SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

DOCUMENT
C-M (55) 15 (FINAL)

0216-97- Jan 99

RECORD OF AMENDMENTS

Strike out corresponding number
as each amendment to inserted

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

Artwork and layout by NATO Graphics Studio
Conception et réalisation réalisées au Studio Graphique de l'OTAN

NOTE BY THE SECRETARY GENERAL

ORIGINAL: ENGLISH/FRENCH
First Issue: 8th March, 1955
Second Issue: 1st October, 1990
Third Issue: 15th October, 1997

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

1. This folder contains a re-issue of C-M(55)15(Final) incorporating the amendments to Enclosures "B", "C" and "D" as approved by Council (C-M(95)79 refers). The amended Enclosure "A" (PO(96)80 refers) will only be incorporated into this document after it has entered into force, that is to say when all member States have signed.

2. A comprehensive index covering Enclosures "A", "B", "C", "D" and "E" and a separate one covering "The Supplement" are also included.

3. Work continues in the NATO Security Committee on the Fundamental Review of NATO Security Policy which introduces a risk management approach to security.

4. This document supersedes all previous versions of C-M(55)15(Final) and its Supplement which should be destroyed.

(Signed) Javier SOLANA

Octobre 97

NATO,
1110 Brussels.

GENERAL TABLE OF CONTENTS

DOCUMENT
C-M (55) 15 (Final)

October 97

DOCUMENT
C-M (55) 15 (Final)

SECURITY AGREEMENT BY THE PARTIES TO THE NORTH ATLANTIC TREATY

1. The parties to the North Atlantic Treaty, having formed an organization for the purpose of uniting their military efforts for their collective defence, and realising that the effective planning for this defence entails the exchange of classified information*(1)* among the parties, agree that they will protect and safeguard the classified information of the others; will make every effort to ensure that they will maintain the security classifications established by any party with respect to information of that party's origin; will safeguard accordingly such information; will not exploit such information for production for other than military purposes; and will not disclose such information to another nation without the consent of the originator. This Agreement applies to information disclosed by any party to another party on and after the date of acceptance of this Agreement by the parties.

2. It is agreed, in respect of classified information communicated by one party to another, that the recipient nation shall use its best endeavours within the framework of its laws and rules to prevent any loss of patent rights in the information. Specifically, it is declared and agreed that:

   (a) any rights of the originator to obtain patent protection in the recipient nation in respect of the information communicated are not, and will not be, prejudiced by virtue of the introduction of the information into such nation;

   (b) each party, when so requested by another and to the extent consistent with its laws and rules, will use its best endeavours:

      (i) to have maintained in secrecy any patent application in the recipient nation in respect of information for so long as may be desired by the party of origin; and

      (ii) to supply, upon request of the originator, reports of the manner in which the information embodied in a patent application has been used or disclosed.

(1) For the definition of "classified information" see footnote to paragraph 1 of the Introduction to Enclosure "C" to C-M(55)15(Final)

THE BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

INTRODUCTION

1. This document lays down the basic principles and minimum standards of security to be applied in an appropriate manner by all members of the North Atlantic Treaty Organization so that each may be assured that a common standard of protection is established in each nation.

2. The principal objectives of protective security are to safeguard :

   (a) classified information(1) from espionage, compromise, or unauthorized disclosure; and

   (b) important installations from sabotage and malicious wilful damage.

3. The foundations of sound national security are:

   (a) a national security organization responsible for:

      (i) the collection and recording of intelligence regarding espionage, sabotage, terrorist and other subversive activities; and

      (ii) information and advice to governments on the nature of the threats to security and the means of protection against them;

   (b) regular collaboration among government departments and agencies to agree:

      (i) what information, assets and resources need to be protected; and

      (ii) common standards of protection.

---

(1) (a) "Classified information" means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

(b) The word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

(c) The word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

4. Care and experience are needed in the selection of information to be protected and the assessment of the degree of protection it requires. It is fundamental that the degree of protection should correspond with the security importance of the information to be protected. The classification system is the instrument for giving effect to this principle; a similar system of classification ought to be followed in the planning of counter-sabotage so that the greatest measure of protection is given to the most important installations and to the most sensitive points within them.

MAJOR PRINCIPLES

5. The security measures adopted in each nation must:

   (a) extend to all persons having access to classified information, information-carrying media, to all premises containing such information and important installations;

   (b) be designed to detect persons whose employment might endanger the security of classified information and important installations and provide for their exclusion or removal;

   (c) prevent any unauthorized person from having access to classified information;

   (d) ensure that classified information is disseminated solely on the basis of the need-to-know principle, which is fundamental to all aspects of security.

