on all the security measures to be implemented and shall sign the Security Acknowledgment at Appendix 10.

110. The courier shall be responsible for the safe custody of the NATO classified material until such time that it has been handed over to the consignee’s FSO. In the event of a breach of security or loss of classified information, the consignor's NSA/DSA may request the authorities in the country (i.e. a NATO nation or non-NATO nation with a Security Agreement/Arrangement with NATO or a NATO nation) in which the breach or loss occurred to carry out an investigation, report their findings and take legal or other action as appropriate.

Procedure

111. When hand carriage of NATO classified material is permitted, the following minimum procedure shall apply:

(a) the courier shall carry a Courier Certificate based on Appendix 11, authorising him to carry the package as identified. The Courier Certificate shall be stamped and signed by the consignor’s NSA/DSA and by the consignor's FSO;

(b) a copy of the "Instructions for the Courier" (Attachment 1 to Appendix 11) shall be attached to the certificate; and

(c) the Courier Certificate shall be returned to the issuing NSA/DSA through the consignor's FSO immediately after completion of the journey(s) or be kept available at the company for monitoring purposes if permitted by the issuing NSA/DSA national laws and regulations. Any circumstances that occurred during the trip which raise security concerns shall be reported by the courier on the certificate.

112. If the courier is making multiple hand carriages of NATO information classified NC and above, then the "Multi-Travels Courier Certificate" (Attachment 2 to Appendix 11) shall include:

(a) the courier's name and the destination countries. It will be stamped and signed by the NSA/DSA and the consignor's FSO. The certificate cannot be valid for more than one year;

(b) for each journey, a "Description of Consignment" must be signed by the consignor's FSO. This description will be returned to the issuing NSA/DSA, through the consignor's FSO in order to assure accountability or be kept available at the company for monitoring purposes if permitted by the issuing NSA/DSA national laws and regulations ; and

(c) at the end of each journey, the courier will sign the Note at the bottom of the "Multi-Travels Courier Certificate" certifying that no situation occurred that might have compromised the security of the consignment during the journey. The declaration will be witnessed by the consignor's FSO.

113. The consignor's FSO is responsible for instructing the courier in all of his/her duties and of the provisions of the "Instructions for the Courier" (Attachment 1 to Appendix 11) and a Security Acknowledgement (Appendix 10) has to be signed.

114. If customs authorities (of the NATO nation or of a non-NATO nation with a Security Agreement with NATO) request to examine the consignment and inspection is unavoidable, the procedures detailed in the customs section below shall be followed. Customs authorities will be permitted to observe sufficient parts of the consignment to determine that it does not contain material other than that which is declared.

Carriage of Material at the level NC by Commercial Courier Companies

115. The following criteria shall be applied when consignments of NATO classified material at the level NC is carried by non-security cleared commercial courier companies;

(a) the use of transmission channels as described above is not feasible due to a case of urgency or cannot meet the needs of industry;

(b) the commercial courier company provides courier services, and if required by national laws and regulations has concluded a framework arrangement with the NSA/DSA of the consignor which describes the specific obligations of the commercial courier company, include reporting obligations in the case of suspected or actual breaches of security, or losses of NATO classified material;

(c) the commercial courier company is located and registered in a NATO nation and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system;

(d) the commercial courier company must obtain and provide to the consignor proof of delivery on the signature and tally record, or the courier must obtain receipts against package numbers;

(e) the commercial courier company must guarantee the consignment will be delivered to the consignee prior to a specific time and date within a 48-hour-period;

(f) the commercial courier company may charge a commissioner or Sub-contractor, which is located and registered in a NATO nation and also meets the above requirements. However, the responsibility for fulfilling the above requirements must remain with the commercial courier company.

Transportation of NATO Classified Material NC or NS as Freight

116. The consignor and the consignee of a consignment of NATO classified material to be transported as freight internationally shall jointly organise the transport arrangements. The consignor shall submit a written transportation plan to its NSA/DSA who, after consultation with the NSA/DSA of the consignee, will advise the consignor whether the transportation plan is acceptable and/or of any changes that are required.

117. The NSA/DSA of the consignor shall notify, as appropriate, the NSA/DSA of any transited nation of the appropriate details of the transportation, including any cancellation thereof, with sufficient advance notice to enable them to provide the necessary security assistance.

118. When, in the opinion of the NSA/DSA concerned, a consignment at the level NC or NS is of such size and weight, or other circumstances render the standards defined in the Directive of Security of Information or hand carriage impractical or unavailable, commercial carriers may be used. The following procedures shall be applied:

(a) the commercial carrier shall hold an FSC if required by national laws and regulations or if it is to store NC or above at its premises;

(b) the commercial carrier shall deploy personnel that have been granted a PSC at a minimum level to the material being transported;

(c) prior to any international transmission by commercial carrier, the NSAs/DSAs of the consignor and of the consignee must agree on an International Transportation Plan as described in Appendix 12; and

(d) when a International Transportation Plan is developed that will involve more than one international shipment of classified material, a Notice of Classified Consignment (Attachment 1 to Appendix 12) shall be used to identify each shipment and provide details to the recipient, transportation personnel and any other personnel who will be involved in ensuring the security of the shipment.

Transportation of NATO Classified Material NC or NS as Freight by Road

119. The following minimum criteria shall be applied when consignments of NATO classified material NC or NS are transported by road:

(a) when storage of classified consignments is required at the carrier's facility, the carrier shall hold an FSC at the appropriate level issued by the respective NSA/DSA;

(b) classified material shall be secured in vehicles or containers by a lock or padlock of a type currently approved by the NSA/DSA concerned. Closed vans and cars that may be sealed should be used since they offer maximum security. If this is not physically possible, the consignment should be encased to protect the classified aspects and prevent unauthorised persons from gaining access;

(c) the transport shall be accompanied by at least two individuals who could be the driver, co-driver or additionally deployed security escorts or guards, and who both shall hold a PSC at the level commensurate with the classification level of the material. At least one individual shall carry a "Courier Certificate" based on Appendix 11 and assume responsibilities of a "Courier" as described above.

(d) in cases where stops must be made, arrangements shall be made in advance to use storage provided by government establishments or facilities having an appropriate FSC and the necessary cleared personnel and capabilities to ensure security of consignment. In

the event such arrangements cannot be made or an emergency situation arises due to accident or breakdown of the vehicle, at least one of the security cleared individuals accompanying the material shall be responsible for keeping the consignment under constant control, and

(e) communication checks along the road shall be pre-arranged to ensure security of the consignment.

Transportation of NATO Classified Material NC or NS as Freight by Rail

120. The following minimum criteria shall apply when consignments of NC and NS material are transported by rail :

(a) passenger accommodation shall be made available for appropriately cleared security guards or escorts who shall carry a Courier Certificate based on Appendix 11 and assume responsibilities of a “Courier” as described above.; and

(b) during stops, the security guards/escorts shall remain with the consignment.

121. Depending on the volume of the consignment, priority shall be given to rail cars or containers that can be closed and sealed, giving maximum security.

Transportation of NATO Classified Material NC or NS as Freight by Sea

122. The following minimum standards shall be applied when consignments of NATO material classified NC or NS are sent by sea:

(a) where possible consignments should be carried in ships sailing under the flag of a NATO nation. Ships sailing under the flag of a non-NATO nation, which represents a special security risk (as defined in the Directive on the Security of Information, "International Transmission") shall not be used. Where practicable, a guard or escort holding an appropriate PSC shall accompany the consignment;

(b) material shall be secured in locked containers approved by the NSA/DSA of the consignor. However, when this is not possible, blocked-off stowage may be approved by the NSA/DSA of the consignor. Use of security tapes or seals on the openings shall be considered. Blocked-off stowage is stowage in the hold of a ship where the material is covered and surrounded by other cargo consigned to the same destination in such a way that access to the material is physically impracticable. Where it is not possible or impracticable to carry a consignment in the hold, it may be carried as deck cargo, provided it is secured in a locked container and packaged so it is not evident that it contains classified material;

(c) stops at or entering the territorial waters of countries presenting special security risks shall normally be avoided but if unavoidable the security risk shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation plan drawn up by the consignor and the consignee. Unless the ship is in an emergency situation, it shall not enter the territorial waters of any of these countries;

(d) stops at any other country shall not be permitted unless the prior approval of the consignor's NSA/DSA has been obtained;

(e) in all cases, loading and unloading shall be under security control; and

(f) deliveries to the port of embarkation and collection from the port of disembarkation must be so timed to prevent, as far as possible, a consignment being held in port warehouses unless the warehouse has been granted an FSC by the *consignor’s* or consignees NSA/DSA, *as applicable*. Where this is not possible, sufficient security guards must be provided to keep the consignment under adequate and permanent supervision until collection is achieved.

Transportation of NATO Classified Material NC or NS as Freight by Aircraft

123. Preference shall be given to the use of military aircraft of a NATO nation to transport NC or NS material. If utilisation of a military aircraft of a NATO nation is not feasible, an NSA/DSA approved commercial air carrier may be used, provided it is registered in or chartered by a NATO nation. Exceptionally, airlines from non-NATO nations may also be used provided the security of the consignment can be assured by the appropriate measures taken by NSA/DSA. Scandinavian Airlines System aircraft also may be used.

