NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

8 September 2009

DOCUMENT
AC/35-D/2003-REV4

NATO SECURITY COMMITTEE

DIRECTIVE on INDUSTRIAL SECURITY

Note by the Chairman

1. At Annex is the fourth revision of the Directive on 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. This revision reflects approved changes concerning Contractors. These changes are reflected in paragraphs 2, 6, 7, 30, 36-39 and 114. Appendix 12 (International Visits Processing Times) has been updated.

3. This document has been approved by the NATO Security Committee under the silence procedure (AC/35-WP(2009)0005 refers) and will be subject to periodic review.

(Signed) Michael T. Evanoff

Annex: 1

Action officer: Robert Keil, NOS/POB, ext. 4084
Original: English

ANNEX 1
AC/35-D/2003-REV4

DIRECTIVE ON INDUSTRIAL SECURITY

INTRODUCTION

1. This Industrial Security Directive is published by the NATO Security Committee (AC/35) in support of Enclosure "G" to the NATO Security Policy (C-M(2002)49). This directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This directive addresses the following aspects :

(a) negotiation and letting of NATO classified contracts;

(b) security requirements for NATO classified contracts;

(c) release of NATO classified information in contracting;

(d) consortia and joint ventures;

(e) industrial security clearances for NATO contracts;

(f) personnel security clearances for facility employees;

(g) international transportation of NATO classified material;

(h) international visit procedures;

(i) personnel on loan within a NATO project / programme; and

(j) NATO classified contracts involving non-NATO Nations.

2. The provisions outlined in this Directive are applicable to Contractors and Consultants in the meaning provided by the following definitions :

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

Consultant: An individual who serves in an independent advisory capacity. A consultant expresses views, gives opinions on problems or questions as requested or advice. The work performed under contract is the provision of advice. Therefore, a Consultant is considered the same as a Contractor.

NEGOTIATION AND LETTING OF NATO CLASSIFIED CONTRACTS

Prime Contracts

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). The prime contractor shall be responsible for all sub-contract activities and shall hold a Facility Security Clearance (FSC), where appropriate. A diagram showing security policy and liaison links related to NPLO programme/projects is at Appendix 2.

4. Before negotiating a NATO classified prime contract classified NC and above, the NATO Programme/Project Agency/Office shall contact the NSA/DSA of the NATO nation in which the potential prime contractor is registered or incorporated to ensure that the potential contractor holds a FSC at least equal to the classification level of the information that will be required during the negotiation of the contract. If the potential contractor has no FSC or it is not at the required level, the NPA/NPO shall forward a request for the initiation/upgrading of a FSC to the appropriate NSA/DSA, using the "Facility Security Clearance Information Sheet" (FIS) at Appendix 3. The NPA/NPO shall include the highest NATO security classification of the information required, as well as the nature of the material or technology to which access is required.

5. All invitations to bid for NATO classified contracts shall contain a clause requiring a prospective contractor who does not submit a bid to return to the NPA/NPO, by the date set for the opening of bids, all documents which were provided to enable the contractor to submit a bid. Similarly, an unsuccessful bidder shall be required to return all documents after a period of time stipulated by the NPA/NPO (normally within 15 days after notification that a bid or negotiation proposal was not accepted).

6. In case NATO information classified NC, or above needs to be furnished to the bidder, or potential contractor, or shall be made accessible to bidder's, or contractor's representatives during the pre-contractual stage the NPA/NPO who negotiates the contract shall ensure that, for contracts classified NC and above :

(a) the potential contractor holds a FSC at the appropriate level for access to classified information and material at an authorized facility; and

(b) records are kept of all participants in the negotiation meetings, including their names, the organisation represented, and the time and purpose of the meeting. Such records shall be retained for a minimum of two years, after which they may be destroyed.

Contracts Requiring Provision of Security Cleared Personnel only

7. For contractors, or sub contractors working with, or accessing NATO information classified NC, or above, whether at NATO premises or at an approved contractor's facility, the procedures set out for Prime and Sub Contracts shall apply accordingly. In this case, a FSC without storage capabilities shall be issued by the appropriate NSA/DSA in compliance with national regulations.

Sub-Contracts

8. After a prime contract has been let, a prime contractor may negotiate sub-contracts with other contractors, i.e., sub-contractors. If there are to be sub-contracts for which permission must be obtained from the programme/project management office/agency prior to negotiation or award, contractors shall be notified by the applicable NPA/NPO :

(a) that they must obtain such permission; and

(b) that they must seek such permission prior to submitting the request for verification or initiation of the FSC for a potential sub-contractor. If deemed necessary, both actions may be accomplished simultaneously, with the consent of the programme/project management agency/office. Close co-operation between the facility Contract Manager and the facility Security Officer will be required.

9. When the contractor and sub-contractor are registered/incorporated in the same NATO nation, permission to negotiate will not be required from the NPA/NPO, unless otherwise required in the contract document. The NPA/NPO will, however, be informed by the contractor that a sub-contract has been negotiated, and be given all contractual details relevant to the security of the NATO classified information involved. It shall be the responsibility of the contractor to ensure through the NSA/DSA that all sub-contractors comply with the appropriate security requirements.

10. The following additional requirements shall apply for all sub-contracts :

(a) before entering into negotiations, the Security Officer of the contractor that is to let the subcontract shall initiate a request as outlined in paragraph 3 above, through his/her NSA/DSA, with respect to a FSC for the potential sub-contractor;

(b) when the potential sub-contractor is under the jurisdiction of the NSA/DSA of another nation, the requesting contractor's NSA/DSA shall forward the request to that NSA/DSA;

(c) the NSA/DSA of the potential sub-contractor shall return the completed FIS request, together with the required information to the requesting contractor, through the responsible NSAs/DSAs. A copy of the FIS shall be forwarded by the requesting contractor's NSA/DSA to the responsible management agency/office;

(d) upon receipt of confirmation that the sub-contractor has been granted the appropriate FSC, the contractor may open negotiations with the potential sub-contractor. All classified information released by the contractor to the potential sub-contractor shall be through, or in compliance with instructions from, the contractor's NSA/DSA. It remains the responsibility of the NSA/DSA of the sub-contractor to make the appropriate arrangements to ensure the protection of all classified information that is received. Such

arrangements shall be co-ordinated with the NSA/DSA of the contractor that is to let the sub-contract, in accordance with arrangements set out in the Project Security Instructions (PSIs); and

(e) the contractor shall comply with the requirements set forth in paragraphs 5 and 6 above with respect to negotiations with the potential sub-contractor. NATO classified information released to the potential sub-contractor shall be returned to the contractor at such time as may be designated by the NPA/NPO or the contractor.

11. For sub-contracts classified NR, the responsibilities outlined in paragraphs 8 to 10 above, shall be taken by the NPA/NPO and/or the prime contractor. An FSC is not required. Government oversight, where required, shall be achieved through the applicable National security rules and regulations.

Letting of Contracts

12. Upon letting the prime contract, the NPA/NPO shall notify the NSA/DSA of the prime contractor that a contract has been let and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to both the NSA/DSA and the prime contractor. An example of a SAL is shown at Appendix 4.

13. Upon letting a sub-contract classified NC or above, the contractor that lets the sub-contract shall notify his parent NSA/DSA, the prime contractor, and the NPA/NPO. For sub-contracts classified NC or above, the sub-contractor's NSA/DSA shall ensure that the sub-contractor makes the necessary arrangements for the protection of all NATO classified information released to the sub-contractor. For sub-contracts classified NR, the NSA/DSA need not be notified, unless specifically required by National security rules and regulations. The contractor shall ensure that the sub-contractor is contractually obliged to comply with the provisions of the applicable PSI or SAL.

14. When the potential sub-contractor is registered or incorporated in another NATO nation, the NSA/DSA of the contractor that is letting the contract shall pass the information regarding the PSI or SAL to the NSA/DSA of the potential sub-contractor, which will be responsible for enforcing the actions related to the PSI or SAL. When, however, a NSA/DSA does not wish to receive this information automatically, they may mutually agree to obtain it on a "specific request" basis only.

15. Prior to a classified prime contract or sub-contract classified NC or above being let, in light of the requirements of the PSI or the SAL respectively attached to the contract, the NSA/DSA that is responsible for the contractor or sub-contractor facility shall :

(a) provide to the NPA/NPO or the contractor that is to let the contract, as applicable, verification that the requisite FSC has been provided, using a FIS format;

(b) ensure that the requisite PSCs are issued for the facility's personnel who will require access to the classified aspects of the NATO contract; and

(c) ensure that the personnel mentioned in sub-paragraph (b) above are briefed on NATO security regulations.

16. The contract shall not enter into force until all of the above measures have been completed.

17. 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 5 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 classified contracts 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.

18. 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.