124. The following minimum standards shall be observed:

(a) every effort shall be made to deliver the consignment straight to the aircraft rather than permitting it to be stored in warehouses, etc., at airports and airfields. When a consignment cannot be loaded straight away, it shall either be stored in a NSA/DSA cleared storage facility, or kept under guard. A sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

(b) every effort shall be made for the aircraft to be met on landing and the consignment to be removed at its final destination. When this is not feasible, the consignment shall be kept at the airport and a sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

(c) direct flights shall be used wherever possible;

(d) intermediate routine stops of short duration may be permitted, provided the consignment shall remain in the aircraft. However, if the cargo compartment is to be opened, every effort shall be made to ensure that the courier or other personnel holding an appropriate PSC are available to ensure the protection of the classified material;

(e) in the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the security guard, or the person fulfilling the duties of the security guard, shall take all measures considered necessary for the protection of the consignment and if necessary seeking the assistance of his Diplomatic mission in the country concerned;

(f) transportation over countries presenting special security risks, as defined in the “Directive on the Security of Information, International Transmission” should be avoided; and

(g) stops in a non-NATO nation having a valid security agreement with NATO, may be allowed by the NSA/DSA of the consignor. Stops at airfields in non-NATO nations not having a Security Agreement with NATO, except in an emergency, shall not be permitted;

125. When the conditions outlined below are met and if permitted by national laws and regulations, the requirements for a commercial air carrier to hold an FSC do not apply:

(a) the commercial air carrier agrees to be responsible for the consignment while it is in the hold of the air plane, and will be cognisant of, and agrees to comply with the security requirements, particularly the emergency procedures specified by the NSA/DSA;

(b) consignments shall be transmitted point-to-point, the service provided by the commercial air carrier cannot be sub-contracted, and the intermediate stops are not permitted;

(c) a written transportation plan approved by the participating NSA/DSA shall be in place before the consignment is released to the cargo handling service or to the commercial air carrier;

(d) sufficient physical protection shall be provided to the consignment as agreed by the NSA/DSA.

126. Companies that provide cargo handling services (such as freight forwarders) for NC and NS consignments shall have an FSC and approved protection capability if the consignment is to be stored at the facility.

Security Principles applicable to all Forms of Transportation

Countries presenting special Security Risks

127. Countries presenting special security risks shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation arrangements. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorised access to classified material.

Customs

128. As a general rule, customs authorities shall be advised by the appropriate national authorities of impending consignments and should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the security guard or courier. Consignments should not be opened unless there is a pertinent reason for so doing. If a consignment is opened, this should be done out of sight of persons who do not have a need-to-know and in the presence of the courier. When access is no longer necessary it shall be repacked securely, and the customs authorities shall be requested to reseal it and endorse the shipping documents, confirming that it was opened by such authorities. To facilitate customs clearance, advantage should be taken of the Transport International Routier (TIR) for road shipments, Transport International Ferroviaire (TIF) for rail shipments, or other similar shipping arrangements.

129. Nothing in the previous paragraph or elsewhere in this section should be construed to abrogate any nation's rights of examination of any consignment.

Acknowledgement

130. The consignee shall acknowledge receipt of the consignment to the sender.

Packaging

131. Packaging of consignments shall be in compliance with the Directive on the Security of Information. The FSO of the consigning facility is responsible for appropriate packaging. In no circumstances shall the packaging reveal the fact that the material is classified.

Security Guards and Escorts

132. Individuals fulfilling the duties of security guards may be civilian or military personnel and may be armed or unarmed depending on national practices and arrangements made between the NSAs/DSAs of the nations affected by the transportation. Similarly, the nationality of such guards in any particular nation shall be subject to mutual agreement of the NSAs/DSAs and in accordance with NATO security policy addressed further at Enclosure "C" to the NATO Security Policy (C-M(2002)49) and in the supporting Directive on Personnel Security (AC/35-D/2000).

133. In addition to the security guards, security escorts may be provided if the NSAs/DSAs concerned consider this desirable or as required under their national laws and regulations. These escorts need not be security cleared unless otherwise required by national laws and regulations.

134. The security guard/escort shall be composed of an adequate number of personnel as to ensure regular tours of duty and rest. The number of guards/escorts on a consignment shall depend on the classification level of the material, the method of transportation to be used, the estimated time in transit, and the quantity of material will also be considered. A reserve of personnel shall be provided to cater for emergencies.

135. It is the responsibility of the consignor (and, where applicable, the consignee) to instruct security guards in their duties. In particular, the route and the security plan must be explained, and

details given, where appropriate, of the authorities that security guards shall contact and other measures to be taken in the event of an emergency. Security guards shall also be given a copy of "Notes for the Courier", and be required to sign the Security Acknowledgement.

136. The consignor's NSA/DSA may issue to the consignor sufficient authorisation documents so that they may be completed and issued to the security guards (Appendix 13).

137. Both the authorisation documents and "Instructions for the Courier" (Attachment 1 to Appendix 11) shall be written in English and French; a copy in other languages may, in addition, be issued if this is deemed necessary or recommended by the NSA/DSA concerned.

Transportation of Explosives, Propellants or Other Dangerous Substances

138. If the classified material contains explosives, propellants or other dangerous substances, the transmission across international borders is subject not only to the security and customs requirements, but also to mandatory international and national safety regulations. The consignor is responsible for compliance with these regulations.

GLOSSARY AND ACRONYMS

GLOSSARY

Attestation of Personnel Security Clearance (APSC)	An approved format to confirm the security clearance level of an individual in the context of a contract involving NATO classified information.
Background Information	Knowledge that has been generated by one of the participants outside of the collaborative programme but which has been provided to the programme. Only the originating participant needs to be consulted for authorising the release of that information to parties outside the programme.
Breach of Security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area, where persons without an appropriate PSC have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Commercial Courier Company	Commercial company that offers a service where a consignment is moved under a trace and tracking scheme.
Compromise	Compromise denotes a situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism**,** sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The Contractor, facility or other organisation receiving material from the consignor.
Consignor	The Contractor, facility or other organisation responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.

Contract involving NATO Classified Information	Any contract issued by a NATO civil or military body or a NATO nation in support of a NATO funded or administered programme/project that will require access to or generation of NATO classified information.
Contractor	An industrial, commercial or other entity that seeks or agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some NATO nations, the function of a DSA may be carried out by the NSA or a DSA may delegate functions to other competent security authorities.
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Escorts	Armed or unarmed national police, military personnel, government personnel or other government designated personnel that facilitate the secure movement of information and materiel.
Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
Facility Security Clearance (FSC)	An FSC is an administrative determination by which an NSA/DSA formally recognizes the capacity and reliability of Contractor's facilities to manage generate and have access to NATO classified information up to a certain level.
Foreground Information	Foreground information is knowledge that has been generated in pursuance of a collaborative/cooperative programme. It is owned by all participants. To determine the releasability of foreground information approval of all owners is required.
Freight	Material carried by a vessel or vehicle, especially by a commercial carrier; cargo. Also – the commercial transportation of material.
Guards	Civilian (Government or participating Contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.

Industry	Organized economic activity concerned with manufacture, extraction and processing of raw materials, construction or output of a specific service.
CIS Security	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Infraction	A security infraction is an act or omission, deliberate or accidental; contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (E.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.).
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO civil and military bodies fall within the security jurisdiction of NATO.
Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and ”Permanent Residents in Canada”. “Permanent Residents in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
National Security Authority (NSA)	An authority of **a** NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad.

NATO	"NATO" denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.
NATO Classified Information	Means information or material determined by or on behalf of NATO to require protection against unauthorised disclosure which has been so designated by a security classification NR or above.
NATO Programme/Project	A Council approved programme/project that is administered by a NATO agency/office under NATO regulations.
NATO Programme/Project Agency/Office (NPA/NPO)	The executive body for the administration of a NATO programme/project.
Need-to-Know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services .
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.
Originator	The nation or international organisation under whose authority information has been produced or introduced into NATO.
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information.
Personnel Security Clearance Certificate (PSCC)	An approved format used by NSAs/DSAs to confirm the level and validity of a PSC.
Prime Contract	The initial contract led by a NATO Project Management/Agency/ Office for a Programme/project.
Prime Contractor	An industrial, commercial or other entity of a NATO nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential Sub-contractors as approved.
Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.

Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI may constitute an Annex to the prime contract, and may be revised throughout the programme lifecycle. For sub-contracts let within the programme, the PSI constitutes the basis for the SAL.
Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Risk management	A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Security Classification Check List (SCCL)	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified specifying the security classification levels. In case of contracts let within a programme/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Sub-contract	A contract entered into by a prime Contractor with another Contractor (i.e., the Sub-contractor) for a provision of goods or services.
Sub-contractor	A Contractor to whom a prime Contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Transportation by freight	Transportation of a consignment of such size and weight which makes the application of the respective standards defined in the Directive of Security of Information or hand carriage impractical.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources.

GENERAL RESPONSIBILITIES

NATO NATIONS

1. Each NATO nation shall:

(a) designate one or more authorities (DSA) responsible to the NSA, where applicable. The DSA is responsible for communicating national and NATO security policy to industry and for providing direction and assistance in its implementation; in some countries there may be more than one authority designated as a DSA or the function of a DSA may be carried out by the NSA;

(b) certain functions of the NSA/DSA may be carried out by other competent security authorities in accordance with national laws and regulations;

(c) ensure that it has the means to make its industrial security requirements binding upon industry and that it has the right to inspect and approve the measures taken in industry for the protection of NATO classified information;

(d) determine, as appropriate, the aspects of a NATO contract or sub-contract requiring security protection and the security classification to be accorded to each aspect. Prior to the release of NATO classified information to a Contractor, prospective Contractor, or Sub-contractor, the NATO nation shall :

(i) ensure that the Contractor(s), prospective Contractor(s), or Sub-contractor(s) and their facility(ies) have the capability to protect NATO classified information adequately, in accordance with national laws and regulations;

(ii) grant a Facility Security Clearance (FSC) to the facility(ies), if appropriate;

(iii) grant a NATO Personnel Security Clearance (PSC) to all personnel whose duties require access to information classified NC or above; and

(iv) ensure that access to the NATO classified information is limited to those persons who have a need-to-know for purposes of performance on the NATO project/programme;

(e) make arrangements whereby persons considered by the NSA/DSA to be a security risk can be excluded or removed from positions in which they might endanger the security of NATO classified information;

(f) implement, as and when necessary, the NATO procedures for the mutual safeguarding of the secrecy of inventions;

(g) provide, upon request to an NSA/DSA of a NATO nation, or to a NATO civil or military body, an FSCC to enable a facility falling within its security cognisance to negotiate or fulfil a contract/sub-contract involving information classified NC or above;

(h) provide, upon request, to a NSA/DSA of another NATO nation, or a NATO civil or military body, a PSC for the persons for whom it has security responsibilities to enable them to fulfil on a NATO classified contract;

(i) take action with regard to the specific arrangements to be carried out in matters of transportation and international visits in accordance with the requirements of NATO security policy and this directive:

(i) investigate all cases in which it is known, or where there are grounds for suspecting, that NATO classified information has been lost or compromised. Each member nation shall comply with the investigative requirements set out in NATO security policy and its supporting directives and promptly inform

the NPA/NPO and the other member nations concerned and if applicable the NOS of the details of any such occurrences; and

(ii) ensure that for any facility in which NATO classified information is to be used, a person or persons shall be appointed, where appropriate, in accordance with national laws and regulations, to effectively exercise the responsibilities for safeguarding the NATO classified information. These officials shall be responsible for limiting access to the NATO classified information involved in a contract to those persons who have been cleared and authorised for access and have a need-to-know.

SECURITY COMMITTEE (SC)

2. The SC shall:

(a) formulate NATO industrial security policy and supporting directive(s) and make appropriate recommendations to the North Atlantic Council (c) for the security protection of NATO classified information entrusted to industry; and

(b) consider matters of industrial security referred to it by the NAC, a member nation, the Secretary General, the NATO Military Committee (NAMILCOM), Strategic Commands and heads of NATO civil and military bodies.

NATO OFFICE of SECURITY (NOS)

3. The NOS shall:

(a) assist and give guidance in industrial security matters to NPA/NPOs and such other NATO industrial projects as may be designated by the NAC and supervise the implementation of NATO security policies and directives in those organisations and projects;

(b) in agreement with the NSAs/DSAs of member nations concerned, assist and give guidance to other NSAs/DSAs in the implementation of NATO security policies and directives in connection with the activities of NPA/NPOs;

(c) in agreement with the NSAs/DSAs of member nations concerned, assist and give guidance on NATO security policies and directives to facilities participating in the activities of NPA/NPOs;

(d) make periodic inspections of the security arrangements for the protection of NATO classified information in NPA/NPOs;

(e) with the agreement of the appropriate NSA/DSA, make periodic examinations of the security arrangements for the protection of NATO classified information in the member nations; and

(f) give guidance and advice, when requested by NSAs/DSAs, on matters of industrial security arising in all NATO-related projects.

NATO PROGRAMME/PROJECT AGENCIES / OFFICES

4. Each of the NPA/NPOs and other NATO agencies with project management responsibilities as may be designated by the NAC will be bound by the general security regulations laid down in NATO security policy and supporting directives, and any other security regulations approved by the NAC as may apply. Each of the NATO Management Agencies/ Offices shall:

(a) draw up the implementing security regulations for the agency/office in compliance with the provisions of NATO security policy and supporting directives and supervise their enforcement;

(b) in conjunction with the NSAs/DSAs concerned and the NOS, co-ordinate the implementation of NATO security policies and directives, both by potential Contractors and by Contractors, and deal with any security problems arising in any NATO project in which the agency/office is engaged;

(c) obtain the appropriate Facility Security Clearance(s) as required in conjunction with contracts involving classified NATO information;

(d) take action as required, and in accordance with the provisions of NATO security policy and this directive, in respect of the special arrangements for International Visits;

(e) be responsible for preparing Project Security Instructions (PSI) for the programmes they manage for approval by participating NSAs/DSAs; and

(f) may be responsible for raising a Transportation Plan as identified in the PSI.

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

1. INTRODUCTION

1.1 Attached is a sample format of a Facility Security Clearance Information Sheet (FSCIS) for the quick exchange of information between National Security Authority or Designated Security Authority or other competent national security authorities (hereinafter referred to as "NSA/DSA") and NATO contracting authorities (NATO Programme/Project Offices/NATO Programme/Project Agencies) with regards to the Facility Security Clearance (FSC) of a facility involved in classified tenders, contracts or sub-contracts.

1.2 The FSCIS is not for use by Contractors.

1.3 The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA/DSA/NPO/NPA in form field 7 of the request section.

1.4 The details contained in the FSCIS shall normally not be classified and therefore the preferable way for the exchange of the FSCIS will be electronically between the respective NSAs/DSAs/NPOs/NPAs.

1.5 NSAs/DSAs should make every effort to respond to a FSCIS request within 5 working days. In urgent cases, NSA/DSA will send the response within 3 working days.

Procedures and Instructions for the Use of the Facility Security Clearance Information Sheet (FSCIS).

These detailed instructions are for the NSA/DSA that completes the FSCIS.

The request should preferably be typed in capital letters

HEADER	The requesting NSA/DSA/NPA/NPO inserts full country or international organization name.
1. REQUEST TYPE	The requesting NSA/DSA/NPA/NPO selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: TS = National TOP SECRET CTS = COSMIC TOP SECRET S = National SECRET NS = NATO SECRET C = National CONFIDENTIAL NC = NATO CONFIDENTIAL CIS = Communication and information systems for processing classified information A FSC is not required by Enclosure G to C-M(2002)49 for access to, or generation of classified information at level of NATO RESTRICTED (NR). However some NATO Nations, as identified in Appendix 3, and as mandated by their national laws and regulations, do require a FSC for Contractors/Sub-contractors under their jurisdiction, for access to classified information at the level of NR.
2. SUBJECT DETAILS	The Form Fields 1 through 6 are self-evident. Form Field number 5 is optional.
3. REASON FOR REQUEST	Give the specific reason for the request, provide project indicators, number of contract, letter of intent or invitation. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates, which may have a bearing on the completion of a FSC, should be included.

4. REQUESTING NSA/DSA/NPA/NPO	State the name of the actual requestor (on behalf of the NSA/DSA) and the date of the request by using the "day/month/year" (dd/mm/yyyy) format.
5. REPLY SECTION	Form Field 1-6: Select appropriate fields. Form Field 2: In case an FSC is in progress it is essential to give the requestor an indication of the required processing-time (if known). Form Field 6: (a) The validation date inputted will be either when the FSC for the Contractor's facility expires, and/or when this FSCIS expires (if different). Any date inputted must be in the "day/month/year" format. It should be noted that some NATO Nations do not have an expiry date for FSCs or the FSCIS, so will be marked "n/a". (b) Should an FSC and/or FSCIS expire prior to the award of a NATO Classified Contract the requesting NSA/DSA/NPA/NPO is responsible for submitting a new FSCIS request to the NSA/DSA of the Contractor to re-validate the FSC of the facility.
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing Items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply by using the "day/month/year" (dd/mm/yyyy) format.

APPENDIX 2
ANNEX 1
AC/35-D/2003-REV5

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

All fields must be completed and the form communicated via Government-to-Government or Government to International Organization channels

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE
TO : _____
(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[ ] Provide an FSC assurance at the level of: [ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC
for the facility listed below
[ ] Including protecting of classified material/information
[ ] Including Communication and Information Systems (CIS) for processing classified information

[ ] Initiate an FSC up to and including the level of ..... with ……level of protection and ……level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

	Corrections / additions:
1. Full facility name: ……	……
2. Full facility address: ……	……
3. Mailing address (if different from 2.) ……	……
4. Zip/postal code / city / country ……	……
5. Name of the Security Officer ……	……
6. Telephone/Fax/E-mail of the Security Officer ……	……

7. This request is made for the following reason(s): (indicate particulars of the pre-contractual stage, contract, sub-contract, programme/project):
……
……

Requesting NSA/DSA/NPA/NPO: Name: …… Date: (*dd/mm/yyyy*) ……

REPLY (within 5 working days)

This is to certify that the above mentioned facility:

1. [ ] holds an FSC up to and including the level of:
[ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC
[ ] Other: ……
2. [ ] on the above mentioned request, the FSC process has been initiated. You will be informed when the FSC has been granted or refused.
3. [ ] does not hold an FSC.
4. has the capability to protect classified information/material:
[ ] yes, level: …… [ ] no
5. has Accredited CIS:
[ ] yes, level: …… [ ] no
6. This FSC assurance expires on …… (*dd/mm/yyyy*), or as advised otherwise by the NSA/DSA.
In case of an earlier invalidation or in case of any changes of the information listed above you will be informed.
7. Remarks:
……
……

Issuing NSA/DSA:
Name: …… Date: (*dd/mm/yyyy*)……

FACILITY AND PERSONNEL SECURITY CLEARANCE FOR CONTRACTS INVOLVING NATO RESTRICTED INFORMATION
- NATIONAL REQUIREMENTS -

"These national requirements for FSC/PSC and notifications for contract involving NR shall not put additional obligations on other NATO nations or Contractors under their jurisdiction".

MEMBER NATION	FSC		Notification of contract/subcontract involving NR information to NSA/DSA		PSC	
	YES	NO	YES	NO	YES	NO
Albania		X	X			X
Belgium		X		X		X
Bulgaria		X		X		X
Canada	X		X		X	
Croatia		X	X			X
Czech Republic		X		X		X
Denmark	X		X		X	
Estonia	X		X			X
France		X		X		X
Germany		X		X		X
Greece		X		X		X
Hungary		X		X		X
Iceland		X		X		X
Italy		X		X		X
Latvia		X		X		X
Lithuania		X		X[2]		X
Luxembourg	X			X	X	
Netherlands	X[3]		X[2]			X
Norway		X	X			X
Poland		X		X		X
Portugal		X		X		X
Romania		X	X			X
Slovakia	X		X			X
Slovenia	X		X			X
Spain		X	X			X
Turkey	X				X	
United Kingdom		X		X		X
United States	X			X		X

[2] NSA/DSA however requests notification by NATO contracting authorities
[3] For military-related contract only

CONTRACT SECURITY CLAUSE

FOR INCLUSION IN

TENDERS AND CONTRACTS

INVOLVING

NATO RESTRICTED INFORMATION

INTRODUCTION

1. This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

BACKGROUND

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

SECTION I - RESPONSIBILITY

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

SECTION II - PERSONNEL SECURITY

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

SECTION III - PHYSICAL SECURITY

6. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet**,** or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[4]).