SECURITY REQUIREMENTS FOR NATO CLASSIFIED CONTRACTS

19. In accordance with NATO security policy, NATO classified contracts for Major Programme/Projects shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other NATO classified contracts shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a “Security Classification Checklist”. The PSI and/or SAL shall be the single source document for the programme/project and, depending on the scope of the programme/project, shall be used, as required, to support and supplement NATO Security Policy and supporting directives in order to standardise programme/project security procedures among the participating nations and NATO bodies, and their contractors.

Project Security Instructions (PSIs)

20. When the PSI is used, the responsible NPA/NPO shall develop it and the Programme/Project Security Classification Guide within a specified time period previously agreed by the NSAs/DSAs, unless otherwise specified in a programme/project agreement. The PSI and the Programme/Project Security Classification Guide shall describe the methods by which programme information and material will be classified/declassified/downgraded, marked, processed, handled, transmitted and safeguarded. The PSI shall include procedures for releasing classified and, if applicable, other programme/project information requiring control, to third parties, including public release. Both documents will be approved by the NSAs/DSAs of the participants and shall

be applicable to all individuals, including contractor employees, participating in the programme.

21. By the terms of the contract, the contractor or sub-contractor shall be specifically obliged to comply with the requirements listed below, which may be included in the PSI or SAL. The contractor or sub-contractor shall :

(a) appoint an official who will be responsible for supervising and directing security measures in relation to the contract or sub-contract;

(b) maintain a continuing relationship with the responsible NSA/DSA;

(c) abstain from copying any NATO classified information provided or generated under the contract, except as permitted by the contract or with the consent of the contracting office/agency;

(d) furnish to the responsible NSA/DSA, on request, information pertaining to all individuals who will be required to have access to NATO classified information;

(e) limit the dissemination of NATO classified information on a need to know basis to the least number of individuals consistent with the proper execution of the contract or sub-contract;

(f) maintain at the place of work a current record of those employees who have been cleared and approved for access to NATO classified information in support of the contract or sub-contract. This record shall show the date and level of clearance, and the date of re-investigation;

(g) deny access to NATO classified information to any person other than those individuals identified to have access, as indicated above;

(h) comply with any request from the responsible NSA/DSA that individuals entrusted with NATO classified information be required to sign a statement in which they agree to safeguard that information and signify their understanding of their obligations, as well as penalties under national legislation or executive order if they fail to so safeguard the information;

(i) report to the NSA/DSA any breaches or suspected breaches of security, suspected sabotage, subversive or terrorist activities, any information giving rise to doubts as to the trustworthiness of an employee, any changes that may occur in the ownership, control or management of the facility, any changes that affect the security arrangements and security status of the facility, and such other reports as may be required by the NSA/DSA (e.g. reports on the holdings of NATO classified information);

(j) place any sub-contractor under security obligations no less stringent than those applied to his own contract or sub-contract;

(k) undertake not to use, without the specific written permission of the NPA/NPO, other than for the specific purpose of the contract or sub-contract, any NATO classified information which is provided or produced (including all reproductions thereof) pursuant to the contract or sub-contract;

(l) return to the NPA/NPO or to the contractor that let the sub-contract, all NATO classified information, unless it has been destroyed, or its retention has been duly authorised with the approval of the NPA/NPO or the contractor, as applicable. Such information shall be returned as the NPA/NPO or the contractor may specify;

(m) ensure that destruction is regulated and recorded following applicable NATO security procedures; and

(n) comply with any procedure that is, or may be, established by the NSAs/DSAs regarding the safeguarding and release of information related to the contract or sub-contract.

Preparation of Security Classification Guidance

22. The following general principles shall be observed in connection with the security classification requirements of NATO classified contracts (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.

23. 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.

24. The Programme/Project Security Classification Guide should be developed in close co-operation with industry. A “Security Classification Board” may be established to assist in the preparation of classification guidance. Such Boards should be comprised of representatives of the NSAs/DSAs of the participating nations and the NPA/NPO, and advised by the participating prime contractor(s). The Programme/Project Security Classification Guide will be subject to regular review and revision, as determined by the participants.

25. 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 Security Classification Guide.

26. 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 Classification Guide.

27. The classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

28. The release of NATO classified information shall be with the consent of the originator and in accordance with Enclosure "E" of NATO Security Policy and the supporting security of information directive. Specifically, :

(a) the responsibility for decisions on the release of NATO classified information connected with a contract or sub-contract rests primarily with the Programme/Project Manager (PM). The PM shall ensure that all such decisions are consistent with the terms of any programme/project agreement, and in compliance with the PSI or SAL, as applicable, including obtaining the consent of the originator; and

(b) in the case of NPLO contracts or sub-contracts, when considering the release of NATO classified information, even within NATO, the terms of the particular NPLO charter and the programme/project PSI or SAL shall be consulted before the information is released. The charter, or the security instructions for the programme/project, may prohibit the release of classified information to non-participating NATO nations, except with the agreement of all the participating member nations.

CONSORTIA AND JOINT VENTURES

29. In the context of this directive, a consortium or joint venture is an association of several business companies, set up to undertake negotiations or contracts with an NPA/NPO. The following shall apply in dealing with consortia and joint ventures :

(a) a contracting consortium or joint venture has the same status as any other prime contractor or sub-contractor in regard to its dealings with a contracting NPA/NPO. The responsible NPA/NPO shall hold a verification of the FSC for the consortium or joint venture, and each constituent element that participates in a NATO classified contract;

(b) a consortium or joint venture requiring access to NATO information classified NC or above shall be issued a FSC by the NSA/DSA of the country in which it is located and incorporated to do business. If constituent elements of the consortium or joint venture require access to such information, they shall be issued a FSC by the NSA/DSA of the NATO nation in which they are located and incorporated to do business;

(c) the verification of PSCs for employees of a consortium or joint venture who are assigned from its constituent elements shall be provided by the NSAs/DSAs of the NATO nation in which the constituent elements are registered or incorporated; and

(d) the PSI or SAL, as applicable, shall include provisions to ensure that the security measures incorporated in it are equally binding on all constituent elements of any contracting consortium or joint venture that are participating in a NATO programme/project requiring access to NATO classified information.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

Facility Security Clearances (FSC)

Issuing Facility Security Clearances

30. In accordance with NATO Security Policy requirements, the NSA/DSA of each NATO nation is responsible for granting a Facility Security Clearance for facilities located on their territory and which are involved in NATO classified contracts. Prior to issuing a FSC an assessment shall be made:

(a) of the integrity and probity of the company which is to be entrusted with NATO classified material at CONFIDENTIAL and above;

(b) of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other

individuals who may, by virtue of their association, position or employment, be required to have access to NATO classified information or supervise a NATO classified contract, 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.

31. The following minimum criteria shall be applied by the NSA/DSA in issuing a FSC :

(a) that the company must establish a security system at the facility which covers all appropriate security requirements for the protection of NATO material and information classified at CONFIDENTIAL 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 NATO classified material at CONFIDENTIAL 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 NATO classified information at CONFIDENTIAL and above; and

(d) that the company responsible for the facility shall appoint a Security Officer responsible for security who is in a position to report directly to an appointed member of the Managing Board of the company.

32. In granting a 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 facility, a realignment of the business associations, the replacement of any of its principal officers or directors, or a change in the facility's physical location, an alteration to the premises it occupies, or a variation in its security procedures).

33. 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 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.

34. The responsible NSA/DSA will verify the issuing of the FSC, when requested, in the FIS format at Appendix 3.

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

Contractor Personnel Performing Works on NATO Premises, or on other Contractor's Facilities

36. Contractor, or sub-contractor 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 project/programme or any other type of NATO classified contract requiring access to NATO classified information NC, or above shall hold a PSC at the requisite level.

37. The facility of the contractor/sub-contractor shall also hold a FSC without storage capabilities for NC and above where required by applicable national regulations.

38. NATO classified information made accessible to such personnel on NATO premises or contractor's facilities shall be treated as if officially provided to the contractor or sub-contractor.

39. In case NATO information classified NC or above needs to be removed by a contractor from NATO premises, or from contractor's facilities, the contractor's facility shall hold a FSC with storage capabilities for NATO classified information at the requisite level.

Changes to or Revocation of Facility Security Clearances

40. Should an NSA/DSA change or withdraw a FSC that it has issued, the NSA/DSA shall at once notify any other NSA/DSA or NATO Programme/Project Management Agency/Office to which it has provided a clearance notification.

41. If a FSC is revoked or withheld from a facility by its parent NSA/DSA, that fact must not be disclosed to the facility by another NSA/DSA, except with prior permission from the parent NSA/DSA.

PERSONNEL SECURITY CLEARANCES FOR CONRACTORS

42. The issuing of PSCs shall be in accordance with Enclosure "C", Personnel Security to NATO Security Policy and its supporting personnel security directive.