7. NR information shall be handled in Administrative Zones or held under personal custody.

[4] An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

SECTION IV - SECURITY of INFORMATION

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

15. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

(a) moved by postal or commercial services;

(b) carried by Contractor's personnel; or

(c) transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

SECTION V - SUB-CONTRACTING

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

21. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

SECTION VI - HANDLING OF NATO RESTRICTED INFORMATION ON INFORMATION AND COMMUNICATION SYSTEMS (CIS)

Security Accreditation of Communication and Information Systems (CIS)

22. Security accreditation shall be performed for all contractors' CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) information.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor under delegation from the Contracting Authority for the accreditation of the contractor's CIS handling NR information. Under this delegated authority the contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

26. The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

26.1 Identification and Authentication

26.1.1. An up-to-date list of authorised users shall be maintained by security management staff.

26.1.2. Credentials shall be established and maintained to identify authorised users.

26.1.3. Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

26.1.4. Passwords shall be a minimum of 9 characters long and shall include numeric and "special" characters (if permitted by the system) as well as alphabetic characters;

26.1.5. Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

26.1.6. The re-use of a number of previous passwords shall be denied.

26.1.7. The system shall provide only limited feedback information to the user during the authentication process.

26.1.8. Accounts that are no longer required shall be locked or deleted.

26.1.9. When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

26.2 Access Control

26.2.1. The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.

26.2.2. From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

26.2.3. Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

26.2.4. Access to security and system information shall be restricted to only authorised security and system administrators.

26.2.5. Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).

26.2.6. The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user's data access/display devices other than unlocking the activity of the session.

26.2.7. The system shall allow user-initiated locking of the user's own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user's data access/display devices other than unlocking the activity of the session.

26.2.8. Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

26.3 Security Audit

26.3.1. An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

- all log on attempts whether successful or failed;
- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

26.3.2. The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in humanreadable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.

26.3.3. Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

26.3.4. The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

26.3.5. A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).

26.4 Protection against Malicious Software

26.4.1. Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).

26.4.2. The virus/malicious code detection software shall be regularly updated.

26.5 Mobile Code

26.5.1. The source of the mobile code shall be appropriately verified.

26.5.2. The integrity of the mobile code shall be appropriately verified.

26.5.3. All mobile code shall be verified as being free from malicious software.

26.5.4. Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

26.6 Availability

26.6.1. Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

26.7 Import/Export of Data

26.7.1. Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

26.7.2. All data imported to or exported from the CIS shall be checked for malware.

26.8 Configuration Management

26.8.1. A detailed hardware and software configuration control system shall be available and regularly maintained.

26.8.2. Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

26.8.3. Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

26.8.4. An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

26.8.5. The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

26.8.6. The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse affects of the modification on existing security measures, shall be considered and appropriate action taken.

26.8.7. The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

26.8.8. The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

26.8.9. Changes to the system or network configuration shall be assessed for their security implications/impacts.

26.8.10. The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

26.9 Security Management

26.9.1. Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

26.9.2. The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

26.10 Approved products

26.10.1. An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

26.10.2. The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

26.11 Security Testing

26.11.1. The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

26.12 Transmission Security

26.12.1. NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

26.13 Wireless LAN

26.13.1. The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

26.13.2. NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

26.14 Virtualisation

26.14.1. When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

26.14.2. A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

26.14.3. Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

26.14.4. Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

26.14.5. The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

26.14.6. Access to the hypervisor functions shall be appropriately controlled.

26.14.7. The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

26.14.8. The ability to create virtual machines shall be appropriately configured and controlled.

26.14.9. Virtual Machines shall be suitably de-commissioned after use.

26.14.10. Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

26.14.11. Virtual Servers and Virtual Workstations shall not be located on the same physical host.

26.14.12. Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.

26.14.13. The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti malware and Active Directory communication mode shall be allowed.

26.14.14. Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.

26.14.15. The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

26.14.16. The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.

26.14.17. Modifications to the ‘Master Copy/Version’ of a Virtual Machine shall be appropriately controlled.

26.14.18. Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

26.15 Interconnections to a CIS not accredited to handle NR information

26.15.1. Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled “INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)” (current reference AC/322-D/0030-REV5) and “Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet” (current reference AC/322-D(2010)0058). These Directives may be obtained from the Contracting Authority.

26.15.2. Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor’s CIS and therefore the risk to the security of the NR information handled by the contractor’s CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process. Security requirements can also be found in the latest version of the NATO document entitled “INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security” (current reference AC/322-D/0048-REV2). This Directive may be obtained from the Contracting Authority.

26.15.3. When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

26.16 Disposal of IT Storage Media

26.16.1. For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:

- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives): overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of 10mm^2 or less;
- Other storage media: seek security requirements from the Security Accreditation Authority.

26.17 Portable Computing Devices (laptops, tablets, etc)

26.17.1. Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor’s premises unless held under personal custody. The term “drives” includes all removable media. Any authentication token and/or password(s) associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

27. Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

28. CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

Security of NR Removable Computer Storage Media

29. Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle.

Use of CIS Equipment Privately Owned by Contractor's Personnel

30. The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

31. CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice

32. Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

33. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this Contract Security Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

SECURITY ASPECTS LETTER (SAL)

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed or in the contracts involving NR information only as established in the Contract Security Clause.

2. All classified information and material shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the work is performed or in the case of NR information as may also be established in the Contract Security Clause.

3. In particular, the Contractor shall:

(a) appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Proposals (RFP), contract or sub- contract;

(b) submit in due time to the NSA/DSA the personal particulars of the person the contractor wishes to employ on the project with a view to obtaining PSCs at the required level where NC and above is involved;

(c) maintain, preferably through this officer responsible for security measures, a continuing relationship with the NSA/DSA and /or the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or sub-contract is properly safeguarded;

(d) limit the copying of any classified materiel (including documents) to the absolute minimum to perform the contract;

(e) supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;

(f) maintain a record of his employees taking part in the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances;

(g) deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA or in the case of NR information as determined by the need-to-know;

(h) limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub- contract;

(i) comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognise that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

(j) report to the Security Officer and to his NSA/DSA any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and security status of the facility, and any other information which may be required by the NSA/DSA, such as reports on holdings of NATO classified information or materiel;

(k) obtain the approval of (programme/project office and NSA/DSA) before beginning negotiations with a view to sub-contracting any part of the work which would involve the Sub-contractor having possible access to NATO classified information, and to place

the Sub-contractor under appropriate security obligations which in no case may be less stringent than those provided for his own contract;

(l) undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of (programme/project office) or the prime Contractor, any NATO classified information supplied to him, and return to (programme/project office) all classified information referred to above, as well as that developed in connection with the contract or sub-contract unless such information has been destroyed, or its retention has been duly authorised by the contracting office or the sub-contracting officer. Such NATO classified information shall be returned at such time as the contracting office may direct; and

(m) comply with any procedure established with respect to the dissemination of NATO classified information in connection with the contract or sub-contract.

4. Any person taking part in the performance of work the classified parts of which are to be safeguarded, must possess the appropriate NATO security clearance issued by his NSA/DSA. The level of this clearance must be at least equal to the security category of the materiel, the related information or specifications where NC or above is involved.

5. Unless specifically authorised to do so by (programme/project office), the Contractor may not pass on any NATO classified information to any third party to whom a request to supply goods or services has been submitted.

6. No change in level of classification or de-classification of documentation or materiel may be carried out unless written authority in this respect is obtained from (programme/project office).

7. No CIS may be used for processing classified information without prior accreditation by the responsible authorities. At the level of NR, such accreditation can be under delegated authority of the responsible accreditation authority or the contracting authority in accordance with Appendix 4.

8. Failure to implement these provisions and the security regulations established by the NSA of the nation where the contractual work is being performed may result in termination of this contract without reimbursement to the Contractor or claim against NATO, (programme/project office) or the national government of the said nation.

9. The (programme/project office) security classification check list indicates the degree of classification of the data and materiel (equipment, information, technical manuals, specifications) which may be handled in the performance of work under this contract and which must be safeguarded in accordance with the provisions of this letter.

10. The contractor shall destroy or return any classified information provided or generated under the contract unless the contracting authority has given written approval to retain such classified information, e.g. for warranty purposes.

11. The Contractor shall be required to acknowledge receipt of an accompanying SAL or Program Security Instruction (PSI) that is made part of the applicable contract and confirm that it understands the security aspects defined. With respect to contracts involving only NR information the Contractor shall also be required to confirm that it will comply with the provisions of the Contract Security Clause and specifically that any company CIS used to handle or process NR classified information has been appropriately security accredited.

Project Security Instructions (PSIs) - Structure and Content

The following is provided as guidance for the structure and content of Project Security Instructions (PSIs).

Section	Content
1 Document Control	• The issue number; • the date of issue; • the reference and details of the latest Change Proposal; • any related Contract Amendment; • index of amendments; • PSIs index of contents.
2 Introduction / Definitions	• The purpose of the PSIs; • the authority of the PSIs (for example, Project Security Group); • definitions of frequently used terms in NATO contracts involving classified information.
3 National/NATO/ Industry Officials	• The contact details (name, address, telephone / fax number, e-mail address) for the national / NATO officials involved in the project/programme, who are responsible for the following: - administration and policy; - technical security; - CIS Security. Note: This may be included as an Annex to the PSIs.
4 Security Instructions	• General aspects relating to the exchange of NATO classified information and the responsibilities of the NSAs/DSAs; • definition of the security classifications and markings appropriate to the project/programme; • explanation of terms - classified information, material and documents. • storage and transmission of NATO classified information; • disposal / destruction of NATO classified information; • breaches of security; instructions relating to the loss, compromise or possible compromise of NATO classified information; • instructions relating to the unauthorised release of NATO information.

Section	Content
5 Release of Information	Definitions of terms, for example, public release, marketing release, sales release, project information, participants, authorities, and approval; • a release statement, for example, "the release of project information (classified or non-classified) to authorities or persons outside of the project (non-participants) without prior approval is strictly prohibited". • release of project information: - general information - NATO/National policies, required Facility Security Clearances, contractual requirements, security agreements for marketing activities; - release of project information to non-participating bodies; - release in connection with sub-contracting; - public release - general instructions, management of public releases; - sales releases - general instructions, management of sales releases; - marketing releases - general instructions, management of marketing releases; • formats for request for release of project information to non-participants, for use at symposia, seminars, etc., and for public release.
6 Change Procedures	• Procedures for changes to security instructions, including the PSIs; • procedures for changes to the Security Classification Guide; • the use of interim procedures.
7 International Hand Carriage of NATO Classified Documents	• Classification of documents for hand carriage; • conditions when hand carriage of documents is permitted; • courier certificate; • responsibilities of Security Offices in the NPA/NPO, Government bodies and industry - administrative procedures, packaging; • responsibilities of the courier; • instructions in the event of loss of documents; • format for "document transmission notification"; • format for "instructions to persons who are authorised to hand-carry NATO classified documents"; • format for "instructions to prevent customs examination".

Section	Content
8 International Visit Control Procedures	• General instructions for international visits; • procedures for one-time and recurring visits, including use of the standard "Request for Visit" format, and lead times; • procedures for emergency visits; • instructions for the use and completion of the standard "Request for Visit" format; • list of authorities concerned with International Visit Control Procedures (Note: This may be included as an Annex to the PSIs).
9 Sub-Contracting	• Definitions of terms, for example, negotiations, Contractor, Sub-contractor, classified contract, and facility security clearance; • security instructions relating to the negotiation of a NATO classified contract; • permission to negotiate contracts; • security classification of contracts.
10 International Transportation	• Security procedures relating to the international transportation of NATO classified material. • Transportation Plan to be established if required.
11 Communication and Information Systems (CIS)	• Security procedures for the accreditation and use of CIS (or reference to a specific document dealing with project-related CIS).
12 Security Classification Guide	• A document which outlines classifications applicable to the programme/project as allocated and approved by the participants (background and/or foreground information, procedures for downgrading and declassification, caveats).

APPENDIX 7
ANNEX 1
AC/35-D/2003-REV5

FACILITIES/ORGANISATIONS LIST

From: (Letterhead of Management Office/Agency)

To: (Relevant NSA/DSA or NATO Civil or Military Body)

List of government departments, establishments, Contractors and Sub-contractors in (insert country) employed on NATO programme/project (insert name) classified NATO……..

Serial Number	**Facilities/ Organisations**	**Address Telephone/Fax/Email of Security Officer**	**Security facilities for holding NATO classified information YES (+ level)/NO**
1	Example British Aerospace Aircraft Group, Warton Division	Warton Aerodrome, Preston, Lancs. UK Tel.: (+44) XXX XXX XXX FAX: (+44) XXX XXX XXX E-mail:	YES (NATO SECRET)
2	……..	……	…….
3	……..	……	…….

The Security Officer:

---------- ----------

(Name) (Signature)

NATO INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs)

1. INTRODUCTION

1.1 When NATO international visits involve access to information subject to government approval or when or unescorted access to security areas (e.g. Class I/II Security Areas) is necessary, a visit request will be submitted by the visitor through his/her Security Officer, certifying/requesting NSA/DSA and receiving NSA/DSA to the agency, organisation, or facility to be visited. These visit requests are formalized in the standard Request for Visit (RFV) procedure. However specific rules apply for NU or NR visits.

1.2 While in principle the requirement for applying the RFV procedure starts with the classification level NC for information as well as unescorted access to security areas, Appendix 9 identifies nations that require by their laws and regulations a RFV submission for NU or NR visits to their country.

1.3 Visits involving NU or NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements The SO of the facility to be visited shall submit a visit request to its NSA/DSA as identified in Appendix 9 on behalf of the visitor. However, visitors are not required to hold a PSC.

1.4 Where international visits involve access by the visitor to NATO classified information at the level NC or above or unescorted access to security areas, such visits shall be subject to a formal request for visit and approval by the NSA/DSA of the facility to be visited following procedures as defined in this Appendix.

2. SCOPE

General

2.1 The attached standard procedures have been approved for visits by personnel to facilities of another country. They may also be applied to visits within a country. Member nations also have agreed to include the procedures in their national regulations that govern international visits. Notwithstanding the procedures agreed in this document NSAs/DSAs may for national security reasons refuse a RFV for a visit to one of its facilities.

Special Arrangements for specific programmes/Projects

2.2. While the NATO IVCPs will normally be those defined in this Appendix, in the case of a specific programme/project, when all NSAs/DSAs involved, in co-ordination with the responsible NPA/NPO, determine that these general procedures would not be the best suitable for their specific requirements, they are authorized to establish other procedures, which will be set out in the PSI, that provide a level of protection no less stringent than the principles set out in this Appendix.

2.2.1 Accordingly, where permitted by national rules and regulations, visits involving access to information classified up to and including NATO SECRET may be arranged by exception, directly between the FSOs of the sending and receiving facility, acting on behalf of the NSAs/DSAs involved, provided that such an arrangement is approved by the relevant national authorities.

2.2.2 International Visits to Non-NATO Nations and International Organisations concerning contracts/sub-contracts involving classified NATO information have to adhere to the respective provisions of the relevant Security Agreement or Arrangement in place.

Personnel on Loan within a NATO programme/Project

2.3 When an individual (not Contractors) who has been cleared for access to NATO classified information is to be loaned within a NATO programme/project or other classified contract from one Contractor's facility to another one located in another NATO country, or to a NATO body, the individual may be assigned, or have access to NATO classified information at the facility the individual is to be loaned on the basis of a RFV, PSCC or an Attestation of Security Clearance, as appropriate. The RFV, PSCC or Attestation of Security Clearance shall be provided by the parent facility to the facility the individual is to be loaned via its respective NSA/DSA.

3. TYPES OF VISITS AND PROCEDURES

3.1 There are four types of international visit requests. They are as follows:

(a) one-time;

(b) recurring;

(c) emergency; and

(d) amendment.

4. ONE-TIME VISIT

4.1 A one-time visit is a single visit for a specific purpose and to a specific site or sites, which is not anticipated to be repeated within the same calendar year. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s).

4.2 Depending on the laws/regulations of the countries involved, a one-time visit request which is issued for the posting of personnel may require additional information/documents to be included with the RFV Form.

5. RECURRING VISIT

5.1 A recurring visit is for intermittent visits over a specified period of time to a specific site or sites and for a specific purpose. A recurring visit covers normally the duration of a government approved programme, project or contract that requires participating personnel to make intermittent (recurring) visits to military, government, *NATO* or industrial facilities of another country participating in the programme. Visits covering a period of more than one year may be subject to annual review, as agreed by the participating countries NSA/DSA. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s).

6. LEAD TIMES FOR ONE-TIME AND RECURRING VISITS

6.1 The lead time to process one-time and recurring visits is depicted in Appendix 9 which identifies the number of working days to the starting date of the one-time or the starting date of the first of the recurring visit that the request should be in the possession of the receiving NSA/DSA.

7. EMERGENCY VISIT

7.1 An emergency visit is for a one-time visit that must take place as a matter of urgency and importance and as such that the normally required lead time identified in Appendix 9 cannot be met.

7.2 Such unplanned or emergency visits should be arranged only in exceptional circumstances. To qualify as an emergency visit at least one of the following conditions must be met:

(a) the proposed visit is related to an official military, government, *NATO* 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);

(b) the visit is to be made in response to the invitation of a host government, military, *NATO* official or host contract official and is in connection with an official military, government, international organisations project, programme or contract;

(c) a programme, project, contract opportunity or otherwise significant financial interest will be placed in jeopardy if the visit request is not approved; or

(d) operations and/or personnel are placed in direct jeopardy if the visit is not approved.

7.3 Emergency visit requests shall be critically reviewed, fully justified and documented by the Security Officer of the requesting military, government agency, NATO or industrial facility. Therefore, the requestor must complete the remarks portion in item 15 of the RFV Form to fully explain the reasons behind the emergency RFV.

7.4 When the Security Officer is satisfied that the conditions cited in paragraph 7.2 of this document have been met, the Security Officer will contact a knowledgeable person at the government agency, organisation, or industrial facility to be visited (host facility), directly by telephone, facsimile or email, to obtain tentative agreement for the proposed visit. If tentative agreement is provided to proceed with the visit request, the Security Officer of the military, government agency, international organisations or industrial facility to be visited (host facility) shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the government agency, organisation, or industrial facility requiring to make the visit (requesting facility) and explain the reason for the emergency. Furthermore, the Security Officer will then follow regular RFV procedures and send the emergency RFV to his/her NSA/DSA.

7.5 As there are no lead times for emergency RFV procedures, it is assumed that mutual understanding between the involved countries about the importance of the emergency RFV will result in adequate processing terms.

8. AMENDMENT

8.1 When an already approved or pending RFV needs to be changed regarding dates, visitors and/or locations, an amendment referring to the original RFV must be submitted.

8.2 Amendments to approved or pending one-time and recurring visits are authorized, provided that the amendments are limited to:

(a) change of dates of visit;

(b) addition and/or deletion of visitors; and

(c) change of location.

8.3 For amendments, the standard RFV Form should be used. The type of visit cannot be changed via the amendment procedure. Amendments should refer to the original request that is still pending or already approved by the receiving NSA/DSA.

8.4 Changes to the dates of a visit, the addition or deletion of visitors or a change of location to be visited should be reported immediately to the receiving NSA/DSA via the standard procedure. Amendments will be accepted by the receiving NSA/DSA up to the number of working days (assuming that there are 5 working days in one calendar week) prior to the approved or pending visit. The lead time to process amendments is depicted in Appendix 9.