Issuing and verification of a PSC

43. If a PSC is required for a contractor's employee whose citizenship is that of another NATO nation, the NSA/DSA of the nation in which the contractor is located and incorporated shall obtain a NATO Personnel Security Clearance Certificate or assurance from the employee's country of citizenship.

44. As an alternative, having the character of subsidiarity, the NSA/DSA of the nation in which the contractor is located and incorporated may grant a PSC to an employee holding the 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 in which the contractor is located and incorporated 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 level; and

(d) an assurance is obtained 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 national security clearance by the parent nation.

45. If a facility wishes to employ a national of a non-NATO nation in a position that requires access to NATO classified information, it is the responsibility of the NSA/DSA of the nation in which the hiring facility is located and incorporated, to carry out the security clearance procedure prescribe herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure "C" and the supporting personnel directive.

46. The verification that an individual has a valid PSC may either be in the form of a Visit Request, as described in this Directive, or in the form of a Certificate of Security Clearance as shown in Appendix 2 to the Directive on Personnel Security.

Procedures to be Followed when a Security Clearance is Denied

47. Should the NSA/DSA of the parent nation of an individual decide not to grant a security clearance, it will immediately inform the NSA/DSA of the nation of origin of the facility that requested the PSC.

48. Equally, should the NSA/DSA of the nation in which the contractor is located and incorporated that requested the PSC decide not to grant a security clearance, it will immediately inform the NSA/DSA of the individual's country of citizenship, giving the reasons for denial.

49. The NSA/DSA of the nation in which the contractor is located and incorporated shall inform the facility where the individual is employed of the denial of a PSC. Other NSAs/DSAs to whom clearance verification has been provided shall be notified of the denial.

50. On receiving the information that a PSC has been denied, the facility which employs the individual shall ensure that he is not involved in classified work.

51. The NSA/DSA that is responsible for granting or denying a clearance shall decide whether the employee concerned is to be informed that the security clearance is denied.

Procedures to be Followed when a Security Clearance is Revoked

52. If the NSA/DSA of the nation in which the contractor is located and incorporated learns adverse information about an individual who is a national of another NATO member nation, it shall immediately inform the NSA/DSA of the individual's country of citizenship in order to determine whether he shall continue to hold a PSC.

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

54. In the case of an individual who has been granted a PSC in accordance with the provisions of paragraph 44 above, the NSA/DSA of the individual's country of citizenship, after receiving the adverse information, shall determine whether the information would be an obstacle to the granting of a national security clearance and inform the NSA/DSA of the nation in which the contractor is located and incorporated in order to determine whether he shall continue to hold a PSC.

55. If an employee's security clearance has been revoked, the NSA/DSA of the nation in which the contractor is located and incorporated shall inform the facility where the individual is employed. Other NSAs/DSAs to whom clearance verification has been provided shall be notified of the revocation.

56. On receiving the information that a PSC has been revoked, the facility which employs the individual shall ensure that he is removed from classified work.

Provisional Security Clearances

57. In exceptional cases, where the attainment of major military objectives would otherwise be impaired, or when other compelling reasons are present, and it is not possible to obtain the clearance in time by prioritising a particular request, provisional appointments may be made or one-time access may be permitted following the procedures set out in the personnel security directive. However, such access may be permitted only for citizens of NATO nations and in connection with contracts requiring access to classified information not higher than NS and not involving Special Category information.

58. The period of validity of a provisional PSC shall be determined and notified by the delivering NSA/DSA, but may never be longer than the necessary timeframe nationally required for the delivery of the full PSC.

INTERNATIONAL TRANSPORTATION OF NATO CLASSIFIED MATERIAL

General

59. The security standards for the international transportation of NATO classified material are set out in the Security of Information directive. This Section describes the additional procedures that apply to the international transportation of material classified NC or NS.

60. The consignor and the consignee of a consignment of NATO classified material to be transported internationally shall jointly organise and submit written transportation arrangements to their respective NSAs/DSAs for approval. The consignor and consignee shall mutually acknowledge and comply with all of the NSAs/DSAs requirements.

61. Where a courier is used, the responsible NSAs/DSAs will issue to the security offices of the consignor and the consignee all official documentation which must be in the possession of the courier.

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

Customs

63. 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 to the authorisation documents carried by the security guard or courier. Consignments should not be opened unless there is a cogent reason for so doing. If a consignment is opened, this should be done out of sight of others. It shall be repacked, 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.

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

Shipping Documents

65. All documents which accompany (but are not packed with) the material to be transmitted, including manifests, TIR carnets, bills of lading, receipts, etc. provide the consignor with a record of all consignments, covering the final destination, time and date of arrival, condition of the shipment (breakage, damage, etc.), and the name of the person and his position in the company or NATO civil and military body who receives the consignment. These documents, prepared by the consignor, will indicate that they accompany a consignment of NATO classified material. Classified information shall not appear in these documents. The consignee shall acknowledge receipt of the consignment by signature on the shipping documents.

Packaging

66. Packaging of consignments shall be in compliance with the Security of Information directive. The security officer of the consignor facility is responsible for supervision of packaging. Special cases requiring additional guidance should be discussed with the facility's NSA/DSA. In no circumstances shall the packaging reveal the fact that the material is classified.

Security Principles Applicable to all Forms of Transportation

67. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

(a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

(b) the degree of protection accorded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC shall be obtained, where appropriate, for companies providing transportation. In such cases, personnel handling the consignment shall be cleared in compliance with the provisions of this Enclosure;

(d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit; and

(e) care shall be exercised to arrange routes only through NATO nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/DSA of the consignor's nation and the consignee and in accordance with the supporting security of information directive.

68. 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.

Hand Carriage of NATO Classified Material

General

69. When transmission through the channels specified in the Security of Information directive 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 carriage may be permitted, provided, the following provisions are complied with :

(a) the courier shall be a permanent employee of the dispatching or receiving facility. Shipping agents or commercial courier services shall not be used;

(b) in exceptional circumstances, a NSA/DSA may, with the previous agreement of the NSA/DSA of the receiving facility, consider issuing a courier certificate to a national of another NATO nation with the appropriate PSC who is assigned to the facility, and to whose NATO nation the release of the classified material relating to the programme/contract has been authorised; and

(c) the procedure shall be used on a case-by-case basis, subject to the prior approval by the NSAs/DSAs of the nations concerned or by the NPA/NPO in the case of NR material.

Security Arrangements

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

71. The bearer shall be briefed by the security officer of the consignor before his departure on all the security measures to be implemented; he will sign the declaration at Appendix 7.

72. The courier shall be responsible for the safe custody of the NATO classified material until such time that they have been handed over to the consignee's security officer. In the event of a breach of security, the consignor's NSA/DSA may request the authorities in the country in which the breach occurred to carry out an investigation, report their findings and take legal action as appropriate.

Procedure

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

(a) the courier shall carry a courier certificate that is recognised by all NATO nations, authorising him/her to carry the package as identified (see Appendix 8) stamped and signed by the consignor’s NSA/DSA and by the consignor's security officer;

(b) a copy of the "Notes for the Courier" (Attachment 1 to Appendix 8) shall be attached to the certificate; and

(c) the courier certificate shall be returned to the issuing NSA/DSA through the consignor's security officer immediately after completion of the journey. Any circumstances that occurred during the trip which raise security concerns shall be reported by the courier on the certificate.

74. The consignor's security officer is responsible for instructing the bearer in all of his duties and of the provisions of the "Notes for the Courier" (Attachment 1 to Appendix 8) and a security acknowledgement (Appendix 7) has to be signed.

75. If Customs authorities request to examine the consignment, and inspection is unavoidable, the procedures at paragraph 63 above, 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.

76. Under no circumstances shall the classified consignment be handed over to Customs or other public officials for their custody.

Transportation of Classified Material by Commercial Carriers as Freight

77. When, in the opinion of the NSAs/DSAs concerned, a consignment is of such size and weight, or other circumstances render government services impractical or unavailable for use, commercial carriers may be used. The following procedures shall be met.

78. Prior to any international transmission by commercial carrier, the NSAs/DSAs of the consignor and of the consignee must agree on a transportation plan as described in Appendix 9.

79. The NSA/DSA of the consignor is responsible and accountable for any NATO classified consignment transferred under these procedures until such time as the consignment has been officially handed over to the receiving NSA/DSA or to that NSAs/DSAs designated government representative. The official transfer may take place in either the dispatching or receiving nation, as mutually agreed by the NSAs/DSAs. The security officers of the consignor and the consignee may be appointed by the NSAs/DSAs as the Designated Government Representative, if permitted by national security regulations.

80. When a transportation plan is developed that will involve more than one international shipment of classified consignment, a procedure is required for identifying each shipment and for providing details of each shipment to the recipient, to transportation personnel and personnel who will be involved in ensuring the security of the shipment. A Notice of Classified Consignment (Attachment 1 to Appendix 9) shall be used for this purpose.