9. USE OF THE STANDARD REQUEST FOR VISIT FORM

9.1 For all types of visit, the standard RFV Form (Attachment 1 to this document) should be used.

9.2 This RFV Form has been designed for automated as well as manual use; however, the use of an electronic form and the transmission via e-mail are strongly encouraged. It is therefore essential that the detailed instructions for completion of a RFV Form described at Appendix A to Attachment 1 of this document be used to fill in each data element. To fulfil this requirement it is advised that Attachment 1 with its two Appendices be used as a hand-out to the visitor through the Security Officer of the agency, organisation or facility. Furthermore, it is advisable to translate those instructions for the use and completion of the RFV Form in the language of the user.

9.3 The completed RFV is normally an unclassified document.

9.4 Completion of the RFV Form should be in one of the official NATO languages.

ATTACHMENT 1

STANDARD FORM FOR REQUEST FOR VISIT

1. The attached guidance contains the instructions for the use and completion of a Request for Visit (RFV) Form when a visit authorization is required by the receiving organisations or governments. This form standardizes the elements required for a RFV and places them in a logical order. The RFV Form can be used for manual as well as automated processing; however, the use of an electronic form and the transmission via e-mail are strongly encouraged.

2. It is advisable to use this Attachment and its two Appendices as a hand-out to the visitor. The general principle of this RFV is that only one format will be used when a visit request is necessary.

3. The following Appendices are contained in this Attachment:

(a) Appendix A: Instructions for the use and completion of a Request for Visit; and

(b) Appendix B: Request for Visit Form (and Annexes thereto).

APPENDIX A to ATTACHMENT 1

INSTRUCTIONS FOR USE AND COMPLETION OF A REQUEST FOR VISIT

1. GENERAL INSTRUCTION

1.1 The Request for Visit (RFV) must be completed without misstatement or omission. Failure to provide all requested information will delay the processing and possibly lead to the denial of the request.

1.2 This RFV should be typed. Electronic processing and transmitting of the RFV is encouraged. The completed RFV is normally an unclassified document. The completion of the RFV Form should be in either one of the official NATO languages.

1.3 The RFV must be in the possession of the receiving host NSA/DSA in accordance with the RFV lead times detailed in Appendix 9.

1.4 The completed RFV has to be submitted to the Security Officer of the requesting agency, organisation or facility. After completion by the Security Officer of the requesting agency, organisation or facility, the RFV should be sent to the following national agency's address that will process the request (to be inserted by issuing NSA/DSA):

Name of Agency	
Address:	
Fax no:	
E-mail address:	

2. DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

2.1 These detailed instructions are guidance for the visitors and the Security Officers who complete the RFV.

HEADER	Insert full country or international organisation name (e.g. NATO CI Agency, NATO International Military Staff, SHAPE, etc) of the host.
1. **TYPE OF VISIT REQUEST**	Select the appropriate checkbox for the type of visit request. If the Emergency checkbox is selected, complete the remarks portion in item 15 of the RFV Form to explain the reasons behind the emergency RFV. If the Amendment checkbox is selected, mark the appropriate checkbox for the type of amendments and insert the reference number provided by the NSA/DSA of the original RFV that the amendment is made to. Depending on the laws/regulations of the countries involved, a one-time visit request which is issued for the posting of personnel may require additional information/documents to be included with the RFV Form.

2. **TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	Select the appropriate checkbox for the type of information/material or site access. The first box covers direct access to information/material classified NC or above. The second box shall be checked when unescorted access to Security Areas (e.g. Class I/II) is required but no direct access to information/material classified NC or above is anticipated.
3. **SUMMARY**	Insert the number of sites to be visited and the number of visitors.
4. **ADMINISTRATIVE DATA**	<u>DO NOT FILL IN - LEAVE BLANK</u> *To be completed by requesting NSA/DSA if required.*
5. **REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY**	Select the appropriate checkbox (only one box) for the entity of the requesting government agency, organisation or industrial facility. Insert the full name, full postal address (include city, province/state, and postal zone), e-mail address, facsimile number and telephone number.
6. **GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED**	Complete Annex 1 to the RFV Form to include information on all of the sites to be visited.
7. **DATE OF VISIT**	Insert the period of the visit by using numeral “day/month/year” (dd/mm/yyyy).
8. **TYPE OF INITIATIVE**	Select one item from each column as indicated.
9. **IS THE VISIT PERTINENT TO**	Select the appropriate checkbox and specify the full name of the government project/programme. Foreign Military Sales-case, etc., or request for proposal or tender offer. Abbreviations should be avoided.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION/ PURPOSE**	Give a brief description of the subject(s) motivating the visit. If known, include the details of the host Government/Project Authority and solicitation/ contract number. Abbreviations should be avoided. <u>Remarks</u>: (1) In case of a recurring visit, this item of the RFV Form should state "Recurring Visits" as the first words in the data element (e.g. Recurring Visits to discuss...). (2) It is strongly advised to repeat the subject to be discussed and/or the justification of the visit in the language of the receiving country. (3) Make sure to describe the subject to be discussed in a way that it does not reveal any classified information since the completed RFV is considered to be an Unclassified document.

11. **ANTICIPATED HIGHEST LEVEL OF INFORMATION/ MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS**	Select the appropriate checkbox for the anticipated highest level of information/material or unescorted access to security areas. If the box "Other" is checked, it shall be specified.
12. **PARTICULARS OF VISITOR(S)**	Complete Annex 2 to the RFV Form to include information on all of the visitors. When there is more than one visitor, enter the visitors' surnames in alphabetic order if possible.
13. **THE SECURITY OFFICER OF THE REQUESTING AGENCY, ORGANISATION OR INDUSTRIAL FACILITY**	This item requires the name, telephone number, e-mail address, and signature of the requesting Security Officer.
14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL**	DO NOT FILL IN - LEAVE BLANK To be completed by government/NATO certifying authority only. In accordance with the laws/regulations of the countries involved, government certifying authority must also complete this item for RESTRICTED. Note for the certifying authority: (1) Insert name, address, telephone number, and e-mail address. (2) Date and signature. (3) If the certifying authority corresponds with the requesting National Security Authority, insert in this item: "See item 14 of the RFV Form". Remark: Items 13 and 14 of the RFV Form may be completed by the appropriate official of the Embassy of the requesting country as per national legislations, policies or directives.
15. **REQUESTING SECURITY AUTHORITY**	DO NOT FILL IN - LEAVE BLANK To be completed by the requesting NSA/DSA or responsible NATO security office only as per below instructions. (1) Insert name, address, telephone number, and e-mail address. (2) Date and signature.

16. **REMARKS**	(1) In case of an emergency visit, it is mandatory to give the reasons for the emergency visit in this field of the RFV Form. The particulars of the knowledgeable person, see paragraph 7.4, should also be identified in this field of the RFV Form. (2) This item can be used for certain administrative requirements (e.g. proposed itinerary, request for hotel, and/or transportation, etc.). (3) This space is also available for the receiving NSA/DSA for processing (e.g., "no security objections", etc.). (4) In case a special briefing is required, the type of briefing and the date that the briefing was given should be stated.

ANNEX 1 TO RFV FORM	
GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED	Select the appropriate checkbox (only one box) for the government agency, organisation or industrial facility to be visited. Repeat for every site to be visited. Insert the full name, full physical address (include city, province/state, and postal zone), telephone number and facsimile number. Insert the name, e-mail and telephone number of the main point of contact or the person with whom the appointment for the visit was made. Insert the name, e-mail and telephone number of the Security Officer or the secondary point of contact. <u>Remarks</u>: (1) For visits to the United States, one RFV Form with Annexes for each agency/organisation/facility to be visited should be filled in. (2) For visits to military sites in the United States, it is mandatory to specify which military unit will be visited (e.g. Army, Air Force, Navy, Marine Corps or Defence Intelligence Agency).

ANNEX 2 TO RFV FORM	
PARTICULARS OF VISITOR(S)	Select the appropriate checkbox (only one box) for the type of employment of the visitor (e.g. military, defence public servant, government, industry/embedded Contractor, international organisation employee (e.g. NATO, EU, etc.). Repeat for every visitors. Surname: Family name. Forenames: As per passport. Rank: Insert the rank of the visitor if applicable. DOB: Insert date of birth by using numeral "day/month/year" (dd/mm/yyyy). POB: Place of birth (city-province/state-country). Nationality: Insert nationality as per passport. Security clearance level: Actual security clearance status (e.g. TS, S, C). Indicate NATO clearance (CTS, NS, NC) if the visit is related to NATO business. PP/ID Number: Enter the passport number or identification card number, as required by host government. Position: Insert the position the visitor holds in the organisation (e.g., director, product manager, etc.) Company/Agency: Insert the name of the government agency, organisation, or industrial facility that the visitor represents.

APPENDIX B to ATTACHMENT 1

All fields must be completed

REQUEST FOR VISIT

TO: _____

(Country/NATO body)

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	**3. SUMMARY**
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Agency/Facility For an amendment, insert the NSA/DSA original RFV Reference No._____	☐ NATO CONFIDENTIAL or above, or ☐ access to security areas.	No. of sites: _____ No. of visitors: _____

4. ADMINISTRATIVE DATA:	
Requestor: To:	NSA/DSA RFV Reference No._____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ NATO ☐ *Other:* _____

NAME:

POSTAL ADDRESS:
E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE *(Select one from each column)*:

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification of the selected subject:

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*:

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/ MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS

☐ NATO CONFIDENTIAL ☐ NATO SECRET

☐ COSMIC TOP SECRET ☐ Other

If other, specify:_____

12. PARTICULARS OF VISITOR(S) - *(Annex 2 to be completed)*

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY/*NATO security office*:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. REMARKS *(*Mandatory justification required in case of an emergency visit):

ANNEX 1 to RFV FORM

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
3. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
1. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
2. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:

PARTICULARS OF VISITOR(S)
3. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
4. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY: ***(Continue as required)***

Annex 3 to Appendix 8

LIST of Authorities concerned with IVCPs

COUNTRY	OFFICE	E-mail
Albania	NSA	E-mail: Sektretaria.nsa@mod.gov.al Tel: +335 4 224 5995
Belgium		
Bulgaria	State Commission on Information Security (NSA)	E-mail: dksi@government.bg
Canada	Industrial Security Sector, Public Works and Government Services Canada, Designated Security Authority (DSA).	E-mail: ssivisites.issvisits@pwgsc.gc.ca
Croatia	NSA/DSA, Office of the National Security Council	E-mail: ivcp@uvns.hr
Czech Republic	NSA	E-mail: posta@nbu.cz
Denmark	Danish Defence Intelligence Service (NSA for the Military Sphere)	E-mail: fe4222@fe-ddis.dk
Estonia	NSA	E-mail: nsa@mod.gov.ee
France	MOD acting as DSA	E-mail: In: Bagneux.sdi–sii@dga.defense.gouv.fr Out: bagneux.sdi-visit@dga.defense.gouv.fr
Germany	RFV's relating to military projects: Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support Division Z1.3 RFV's relating to civil projects: Federal Ministry for Economic Affairs and Energy (DSA) Division - ZB2	E-mail: baainbwZ1.3-bkv@bundeswehr.org Tel.: +49.261.400.13190/13192 Fax: +49.261.400.13189 E-mail: zb2-international@bmwi.bund.de Tel.: +49 228 99615 3621/3605 Fax: +49 228 99615 2603

COUNTRY	OFFICE	E-mail
Greece	Hellenic National Defence General Staff F' Division Security Directorate - Industrial Security Office	E-mail: daa.industrial@hndgs.mil.gr Tel: 00 30 210 6572022 Fax: 0030 210 6527612
Hungary	NSA	E-mail: nbf@nbf.hu Tel.: +36.17.95.23.03 Fax: +36.17.95.03.44
Iceland		
Italy	Dipartimento delle Informazioni per la Sicurezza – Ufficio Centrale per la Segretezza	E-mail: mg3437.a03@alfa.gov.it
Latvia	The Constitution Protection Bureau (SAB)	E-mail : ndi@sab.gov.lv
Lithuania	Commission for Secrets Protection Co-ordination	E-mail: nsa@vsd.lt Tel.: +370 706 66701(03) +370 706 66708 Fax: +370 706 66700
Luxembourg	Autorité nationale de Sécurité 207, route d'Esch L-1471 Luxembourg	E-mail: ans@me.etat.lu Tel.: +352.24.78.2210 Fax.: +352.24.78.2243
Netherlands	NSA/DSA	E-mail: NSA**:** NIVCO@minbzk.nl DSA**:** indussec@mindef.nl*
Norway	The Norwegian Defence Security Agency	E-mail: fsa.kontakt@mil.no
Poland	NSA	E-mail: nsa@abw.gov.pl
Portugal	NSA/GNS –Rua da Junqueira, 69, 1300-342 Lisboa	E-mail: geral@gns.gov.pt
Romania	National Registry Office for Classified Information (ORNISS)	E-mail: relatii.publice@orniss.ro
Slovakia	NSA	E-mail: podatelna@nbusr.sk

* For visits of military and civilian personnel of NLD MoD and for visits to NLD military premises'

COUNTRY	OFFICE	E-mail
Slovenia	NSA	E-mail: gp.uvtp@gov.si
Spain	NSA	E-mail: sp-ivtco@areatec.com
Turkey		
United Kingdom	Defence Equipment and Support PSyA, Ministry of Defence, International Visits Control Office, Poplar-1 # 2004, Abbey Wood, Bristol, England, BS34 8JH, UK	Email: Desinfra-ivco@mod.uk Tel.: + 44 117 91 33840 Fax.: + 44 117 91 34924
United States	For Department of Defense: Mr. Mario Rubio International Security Directorate Office of the Under Secretary of Defense (Policy) Defense Technology Security Administration 4800 Mark Center Drive Suite 07E12 Alexandria, VA 22350	E-mail : Mario.rubio@dtsa.mil Tel.: +1.571.372.2561 Fax.: +1 571.372.2559

INTERNATIONAL VISITS PROCESSING TIMES/LEAD TIMES
And
NU OR NR NOTIFICATION REQUIREMENTS

The national requirements for RFV for NU or NR notification shall not put additional obligations on other NATO nations or Contractors under their jurisdiction.

1. The following table depicts the number of working days prior to the date of the one-time visit or the date of the first recurring visit that the request should be in the possession of the receiving host NSA/DSA.

2. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Albania	No	Yes	20	10
Belgium	No	No	20	09
Bulgaria	No	Yes	20	No deadline
Canada	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Croatia	No	No	20	7
Czech Republic	No	Yes	20	10
Denmark	No	No	07	05
Estonia	No	Yes	20	05
France	No	No	15	05
Germany	No	No	20	10
Greece	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Hungary	No	No	20	10
Iceland	-	-	-	-
Italy	No	Yes	20	07
Latvia	No	No	20	05
Lithuania	No	Yes	20	10
Luxembourg	No	Yes	20	09
Netherlands	No	Yes required for military facilities only	10	05
Norway	No	Yes	10	05
Poland	No	No	25	10
Portugal	No	No	21	07

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Romania	No	No	25	10
Slovakia	No	No	20	10
Slovenia	No	Yes	21	07
Spain	No	No	20	08
Turkey	Yes For military facilities only	Yes For military facilities only	21	10
United Kingdom	No	No	20	05
United States	No	Yes	21	05

NATO Agency	NUMBER OF WORKING DAYS	
	Request	Amendment/ Change
NATO Allied Ground Surveillance Management Agency (NAGSMA)	3	2
NATO Helicopter Design & Development Production & Logistics management (NAHEMA)	3	
NATO Medium Extended Air Defence System Design & Development, Production & Logistics Management Agency (NAMEADSMA)	3	
NATO AEW&C Programme Management Agency (NAPMA)	3	1
NATO Communications and Information Agency (NCIA)	3	
NATO EF2000 & TORNADO Development, Production & Logistics Management Agency (NETMA)	3	1
NATO Support Agency (NSPA)	3	1

SECURITY ACKNOWLEDGEMENT
(in case of Hand Carriage)

[LETTERHEAD]

SECURITY ACKNOWLEDGEMENT

DECLARATION

(name, forename)

(name of company)

(position in company)

I have been briefed on and provided with instructions concerning the handling and custody of classified documents/equipment to be carried by me. I have read and understood their contents.

I shall always retain en route the classified documents/equipment and shall not open the package unless required by the Customs Authorities.

Upon arrival, I shall hand over the classified documents/equipment intended for the receiving company/organisation, against receipt, to the designated consignee.

(**Place and date**) (**Signature of courier**)

Witnessed by:

(**Security Officer's signature**)

APPENDIX 11
ANNEX 1
AC/35-D/2003-REV5

COURIER CERTIFICATE

[LETTERHEAD] COURIER

CERTIFICATE **PROGRAMME**

TITLE (optional)

COURIER CERTIFICATE NO. …….. (*)

FOR THE INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer:

Mr./Ms. (**name/title**):

born on: (**day/month/ year**), in (**country**):

a national of (**country**):

holder of passport/identity card no.: (**number**)

issued by: (**issuing authority**)

on: (**day/month/year**)

employed with: (**company or organisation**)

is authorised to carry on the journey detailed below the following consignment:

(**Number and particulars of the consignment in detail, i.e., No. of packages, weight and dimensions of each package and other identification data as in shipping documents**)

……
……

* May also be used by security guards.

The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- The material comprising this assignment is classified in the interests of the security of:

(NATO, the country of origin of the shipment and that of the destination shall be indicated. The country(ies) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly- authorised persons or those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police, and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

ITINERARY

From: (**originating country**) ……..

To: (**country of destination**) ……

Through: …… (**list intervening countries**)

Authorised stops: …… (**list locations**)

Date of beginning of journey: …… (**day/month/year**)

Signature of Security Officer of the facility	Signature of the Designated Security Authority
……. (name)	……. (name)
Facility's stamp	Official stamp or NSA/DSA's seal
…….	…….

NOTE: To be signed on completion of journey:

I declare in good faith that, during the journey covered by this ″Courier Certificate″, I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature: …….

Witnessed by: …….
(signature of Security Officer of the facility)

Date of return of the ″Courier Certificate″: …….
(day/month/year)

[LETTERHEAD]

Annex to the "Courier Certificate", No. …….
for the International Hand Carriage of Classified Material

INSTRUCTIONS FOR THE COURIER ([6])

1. You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE"/"MULTI-TRAVEL COURIER CERTIFICATE" has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behaviour, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security regulations.

2. The following general points are brought to your attention:

(a) you will be held liable and responsible for the consignment described in the Certificate;

(b) throughout the journey, the classified consignment must stay under your personal control;

(c) the consignment will not be opened en route except in the circumstances described in sub-paragraph (j) below;

(d) the classified consignment is not to be discussed or disclosed in any public place;

(e) the classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilised. You are to be instructed on this matter by your facility Security Officer;

(f) while hand carrying a classified consignment, you are forbidden to deviate from the travel schedule provided;

(g) in cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (l) below. If you have not received these details, ask for them from your facility Security Officer;

(h) you and the facility Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current;

(i) if unforeseen circumstances make it necessary to transfer the consignment to other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (l);

[6] May also be used by security guards.

(j) there is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your Certificate and this note and insist on showing them to the actual senior Customs, Police, and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public;

You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination.

You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving facility Security Officer and the dispatching facility Security Officer, who should be requested to inform the NSA/DSA of their respective government.

(k) upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the facility or agency receiving the consignment or by an NSA/DSA of the receiving government;

(l) along the route you may contact the following officials to request assistance :

……

……...

……...

……...

……..

……..

ATTACHMENT 2
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV5

Multi-Travels Courier Certificate

[LETTERHEAD]

PROGRAMME TITLE (optional)

MULTI-TRAVELS COURIER CERTIFICATE N° …….

FOR INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENTS AND/OR COMPONENTS

This is to certify that the bearer

Mr/Ms (name/title)

born on (day/month/year) ……. in (country) ……..……,

a national of (country) ……..

holder of passport or identity card n° …….

issued by (issuing authority): …….

on (day/month/year):…….

employed with (facility): ……..……...

is authorized to carry the classified documents, equipments and/or components between the following countries:
……...