Commercial Carrier Criteria

81. A commercial carrier shall meet the following minimum criteria for handling international shipments :

(a) hold an appropriate FSC, which should, if appropriate, include an approved document safeguarding capability, issued by the NSA/DSA of the nation of origin if deemed necessary and according to national security regulations;

(b) be authorised by the laws or regulations of the nation of origin to provide international transportation services; and

(c) is obligated to comply with safety, security and emergency procedures which must be observed.

Transportation by Road

82. The following minimum standards shall be applied when consignments of NATO classified material are transmitted by road transportation :

(a) material classified NC and NS 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 or sheeted so as to protect the classified aspects and prevent unauthorised persons from gaining access;

(b) when the consignment is classified NS or NC, either the driver or the co-driver and the security guard shall be cleared to the classification level of the consignment. Where no separate security guard is provided, either the driver or the co-driver shall be cleared;

(c) in cases where stops must be made, arrangements shall be made in advance to use storage provided by government establishments or facilities having the necessary cleared personnel and capabilities to handle the consignment. In the event such arrangements cannot be made or an emergency situation arises due to accident or breakdown of the truck, the security guard is responsible for keeping the consignment under constant protection during the period;

(d) telephonic or telex checks along the road between the person responsible for the consignment and the security guard concerned shall be pre-arranged; and

(e) when electronic monitoring of the truck is used in accordance with national regulations, the requirements of paragraph (d) above, may not be necessary.

Transportation by Rail

83. Transportation by rail may be used for consignments of NC and NS material only in the following conditions :

(a) passenger accommodations shall be made available for security guard personnel; and

(b) during stops, the security guard shall remain with the consignment.

84. 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 by Sea

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

(a) 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 security of information directive, "International Transmission") shall not be used. The masters of all ships used to carry consignments of NATO material classified NC or NS shall be nationals of NATO nations and shall hold an appropriate PSC, or a cleared guard or escort shall accompany the consignment;

(b) material shall be stowed in locked stowage space approved by the NSA/DSA of the consignor; when this is not available, blocked-off stowage may be approved. 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, in the opinion of the designated security officer, access to the material is physically impracticable. Where it is impracticable to carry a consignment in the hold, it may be carried as deck cargo, provided it is in a secure container and packaged so it is not evident that it contains classified material. In all cases, the consignment must be under security control;

(c) stops at maritime 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 plan drawn up by the consignor and the consignee. Unless the ship is in emergencies, it shall not enter the territorial waters of any of these countries;

(d) stops at any non-NATO port shall not be permitted unless 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. Where this is unavoidable, sufficient security guards must be provided to keep the consignment under adequate supervision, unless it can be stored at a secure facility that is cleared by the consignee’s NSA/DSA.

86. Where the consignment is of material classified NR or NC, the security guard's duties may be carried out by the ship's master or specially designated crew members.

Transportation by Aircraft

87. 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 practicable, a cleared commercial air carrier may be used, provided it is registered in a NATO nation. Scandinavian Airlines System aircraft also may be used, provided the captain is from a NATO nation.

88. 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 returned, 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 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 practicable, the consignment shall be kept at the airport and a sufficient number of security guards must be provided to keep the consignment under adequate supervision;

(c) 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, the courier or other appropriately cleared personnel must be available to ensure the protection of the classified material;

(d) 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. Where such a stop is in a NATO nation, the guard shall be entitled to call upon, and expect to receive, the assistance of the NSA/DSA of that nation;

(e) 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 plan drawn up by the security officer of the consignor;

(f) direct flights shall be used wherever possible; and

(g) except in an emergency, stops at airfields in non-NATO nations shall not be permitted.

89. 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 NSAs/DSAs;

(b) the NSA/DSA of the consignor shall provide to the NSA/DSA of the consignee a written assurance that the commercial air carrier will comply with the security measures;

(c) companies that provide cargo handling services (such as freight forwarders) shall have a current FSC and approved safeguarding capability and must agree in writing to comply with the security requirements established by the responsible NSAs/DSAs;

(d) the cargo handling company and commercial air carrier shall be capable of providing the level of protection specified by the NSAs/DSAs;

(e) 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;

(f) overflights over countries presenting special security risks shall not be permitted without the written permission of the NSAs/DSAs;

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

(h) the NSA/DSA of the consignor shall be responsible for the protection of any classified consignment transmitted under these procedures until such time as custody of the consignment is transferred to a Designated Government Representative appointed by the NSA/DSA of the consignee, as identified in an approved transportation plan; and

(i) sufficient physical protection shall be provided to the consignment as agreed by the NSAs/DSAs.

Security Guards and Escorts

90. 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. However, they must be nationals of NATO nations and be security cleared.

91. In addition to the security guards, security escorts may be provided if the NSAs/DSAs concerned consider this desirable. These escorts need not be security cleared.

92. 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.

93. 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" (Attachment 1 to Appendix 8). and be required to sign a receipt for it (Appendix 7).

94. 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 10).

95. Both the authorisation documents and "Notes for the Courier" 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 NSAs/DSAs concerned.

Transportation of Explosives, Propellants or Other Dangerous Substances

96. 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.

INTERNATIONAL VISIT PROCEDURES

Requirements and Procedures for Visits

97. The procedures for NATO international visits are based on the use of the "Request for Visit" (RFV), as shown at Appendix 11 and its Attachments.

98. The procedures apply to the following types of visits :

(a) one-time visits - single visits for a specified purpose, normally lasting less than 30 days and which are not anticipated to be repeated within the year;

(b) recurring visits - intermittent, recurring visits to specified organisations, commands or facilities over a specified period of time, normally not exceeding one year, and for a specified purpose; and

(c) emergency visits - one-time visits that must take place as a matter of urgency and importance, such that the standard visit request procedures cannot be used.

99. Intended one-time and recurring visits shall be initiated by means of a "Request for Visit" sent by the visiting establishment or facility to the host facility or establishment through the NSAs/DSAs concerned. The request shall follow the procedures and contain the basic information indicated on the RFV at Appendix 11 and its Attachments.

100. Changes to pending RFVs are permitted, using the same RFV format and procedures, with reference to the original request, but are limited to :

(a) one-time visits - date of visit; additions or deletions of names; and

(b) recurring visits - additions or deletions of names.

101. The lead times allowed are set out at Appendix 12. Deletions (namely those due to withdrawal of security clearance) must be forwarded by the fastest means available to the NSA/DSA of the host NATO member nation. Amendments that request earlier dates than originally specified shall not be accepted. Emergency visits shall not be amended.

102. Before permitting the visitor(s) to have access to NATO information, the host facility shall verify that :

(a) it has received the authorisation of its parent NSA/DSA;

(b) the visitor provides proper identification; and

(c) the level of security clearance shown in the RFV is appropriate for the purpose of the visit.

103. Requests for recurring visits should normally be used for contracts for all NATO programmes/projects. They shall be valid for one year from the start date requested in the RFV. Recurring visits shall be re-submitted for re-issuance annually. Superseded lists of participating individuals and facilities shall be retained in accordance with national requirements.

104. If the requesting NSA/DSA does not receive any adverse notice at least three (3) working days in advance of the starting date of a one-time visit from the NSA/DSA of the host NATO member nation, then the visit may take place. This does not override the provisions of paragraph 102 above.

105. Where permitted by National security rules and regulations, NR and NU visits may be arranged directly between the Security Officer for the visitor and the Security Officer of the facility to be visited.

Emergency Visit Arrangements

106. Unforeseen circumstances may occur which do not permit the use of standard procedures for a one-time or recurring visit. Such unplanned or emergency visits shall be arranged only in exceptional circumstances. If visits are properly planned at the beginning of

NATO activities, the one-time and recurring visits authorisations should satisfy the majority of requirements for visits.

107. Emergency visit procedures shall not be used in lieu of standard visit request procedures. Therefore, each NATO member nation will establish guidelines to ensure compliance with these procedures. If it becomes apparent that the procedures are being abused by personnel of another NATO nation, the NSA/DSA of that NATO nation shall be notified and shall take action against the offender.

108. To qualify as an emergency visit, the following conditions shall be met :

(a) the proposed visit is related to an official NATO request for proposal/request for tender offer, or

(b) the visit is to be made in response to the invitation of the host government official or the NATO Programme/Project Management Agency/Office; or

(c) a NATO project/programme will be adversely affected or a contract opportunity will be lost if the visit request is not approved.

109. Emergency visit requests shall be critically reviewed, fully justified and documented by the Security Officer of the requesting government departments, establishments, contractors or sub-contractors.

110. When the Security Officer is satisfied that the conditions cited in paragraphs 107 or 108 have been met, he shall contact a knowledgeable person at the government department or establishment or contractor or sub-contractor facility to be visited, directly by telephone or facsimile, to obtain tentative verbal agreement for the proposed visit. This normally should be accomplished three working days in advance. If tentative verbal agreement is provided to proceed with a visit request, the government department, establishment, contractor or sub-contractor to be visited (host facility) shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the facility that wants to make the visit (requesting facility) and explain the reason for the emergency.

111. Following receipt of tentative verbal agreement from the host facility, the Security Officer of the requesting facility shall then send a message in the RFV format as follows :

(a) the message must be sent by priority precedence, within 24 hours of the verbal agreement for the requested emergency visit, to the NSA/DSA of the NATO member nation to be visited, through the NSA/DSA of the originating NATO member nation, and to the Security Officer of the host facility. Any of those officials may deny the visit;

(b) the subject of the message shall be :

EMERGENCY VISIT – (Name of program, project or contract or request for proposal or tender offer.)

The message must contain all of the information included in the RFV format. The name and telephone and facsimile numbers of the person who provided tentative verbal agreement will be placed in the Remarks section of the RFV;

(c) each NSA/DSA involved shall, upon receipt of the request, check its records to ensure that the information provided meets the requirements set forth in this section. If the requesting NSA/DSA does not receive a denial notice at least one working day in advance of the starting date of the emergency visit from the NSA/DSA of the host NATO member nation, then the visit may take place.

Special Arrangements for Specific Projects / Programmes

112. The NATO international visit procedures will normally be those defined above and in Appendix 11. However, in case of a specific project / programme, 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 authorised 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 section.

113. Accordingly, where permitted by National security rules and regulations, visits involving access to information classified up to NATO SECRET may be arranged directly between the Security Officer of the visitor and the Security Officer of the facility to be visited, acting on behalf of the NSAs/DSAs involved provided that such an arrangement is approved by the relevant national authorities.

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

114. When an individual who has been cleared for access to NATO classified information is to be loaned within a NATO programme/project or other NATO classified contract from one contractor facility to another 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 or a Certificate of Security Clearance, as appropriate. The RFV, or Certificate of Security Clearance shall be provided by the parent facility to the facility the individual is to be loaned via its respective NSA/DSA.

NATO CLASSIFIED CONTRACTS INVOLVING NON-NATO NATIONS

115. This section of the directive provides specific clarifications in respect to the requirements for NATO classified contracting involving non-NATO nations. All other aspects of this directive are applicable irrespective of whether the contracting is with a NATO nation or a non-NATO nation.

116. This section applies to the following scenarios involving NATO classified contracts / sub-contracts :

(a) a NATO body negotiating with, or awarding to, industry which is located and incorporated in a non-NATO nation;

(b) a contractor in a NATO nation negotiating with, or awarding to, industry which is located and incorporated in a non-NATO nation;

(c) a contractor in a non-NATO nation negotiating with, or awarding to, industry which is located and incorporated in a NATO nation;

(d) a contractor in a non-NATO nation negotiating with, or awarding to, industry which is located and incorporated in the same or another non-NATO nation;

(e) a contractor in a non-NATO nation negotiating with, or awarding to, a NATO body.

117. NATO contracts / sub-contracts classified NC and above shall only be negotiated with, or awarded to, industry which is located and incorporated in :

(a) a NATO nation; or

(b) in a non-NATO nation that has signed a Security Agreement with NATO; or

(c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 119 below).

118. NATO contracts / sub-contracts classified NR shall only be negotiated with, or awarded to, industry which is located and incorporated in :

(a) a NATO nation; or

(b) in a non-NATO nation that has signed a Security Agreement with NATO; or

(c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 119 below); or

(d) in a non-NATO nation that has provided a Security Assurance to NATO (either directly or through a NATO nation or the NATO Programme / Project Agency / Office (NPA/NPO)).

119. In the case of a bilateral Security Agreement / Arrangement (see paragraphs 117(c) and 118(c) above), in accordance with the requirements of Enclosure "E" to this C-M, the NATO nation shall provide a written assurance to NATO based upon a separate exchange of letters of understanding shall be agreed between the NATO nation and the non-NATO nation requiring the latter to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement. This understanding shall identify the NATO security classifications as equivalents to the national classifications on which the bilateral Security Agreement /

Arrangement is based; and identify that NATO classified information shall not be transferred to a third party without the prior approval of the originator of the information.

120. For non-NATO nations, an appropriate security authority shall be identified that fulfils the equivalent functions of the NSA/DSA in a NATO nation. It shall be certified that a non-NATO nation has implemented a degree of protection, no less stringent than that defined in NATO Security Policy, for any NATO classified information released. This includes, in particular, verification that the non-NATO nation has the FSC, PSC and personnel briefing processes in place that meet the requirements of NATO Security Policy.

121. The release to non-NATO nations of NATO classified information in contracting shall be subject to the requirements of Enclosure "E" of NATO Security Policy and supporting directives, specifically the Directive on the Security of Information.

Negotiation and Letting of NATO Classified Contracts

Prime Contracts

122. Before negotiating a NATO classified prime contract classified NC and above, the NATO Programme/Project Agency/Office shall contact the appropriate security authority of the non-NATO nation in which the potential prime contractor is registered or incorporated to ensure that the potential contractor holds a FSC at least equal to the classification level of the information that will be required during the negotiation of the contract. If the potential contractor has no FSC or it is not at the required level, the NPA/NPO shall forward a request for the initiation/upgrading of a FSC to the appropriate security authority of the non-NATO nation, using the “Facility Security Clearance Information Sheet” (FIS) at Appendix III. The NPA/NPO shall include the highest NATO security classification of the information required, as well as the nature of the material or technology to which access is required.

Sub-Contracts

123. After a prime contract has been let, a prime contractor in a non-NATO nation may negotiate sub-contracts with other contractors, i.e., sub-contractors. When the prime contractor or prospective sub-contractor is located and incorporated in a non-NATO nation, permission shall be obtained from the programme/project management office/agency prior to negotiation or award of a sub-contract to a contractor located or incorporated in the same or another non-NATO nation or in a NATO nation.

124. Before negotiating a NATO classified sub-contract, the contractor shall contact its parent security authority to ensure that the potential sub-contractor holds an appropriate FSC. Where the potential sub-contractor is under the jurisdiction of another nation (NATO or non-NATO), the parent security authority of the contractor shall contact the security authority of the nation of the sub-contractor to confirm the presence of an appropriate FSC, or submit a request to initiate / upgrade the required FSC. It shall be the responsibility of the parent security authority of the sub-contractor to ensure that all the appropriate security requirements are complied with.

Letting of Contracts

125. Upon letting the prime contract, the NPA/NPO shall notify the appropriate security authority of the non-NATO nation of the prime contractor that a contract has been let and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to both the appropriate security authority of the non-NATO nation and the prime contractor.

126. Upon letting a sub-contract, the contractor that lets the sub-contract shall notify his parent security authority, the prime contractor, and the NPA/NPO. The sub-contractor's security authority shall ensure that the sub-contractor makes the necessary arrangements for the protection of all NATO classified information released to the sub-contractor. The contractor shall ensure that the sub-contractor is contractually obliged to comply with the provisions of the applicable PSI or SAL.

127. When the contractor or potential sub-contractor is located and incorporated in a non-NATO nation or they are located and incorporated in different non-NATO nations, the security authority of the contractor that is letting the contract shall pass the information regarding the PSI or SAL to the security authority of the potential sub-contractor, which shall be responsible for enforcing the actions related to the PSI or SAL.

128. Prior to a classified prime contract or sub-contract being let, in light of the requirements of the PSI or the SAL respectively attached to the contract, the security authority that is responsible for the contractor or sub-contractor facility shall :

(a) provide to the NPA/NPO or the contractor that is to let the contract, as applicable, verification that the requisite FSC has been provided, using a FIS format;

(b) ensure that the requisite PSCs are issued for the facility's personnel who will require access to the classified aspects of the NATO contract; and

(c) ensure that the personnel mentioned in sub-paragraph (b) above are briefed on NATO security regulations.

129. The contract shall not enter into force until all of the above measures have been completed.

130. 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 5 and be available to all NSAs/DSAs and NATO civil and military bodies upon request. The list shall include the prime contractors, sub-contractors and project offices of non-NATO nations that hold classified contracts connected with the NATO project/programme.

131. 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 NATO classified information.

Industrial Security Clearances for NATO Contracts

Facility Security Clearances (FSC)

132. The appropriate security authority of the non-NATO nation is responsible for furnishing a Facility Security Clearance Certificate (FSCC) (see Appendix 6). Prior to issuing a FSC an assessment shall be made :

(a) of the integrity and probity of the company which is to be entrusted with NATO classified material;

(b) of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other individuals who may, by virtue of their association, position or employment, be required to have access to NATO classified information or supervise a NATO classified contract, 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. In the case of foreign ownership, permission to proceed with contracting shall be sought from the NPA/NPO, who shall be responsible for seeking the appropriate political and security approval; and

(d) of the security arrangements provided for the protection of NATO classified information to ensure that the degree of protection is no less stringent than that specified in NATO Security Policy.