The bearer above is authorized to use the present certificate as many times as necessary, for classified shipments between the countries here above until (day / month / year): …….

Each sending is attached with the shipment description.

The attention of Customs, Police and/or Immigration Officials is drawn to the following:

- The material comprising each consignment is classified in the interest of the security of:

(**NATO, the country of origin of the shipment and that of the destination shall be indicated. The country(ies) to be transited also may be indicated).**

- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

Customs, Police and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

Instructions for the Courier (Attachment 1 of this Appendix) are also applicable.

ATTACHMENT 2
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV5

Attachment to multi-travels courier certificate No:.....

Description of consignment nr: ……..

Transport from (**day/month/year**): ……. to (**day/month/year**): …….

Bearer (name): ……

Itinerary: from (originating country) ……. to (destination country) …….
through (crossed countries) …….
authorized stops (list of locations): ……

References of receipt or inventory list:

Description of the consignment (number of package, dimensions and, if needed, weight of each package):

Officials you may contact to request assistance

Signature of the consignor's security officer ……	Signature of the NSA/DSA ……
Facility stamp ……	Official stamp or NSA/DSA's seal ……

Note to be signed on completion of each journey:

I declare in good faith that, during the journey covered by this "shipment consignment", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature: ……..

Witnessed by (name and signature of consignor's security officer): …….

Date of return of the "shipment consignment" (day/month/year): …….

INTERNATIONAL TRANSPORTATION PLAN

[LETTERHEAD]

TRANSPORTATION PLAN FOR THE MOVEMENT OF CLASSIFIED CONSIGNMENTS (INSERT NAME OF PROGRAMME OR PROJECT)

1. INTRODUCTION

This transportation plan lists the procedures for the movement of classified (**insert Programme/Project/Contract name**) consignments between (**insert Programme Participants**).

2. DESCRIPTION OF CLASSIFIED CONSIGNMENT

Provide a general description of the consignment to be moved. If necessary, a detailed, descriptive listing of items to be moved under this plan, including military nomenclature, may be appended to this plan as an annex. Include in this section a brief description as to where and under what circumstances transfer of custody will occur.

3. IDENTIFICATION OF AUTHORISED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organisation, the authorised representatives of each Programme/Project participant who will receipt for and assume security responsibility for the classified consignment. Mailing addresses, telephone numbers, fax numbers and network addresses should be listed for each country's representatives.

4. DELIVERY POINTS

(a) Identify the delivery points for each participant (e.g., ports, railheads, airports, etc.) and how transfer is to be effected;

(b) describe the security arrangements that are required while the consignment is located at the delivery points; and

(c) specify any additional security arrangements, which may be required due to the unique nature of the movement or of a delivery point (e.g., an airport freight terminal or port receiving station).

5. IDENTIFICATION OF CARRIERS

Identify the commercial carriers, freight forwarders and transportation agents, where appropriate, that might be involved to include the level of security clearance and storage capability.

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

(a) List, by participants, the storage or processing facilities and transfer points that will be used; and

(b) describe specific security arrangements necessary to ensure the protection of the classified consignment while it is located at the storage / processing facility or transfer point.

7. ROUTES

Specify in this section the routes for movements of the classified consignments under the plan. This should include each segment of the route from the initial point of movement to the ultimate destination including all border crossing. Routes should be detailed for each participant in the logical sequence of the shipment from point to point. If overnight stops are required, security arrangements for each stopping point should be specified. Contingency stop-over locations should also be identified as necessary.

8. PORT SECURITY AND CUSTOMS OFFICIALS

In this section, identify arrangements for dealing with customs and port security officials of each participant. The facility must verify that the courier has been provided with the necessary documentation and is aware of the rules necessary to comply with customs and security requirements. Prior co-ordination with customs and port security agencies may be required so that the Project/Programme movements will be recognised.

Procedures for handling custom searches and points of contact for verification of movements at the initial despatch points should also be included here.

9. COURIERS

When couriers are to be used, relevant provisions specified in Appendix 10 and 11 apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to inventory the movement and to examine all documentation upon receipt of the movement and:

(a) notify the dispatcher of any deviation in routes or methods prescribed by this plan;

(b) notify the dispatcher of any discrepancies in the documentation or shortages in the shipment; and

(c) clearly state the requirement for recipients to promptly advise the NSA/DSA of the dispatcher of any known or suspected compromise of classified consignment or any other exigencies which may place the movement in jeopardy.

11. DETAILS OF CLASSIFIED MOVEMENTS

This section should include the following items:

(a) identification of dispatch assembly points;

(b) packaging requirements that conform to the national security rules of the Project/Programme participants. The requirements for dispatch documents seals, receipts, and storage and security containers should be explained. Any unique requirement of the Projects/Programme participants should also be stated; documentation required for the dispatch points;

(c) courier authorisation documentation and travel arrangements;

(d) procedures for locking, sealing, verifying and loading consignments. Describe procedures at the loading points, to include tally records, surveillance responsibilities and witnessing of the counting and loading arrangements;

(e) procedures for accessibility by courier to the shipment en route;

(f) procedures for unloading at destination, to include identification of recipients and procedures for change of custody, and receipt arrangements;

(g) emergency communication procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency; and

(h) procedures for identifying each consignment and for providing details of each consignment (see Attachments); the notification should be transmitted no less than six working days prior to the movement of the classified consignment.

12. RETURN OF CLASSIFIED MATERIAL

This section should identify requirements for return of classified material to the manufacturer or sending country (e.g., warranty, repair, test and evaluation, etc.).

(a) Samples of these forms should be included, as appropriate, as enclosures to the plan as necessary.

(1) packing list;

(2) classified material receipts;

(3) bills of lading;

(4) export declaration;

(5) waybills;

(6) other nationally-required forms.

(b) NSAs/DSAs reserve their right to add additional measures in the course of establishing the Transportation Plan if required.

ATTACHMENT 1
APPENDIX 12
ANNEX 1
AC/35-D/2003-REV5

NOTICE OF CLASSIFIED CONSIGNMENT

NOTICE OF (INSERT PROGRAMME/PROJECT NAME)

CONSIGNMENT APPROVED TRANSPORTATION PLAN REFERENCE No.
(INSERT REFERENCE)

REPLY BEFORE: (insert date)

1. Consignor / consignee:
(include the name, telephone number and address of the person(s) responsible for the consignment at both locations).

2. Government Designated Personnel:
(include name, telephone number and address of releasing and receiving authorised representatives, as applicable).

3. Description of consignment:

   (a) contract or Tender Number;

   (b) export licence or other applicable export authorisation citation;

   (c) consignment description:
   (describe items to be shipped and their classification);

   (d) package description:
   - type of package (wood, cardboard, metal, etc.);
   - number of packages;
   - number of enclosed classified items in each package;
   - package dimensions/weight:
     (include length, width, height and weight);

   (e) indicate if package contains any hazardous material.

4. Routing of consignment:

   (a) date / time of departure;

   (b) date / estimated time of arrival;

   (c) routes to be used between point of origin, point of export, point of import and ultimate destination:
   (identify specific transfer points; use codes that appear in transportation plan, if applicable);

   (d) method of transport for each portion of the shipment:
   (include names and addresses of all carriers and flight, rail or ship numbers, as applicable);

   (e) freight forwarders/transportation agents to be used:
   (include name, telephone number, address of companies if not specified in transportation plan);

   (Note: ***Consignor must re-verify clearance and safeguarding capability of these entities prior to releasing shipments*****);**

(f) customs or port security contacts:
(list names and telephone numbers, if different from approved transportation plan procedures).

5. Name(s) and identification of authorised courier.

AUTHORISATION FOR SECURITY GUARDS

Valid until ……

This is to certify that Mr./Ms. ……..

a member of the (firm/establishment) ……..

……

holder of Passport No. ……. is authorised to act as security guard on the journey detailed below for transportation by:

- air*
- rail*
- road*
- sea*

of a classified consignment relating to the work carried out by the above-mentioned firm/ establishment in the interests of the **North Atlantic Treaty Organisation**.

ITINERARY

From … …… To … …… Approximate Date …….

Stamp of Firm/Establishment Signature of Authorising Official

Stamp of Government Agency Signature of Authorising Official

* Delete as applicable

APPENDIX 14
ANNEX 1
AC/35-D/2003-REV5

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE (PSCC)

1. Certification is hereby given that:

Full Name:

.....

Date and Place of Birth:

.....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including[1]:

.....
.....

2. The validity of this certificate will expire not later than[2]:

.....

Signed:

Title: Official government stamp

Date of Issue:

Contact details of the issuing authority (Phone, e-mail, fax):

.....

---

1 Insert, as appropriate, one or more of the following:

(a) COSMIC TOP SECRET
(b) NATO SECRET
(c) NATO CONFIDENTIAL
(d) COSMIC TOP SECRET ATOMAL
(e) NATO SECRET ATOMAL
(f) NATO CONFIDENTIAL ATOMAL

2. The date of expiry shall conform with the provisions of paragraph 18 of the Directive on Personnel Security.

(*) The marking is not part of the template.

APPENDIX 15
ANNEX 1
AC/35-D/2003-REV5

ATTESTATION OF NATO PERSONNEL SECURITY CLEARANCE (APSC)

1. Attestation is hereby given that:

Full Name ……

Date of Birth ……

Place of Birth ……..

Nationality ……

Where employed ……

Purpose and Duration of Visit ……..
……..
……..

Holder of Passport/Identity Card No. .....……
Issued at ..... Dated .....……

Military Rank and Number (where applicable) .....
.....
has been granted access to NATO information classified up to and including ..... in accordance with current NATO security regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and has been briefed accordingly by
.....

Signed:

Title: Official stamp

Date of Issue:

2. The validity of the attestation will expire no later than:
.....

3. Issued by …….
(Member nation or NATO civil or military body)

Date and Place of Issue:
.....

Contact details of the issuing authority (Phone, e-mail, fax):
.....

(*) The marking is not part of the template.