133. The following minimum criteria shall be applied by the appropriate security authority of the non-NATO nation in issuing a FSC :

(a) that the company must establish a security system at the facility which covers all appropriate security requirements for the protection of NATO material and classified information in a manner no less stringent than that specified in NATO Security Policy;

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

(c) that the appropriate security authority 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 NATO classified information; and

(d) that the company responsible for the facility shall appoint a Security Officer responsible for security who is in a position to report directly to an appointed member of the Managing Board of the company.

Personnel Security Clearances for Contractors

134. If a PSC is required for a contractor's employee whose citizenship is that of a NATO nation, or a non-NATO nation with whom NATO has a Security Agreement, the appropriate security authority of the NATO nation or non-NATO nation in which the contractor is located and incorporated shall obtain the appropriate Personnel Security Clearance Certificate from the employee's country of citizenship.

135. If the security authority of the non-NATO nation in which the contractor is located and incorporated learns adverse information about an individual who is a national of a NATO nation or of a non-NATO nation, it shall immediately inform the appropriate security authority of the individual's country of citizenship in order to determine whether he shall continue to hold a PSC. If the NSA/DSA of a NATO nation in which the contractor is located and incorporated learns adverse information about an individual from a non-NATO nation, it shall advise the security authority of the non-NATO nation of the contractor.

Personnel on Loan Within a NATO Project / Programme

136. When an individual who has been cleared for access to NATO classified information is to be loaned from one facility to another in the same NATO programme/project, but in a non-NATO nation, the individual's parent facility shall request its NSA/DSA to provide the appropriate PSC for the individual to the appropriate security authority of the non-NATO nation of the facility to which he/she is to be loaned. The individual on loan shall be assigned using the international visit request procedures set out in the industrial security directive, and in accordance with National security rules and regulations.

137. Where an individual from a non-NATO nation is to be loaned to a facility in a NATO nation, the individual's parent facility shall request its security authority to provide the appropriate PSC to the NSA/DSA of the facility to which he is to be loaned.

LIST OF AUTHORITIES

138. The NOS will maintain a list of authorities, based on periodic updates by NSAs/DSAs and, where appropriate, NATO civil and military bodies. The list, to be published as a separate AC/35 Notice, will include the following :

- authorities for granting FSCs.
- authorities for granting PSCs.
- authorities for international transport of classified material.
- authorities for the control of international visits.
- NATO agencies programmes / projects, and participating nations.

APPENDICES

139. The following Appendices to this directive address the specific procedures, arrangements, and sample documents :

(a) APPENDIX 1 - General Responsibilities;

(b) APPENDIX 2 - Security Policy and Liaison Diagram;

(c) APPENDIX 3 - Facility Security Clearance Information Sheet (FIS);

(d) APPENDIX 4 - Example of a Security Aspects Letter (SAL);

(e) APPENDIX 5 - Facilities / Organisations List;

(f) APPENDIX 6 - Facility Security Clearance Certificate (FSCC);

(g) APPENDIX 7 - Security Acknowledgement (in case of Hand Carriage);

(h) APPENDIX 8 - Courier certificate;

(i) APPENDIX 9 - International Transportation Plan;

(j) APPENDIX 10 - Authorisation for Security Guards;

(k) APPENDIX 11 - Instruction for the Use and Completion of a Request for Visit (RFV); and

(l) APPENDIX 12 - International Visits Processing Times.

GENERAL RESPONSIBILITIES

MEMBER NATIONS

1. Each member nation shall :

   (a) designate one or more authorities (DSA) subordinate to the NSA where applicable. The DSA is responsible for communicating national security policy to industry and for providing direction and assistance in its implementation; in some countries, the function of a DSA may be carried out by the NSA; theNSAs/DSAs are published as AC/35 Notices;

   (b) 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;

   (c) 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 member nation shall :

      (i) ensure that such contractor(s), prospective contractor(s), or sub-contractor(s) and their facility(ies) have the capability to protect information classified NC or above adequately;

      (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;

   (d) 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;

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

(f) provide, upon request to an NSA/DSA of a member nation, or to a NATO civil or military body, an FSC to enable a facility falling within its security cognisance to negotiate or fulfil a NATO classified contract or sub-contract;

(g) provide, upon request, to a NSA/DSA of another member 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;

(h) 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 provided or generated pursuant to a NATO contract has been lost or disclosed to unauthorised persons. Each member nation shall comply with the investigative requirements set out in NATO security policy and its supporting directives and promptly inform the other member nations concerned via NOS of the details of any such occurrences; and

(j) 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 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 approved for access and have a need-to-know.

NATO SECURITY COMMITTEE (NSC)

2. The NSC shall :

(a) formulate NATO industrial security policy and supporting directive(s) and make appropriate recommendations to the Council for the security protection of NATO classified information entrusted, or likely to be entrusted, to industry; and

(b) consider matters of industrial security referred to it by the Council, 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 NPLOs and such other NATO industrial projects as may be designated by the Council 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 NPLOs;

(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 NPLOs;

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

(e) with the agreement of the appropriate NSA, make periodic examinations of the security arrangements for the protection of NATO classified information in the DSAs of the member nations responsible for the activities of NPLOs;

(f) with the agreement of the NSAs/DSAs concerned, make periodic examinations of the security arrangements in national facilities engaged in NATO classified industrial contracts administered by a NATO Project Management Agency / Office; and

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

NATO PROJECT MANAGEMENT AGENCIES / OFFICES

4. Each of the NPLOs and other NATO agencies with project management responsibilities as may be designated by the Council will be bound by the general security regulations laid down in NATO security policy and supporting directives, and all amendments thereto, and by such other security regulations approved by the North Atlantic Council (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) 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; and

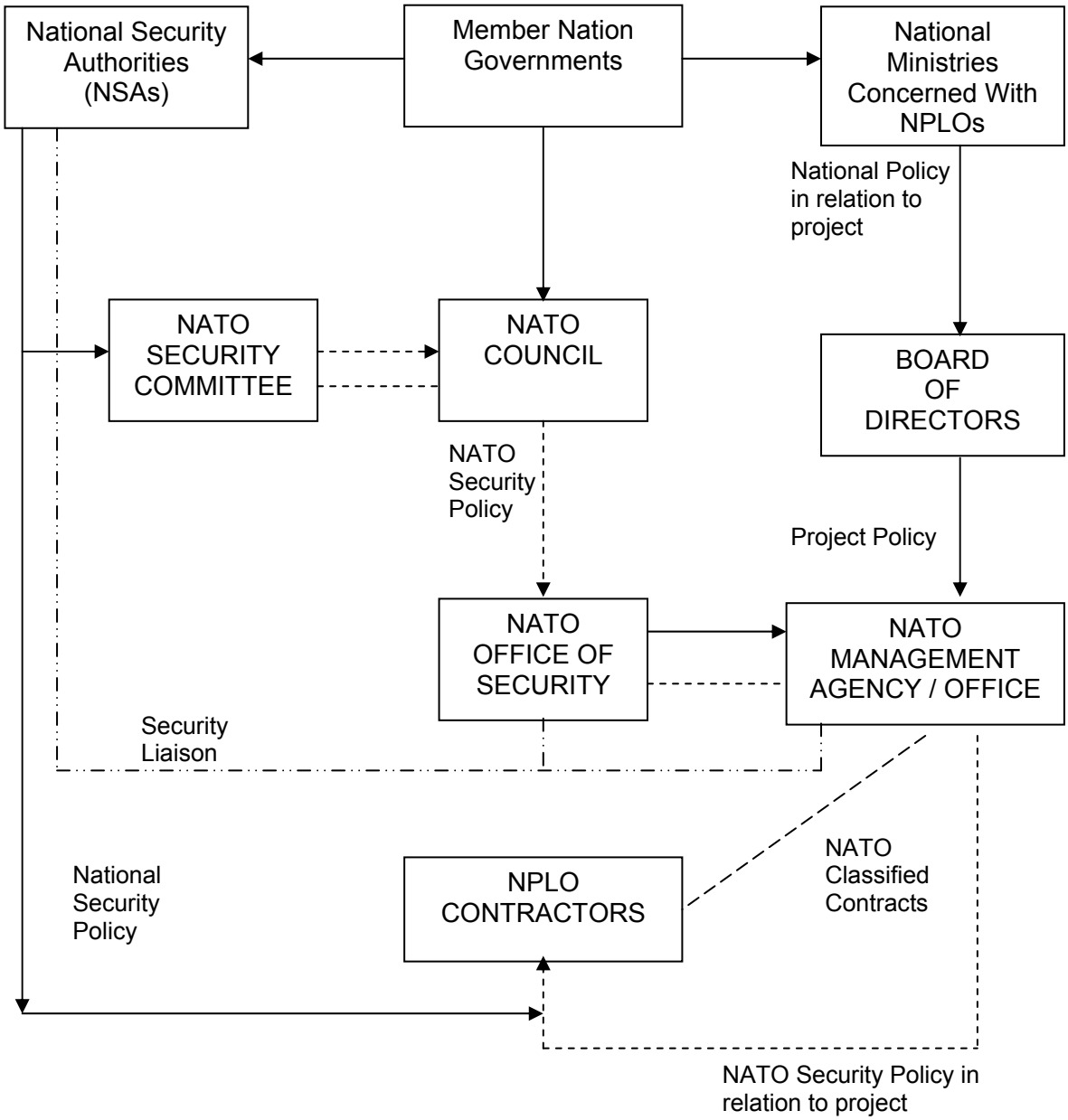
(d) be responsible for preparing Project Security Instructions (PSI) for the programmes they manage for approval by participating NSAs/DSAs.

NATO COMMANDS

5. Each NATO command will take action in accordance with the provisions of NATO security policy and this directive, in respect of those of its personnel to whom the special arrangements for International Visits apply.

APPENDIX 2
ANNEX 1
AC/35-D/2003-REV4

SECURITY POLICY AND LIAISON DIAGRAM IN RESPECT TO NPLO PROJECTS



FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS)

REQUEST

Please [ ] provide a FSC assurance of the facility listed below.
[ ] start initiating a FSC up to and including the level of …… if the facility does not hold a current FSC.
[ ] confirm the FSC up to and including the level of …… as provided on …… (ddmmyy)
[x] provide the current and complete information, if applicable.

1. Full facility name : / corrections / additions :
   /
   …….. / ……..…….
2. Full facility address :
   /
   …….. / …….
3. Mailing address (if different from 2.)
   /
   …….. / …….
4. Zip/postal code / city / country
   /
   …….. / …….
5. Name of the Security Officer (optional)
   /
   …….. / …….
6. This request is made for the following reason(s) :
   (indicate particulars of the precontractual stage, contract, sub-contract, programme / project)

   ……
   ……

Requesting NSA/DSA Name : …… Date : ……

REPLY

1. This is to certify that the above mentioned facility :

   [ ] holds a FSC up to and including the level of : [ ] NS [ ] NC
   [ ] does not hold a FSC
   [ ] does not hold a FSC but, on the above mentioned request, the FSC is in progress. You will be informed when the FSC has been established.
   Expected date : …/… (mmyy). (if known).
2. Safeguarding of classified documents : [ ] yes, level : …… [ ] no.
   Safeguarding of classified material : [ ] yes, level : …… [ ] no.
3. This FSC certification expires on : ……. (ddmmyy). In case of an earlier invalidation or in case of any changes of the information listed above you will be informed.
4. Should any contract be let of classified information be transferred in relation to this certification, please inform us on all relevant data including security classification.

5. Remarks : ……..
   ……...

Issuing NSA/DSA Name : …… Date : ……

APPENDIX 4
ANNEX 1
AC/35-D/2003-REV4

EXAMPLE OF A 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 of the nation in which the work is performed.

2. All classified information and materiel shall be safeguarded in accordance with the requirements established by the NSA of the nation in which the work is performed.

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 his NSA the personal particulars of the persons he wishes to employ on the project with a view to obtaining PSCs at the required level;

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

(d) abstain from copying by any means, without first obtaining …… (programme / project office) permission, any classified materiel (including documents) entrusted to him by …… (programme / project office);

(e) supply his NSA, 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 his NSA;

(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 from …… (programme / project office) or his NSA 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 …… (programme / project office) Security Officer and to his NSA 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, such as reports on holdings of NATO classified information or materiel;

(k) obtain the approval of …… (programme / project office) 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. The level of this clearance must be at least equal to the security category of the materiel, the related information or specifications.

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. 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.

8. 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.

9. The transportation / return of NATO classified documents from private firms to …… (programme / project office) is to be performed on the firm's initiative through their NSAs.

APPENDIX 5
ANNEX 1
AC/35-D/2003-REV4

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 / Telefax / Telex No. 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) 772 633 333 Telex. 56789	YES (NATO SECRET)
2	……..	……	……
3	……..	……	……

The Security Officer :

---------- ----------
(Name) (Signature)

APPENDIX 6
ANNEX 1
AC/35-D/2003-REV4

Facility Security Clearance Certificate (FSCC)

1. This is to certify that on …….. (date), the National Security Authority of ……..…… granted to the ……..…….. (name of facility) located at …….. (address of facility) a NATO …….. (classification) security clearance in accordance with the provisions of the Industrial Security Directive supporting Enclosure ″G″ to the NATO Security Policy, C-M……., valid until ……. (date).

2. The National Security Authority of ……. confirms that the facility referred to in paragraph 1 above :

   (a) * possesses storage capabilities approved for the safeguarding of classified information up to the NATO ……. level;

   (b) * possesses NO storage capabilities approved for the safeguarding of NATO classified information.

…… ……

(Signature) (Stamp or seal of Issuing Authority)

* Delete (a) or (b) as applicable.

APPENDIX 7
ANNEX 1
AC/35-D/2003-REV4

SECURITY ACKNOWLEDGEMENT (in case of Hand Carriage)

[LETTERHEAD]

SECURITY ACKNOWLEDGEMENT

DECLARATION

(name, forename)

of **(name of company)**

(position in company)

The Security Officer of the (**name of company / organisation**) has handed to me the Notes 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 : (**company Security Officer's signature**)

APPENDIX 8
ANNEX 1
AC/35-D/2003-REV4

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 :

  (Indicate the countries having interest. At least the country of origin of the shipment and that of the destination should be indicated. The country(ies) to be transitted 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 transitted, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

APPENDIX 8
ANNEX 1
AC/35-D/2003-REV4

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 Company's Security Officer	Signature of the Designated Security Authority
……. (name)	……. (name)
Company'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 : …….
(company Security Officer's signature)

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

ATTACHMENT 1
APPENDIX 8
ANNEX 1
AC/35-D/2003-REV4

[LETTERHEAD]

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

NOTE FOR THE COURIER (*)

1. You have been appointed to carry / escort a classified consignment. Your "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 Courier 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 company 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 company Security Officer;

* May also be used by security guards.

(h) you and the company 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);

(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 ″Courier 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 company Security Officer and the dispatching company Security Officer, who should be requested to inform the DSAs of their respective governments.

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

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

……

……

……

……

……

……

APPENDIX 9
ANNEX 1
AC/35-D/2003-REV4

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, telefax numbers, and/or telex addresses, 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;

(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;

(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, provisions for the international hand carriage of classified material specified in APPENDIX 8, will 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 despatcher of any deviation in routes or methods prescribed by this plan;

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

(c) clearly state the requirement for recipients to promptly advise the NSA/DSA of the despatcher 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 despatch documents seals, receipts, storage and security containers should be explained. Any unique requirement of the Project / Programme participants should also be stated;

(c) documentation required for the despatch points;

(d) courier authorisation documentation and travel arrangements;

(e) 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;

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

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

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

(i) 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 or sensitive material to the manufacturer or sending country (e.g., warranty, repair, test and evaluation, etc.).

NOTE : 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.

ATTACHMENT 1
APPENDIX 9
ANNEX 1
AC/35-D/2003-REV4

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. Designated Government Representatives : (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 : Shipper 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.

APPENDIX 10
ANNEX 1
AC/35-D/2003-REV4

AUTHORISATION FOR SECURITY GUARDS

Valid until ……

This is to certify that Mr. ……..

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

INSTRUCTION FOR THE USE AND COMPLETION OF A REQUEST FOR VISIT (RFV)

GENERAL INSTRUCTIONS

(a) The Request for Visit (RFV) (Attachment 1) is an important document and must be completed without mis-statement or omission. Failure to provide all requested information will delay the processing of the request.

(b) The RFV should be used for a ″one-time″ visit and/or ″recurring visits″ during a certain period of time not to exceed one year.

(c) This RFV should be hand-written in block letters or typed. Processing of the RFV on a PC is allowed, provided that the original form and content are consistent.

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

These detailed instructions are guidance for the visitors who complete the RFV in the case of one-time visit or by the agency or facility Security Officer in case of recurring visits in the framework of approved programmes or projects. Since this RFV format is designed for manual as well as automated use it is required that a corresponding distinction is made in the completion of some items. When this distinction is applicable, reference is made in the text of the item under ″Remark(s) ″.

In case of a manual application, mark the appropriate box in left and right columns.

1.	ADMINISTRATIVE DATA	Do not fill in (to be completed by requesting NSA)
2.	REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY	Mention full name and postal address, include city, state, postal zone, as applicable.
3.	GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED	Mention full name and full address, include city, state, postal zone, telex or fax number. Mention the name and telephone number of your main point of contact or the person with whom you have made the appointment for the visit. **Remarks** : (1) Mentioning the correct postal zone (zip code) is very important because there can be different facilities of the same company. (2) In case of an automated application, only one agency or facility can be stated. (3) In case of a manual application, Attachment 1 can be used. When two or more agencies or facilities have to be visited in the framework of the same subject, Attachment 2 will be used and item 3 should state : ″SEE ANNEX, NUMBER OF AGENCIES/FAC. :… ″ (state number of agencies / facilities).
4.	DATES OF VISIT	Mention the actual date or period (date-to-date) of the visit by ″day-month-year″. If applicable, place an alternative date or period in brackets.
5.	TYPE OF VISIT	Mark one item of each column as indicated.

6.	SUBJECT TO BE DISCUSSED / JUSTIFICATION	Give a brief description of the subject(s) stating the reason of your visit. Avoid the use of unexplained abbreviations. **Remarks** : (1) In case of a recurring visit, this item 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.
7.	ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	Mention NATO SECRET, NATO CONFIDENTIAL, NATO RESTRICTED or NATO UNCLASSIFIED as applicable.
8.	IS THE VISIT PERTINENT TO :	Mark the appropriate line yes (Y) and, if applicable, specify the full name of the project / programme, FMS-case, etc., using commonly-used abbreviations only.
9.	PARTICULARS OF VISITOR	NAME : Family name, (comma) followed by first name in full and middle initial(s). DOB : Date of birth (day-month-year). POB : Place of birth. SC : Actual security clearance status, e.g., CTS, NS, NC. ID-PP : Enter the number of identification card or passport, as required by host government. NAT : Enter nationality in two-letter code. POSITION : Mention the position the visitor holds in the organisation (e.g., director, product manager, etc.). COMPANY / AGENCY : Mention the name of the government agency or industrial facility that the visitor represents (if different from item 2.). **Remark :** When more than two visitors are involved in the visit, Attachment 3 should be used. In that case, Item No. 9 should state ″SEE ANNEX, NUMBER OF VISITORS : …″ (state the number of visitors).

10.	THE SECURITY OFFICER OF THE REQUESTING AGENCY	This item requires the name, signature and telephone number of the requesting Facility agency / facility Security Officer.
11.	CERTIFICATION OF SECURITY CLEARANCE	**Do not fill in** (to be completed by government certifying authority). Note for the certifying authority : (a) Mention name, address and telephone number (can be pre-printed); (b) This item should be signed and eventually stamped, as applicable; (c) If the certifying authority corresponds with the requesting National Security Authority, enter ″See item 12″. **Remark** : Items 11 and 12 may be filled in by the appropriate official of the NSA of the requesting country.
12.	REQUESTING NATIONAL SECURITY AUTHORITY	**Do not fill in**. Note for the requesting NSA : (a) Mention name, address and telephone number (can be pre-printed); (b) Sign and eventually stamp this item.
13.	REMARKS	(a) This item can be used for certain administrative requirements (e.g., proposed itinerary, request for hotel and/or transportation; (b) This space is also available for the receiving NSA for processing, e.g., ″no security objections″, etc.; (c) ID number amendment.

ATTACHMENT 1
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV4

One-time
Recurring

REQUEST FOR VISIT

Annex(es)
[ ] Yes : …
[ ] No

ADMINISTRATIVE DATA

1. REQUESTOR : DATE : …/…/…
   TO : VISIT ID :

REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY

2. NAME :
   POSTAL ADDRESS :

   TELEX/FAX No : TELEPHONE No. :
   POINT OF CONTACT :

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

3. NAME :
   ADDRESS :

   TELEX/FAX No : TELEPHONE No. :
   POINT OF CONTACT :

4. DATES OF VISIT : …/…/… to …/…/… (…/…/… to …/…/…)

5. TYPE OF VISIT : (SELECT ONE FROM EACH COLUMN)

( ) GOVERNMENT INITIATIVE ( ) INITIATED BY REQUESTING AGENCY OR FACILITY
( ) COMMERCIAL INITIATIVE ( ) BY INVITATION OF THE FACILITY TO BE VISITED

6. SUBJECT TO BE DISCUSSED / JUSTIFICATION

7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED :

8. IS THE VISIT PERTINENT TO : (Y) SPECIFY

A SPECIFIC EQUIPMENT OR WEAPON SYSTEM	( )
FOREIGN MILITARY SALES OR EXPORT LICENCE	( )
A PROGRAMME OR AGREEMENT	( )
A DEFENCE ACQUISITION PROCESS	( )
OTHER	( )

9. PARTICULARS FOR VISITORS

NAME :
DATE OF BIRTH : …/…/… PLACE OF BIRTH :
SECURITY CLEARANCE : NATIONALITY :
POSITION : ID/PP NUMBER :
COMPANY / AGENCY :

NAME :
DATE OF BIRTH : …/…/… PLACE OF BIRTH :
SECURITY CLEARANCE : NATIONALITY :
POSITION : ID/PP NUMBER :
COMPANY / AGENCY :

10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY

NAME : TELEPHONE NO. :

SIGNATURE :

11. CERTIFICATION OF SECURITY CLEARANCE NAME : ADDRESS : STAMP TELEPHONE NO. : SIGNATURE : (optional)
12. REQUESTING NATIONAL SECURITY AUTHORITY NAME : ADDRESS : STAMP TELEPHONE NO. : SIGNATURE : (optional)
13. REMARKS

ATTACHMENT 2
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV4

REQUEST FOR VISIT

Reference : RFV – format, Item 3.

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

1. NAME :
   ADDRESS :

   TELEX/FAX No. : TELEPHONE No. :
   POINT OF CONTACT :

2. NAME :
   ADDRESS :

   TELEX/FAX No. : TELEPHONE No. :
   POINT OF CONTACT :

3. NAME :
   ADDRESS :

   TELEX/FAX No. : TELEPHONE No. :
   POINT OF CONTACT :

4. NAME :
   ADDRESS :

   TELEX/FAX No. : TELEPHONE No. :
   POINT OF CONTACT :

5. NAME :
   ADDRESS :

   TELEX/FAX No. : TELEPHONE No. :
   POINT OF CONTACT :

ATTACHMENT 3
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV4

REQUEST FOR VISIT

Reference : RFV – format, Item 9.

PARTICULARS OF VISITORS

1. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

2. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

3. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

4. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

5. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

6. NAME :
   DATE OF BIRTH : …/…/… PLACE OF BIRTH :
   SECURITY CLEARANCE : NATIONALITY :
   POSITION : ID/PP NUMBER :
   COMPANY / AGENCY :

APPENDIX 12
ANNEX 1
AC/35-D/2003-REV4

INTERNATIONAL VISITS PROCESSING TIMES

Upon receipt by the various NSAs/DSAs and NATO Management Agencies / Offices of a request for an international visit, the processing times are set forth below in column 1; column 2 gives the minimum number of days for any change.

MEMBER NATION		NUMBER OF WORKING DAYS	
		Request	Changes
Albania	ALB	20	10
Belgium	BEL	10	5
Bulgaria	BGR	15	10
Canada	CAN	20	5
Croatia	HRV	20	7
Czech Republic	CZE	20	7
Denmark	DNK	15	7
Estonia	EST	21	5
France	FRA	25	5
Germany	DEU	20	7
Greece	GRC	20	10
Hungary	HUN	20	10
Iceland	ISL	-	-
Italy	ITA	20	7
Latvia	LVA	20	5
Lithuania	LTU	14	-
Luxembourg	LUX	10	5
Netherlands	NLD	10	5
Norway	NOR	10	-
Poland	POL	25	10
Portugal	PRT	15	10
Romania	ROU	25	10
Slovakia	SVK	20	10
Slovenia	SVN	21	7
Spain	ESP	20	7
Turkey	TUR	25	10
United Kingdom	GBR	21	7
United States	USA	21	5

NATO Management Agency / Office		NUMBER OF WORKING DAYS	
		Request	Changes
Central European Pipeline Management Agency	CEPMA	3	-
NATO HAWK Management Office	NHMO	7	-
NATO EF2000 and Tornado Development, Production & Logistics Management Agency	NETMA	3	-
NATO Maintenance & Supply Agency	NAMSA	3	-
NATO Consultation, Command & Control Agency	NC3A	3	-
NATO Airborne Early Warning and Control Programme Management Agency	NAPMA	3	1
NATO ACCS Management Agency	NACMA	-	-
NATO Helicopter D&D Production & Logistics Management Agency	NAHEMA	3	-
NATO Medium Extended Air Defence System D&D, Production & Logistics Management Agency	NAMEADSMA	-	-
NATO BICES Agency	NBA	-	-