ORGANIZATION OF SECURITY

Common Minimum Standards

6. Each nation should ensure that common minimum standards of security are observed in all its government departments and agencies so that classified information can be passed in the confidence that it will be handled with equal care. Such minimum standards should include criteria for the clearance of personnel and procedures for the protection of classified information.

Co-ordination of Information on Espionage, Sabotage, Terrorist and Other Subversive Activities

7. All information and records on espionage, sabotage, terrorist and other subversive activities in each nation should be so centralised that they can readily be applied to any question relating to the appointment and continued employment of persons in government service or to the protection of classified information and of installations.

PERSONNEL SECURITY

Clearance of Personnel

8. All persons, civilian and military, who require access to information classified CONFIDENTIAL or above must be appropriately cleared before such access is authorized. This clearance should be designed to determine whether such individuals are of:

   (a) unquestioned loyalty; and

   (b) such character, habits, associations and discretion as to cast no doubt upon their trustworthiness in the handling of classified information.

Particularly close scrutiny in the clearance procedures should be given to persons:

(c) to be granted access to TOP SECRET information;

(d) occupying positions involving constant access to a considerable volume of information classified SECRET;

(e) who may be vulnerable to pressure from foreign or other sources, e.g. due to former residence or past associations.

In the circumstances outlined in sub-paragraphs (c), (d) and (e) above, the fullest practicable practicable use should be made of the technique of background investigation.

9. When persons are employed in circumstances in which they may have access to classified information (e.g. security guards, messengers, maintenance personnel, etc.) consideration must be given to their first being appropriately security cleared.

Records of Personnel Clearances

10. All establishments handling classified information should maintain a register of the clearances granted to the personnel assigned thereto. Each clearance should be reviewed as the occasion demands to ensure that it conforms with the current standards applicable to the person's employment, and should be re-examined as a matter of priority whenever new information is received which indicates that continued employment on classified work is no longer consistent with the interests of security.

Security Instruction of Personnel

11. All personnel employed in positions where they have access to classified information should be thoroughly instructed, upon employment and at regular intervals, in the need for security and the procedures for accomplishing it. It is a useful procedure to require that all such personnel should certify in writing that they fully understand the security regulations relevant to their employment.

Security Status of Personnel

12. Procedures should be established to ensure that when adverse information becomes known concerning an individual, it is determined whether the individual is employed on classified work, and the authority concerned informed.

Supervision of Staff

13. Supervising officials should have the duty of knowing those of their staff who are engaged on classified work and of recording and reporting any incidents, associations or habits likely to have a bearing on security.

Removal of Personnel

14. Persons who are considered to be security risks or those about whose loyalty or trustworthiness there is reasonable doubt, should be excluded or removed from positions where they might endanger security.

PHYSICAL SECURITY

Need for Protection

15. The degree of physical security measures applied depends in particular on the classification and volume of the information held. Therefore care must be taken to avoid over-classification and classification must be subject to regular review. All government departments should follow uniform practices regarding the classification, including downgrading and declassification, custody, transmission and disposal of information requiring protection.

Inspection

16. Before leaving areas containing classified information unattended, persons having custody of such information must ensure that it is securely stored and that all locking devices are secure. Further independent inspections should be carried out after working hours.

Building Security

17. Buildings which house classified information must be protected against unauthorized access. The nature of the protection, e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security inspections and patrols, alarm systems, intrusion detection systems, watch-dogs, will depend on:

    (a) the classification, volume and location of the information in a particular building;

    (b) the quality of the containers for this information; and

    (c) the character of the building.

Emergency Plans

18. Complete plans should be prepared in advance for the protection of classified information during a local or national emergency.

CLASSIFIED INFORMATION ENTRUSTED TO PERSONS AND ORGANIZATIONS OUTSIDE THE GOVERNMENT

19. The standards for the protection of classified information entrusted to persons and organizations outside the government, e.g. consultants, industry, universities, should be comparable to those laid down for government departments.

COUNTER-SABOTAGE AND SAFEGUARDS AGAINST MALICIOUS WILFUL DAMAGE

20. Physical precautions for the protection of important installations are the best protective security safeguards against sabotage and malicious wilful damage and clearance of personnel alone is not an effective substitute. The national security organisation should collect intelligence regarding sabotage, terrorist and other subversive activities.

Protection of Information on Key Points

21. The distribution of industrial information of military significance, which might be translated into bombing, sabotage or terrorist targets, should be controlled by means of a policy designed to hamper the compilation by potential enemies of a Key Points List.

ENCLOSURE "C"

SECURITY REQUIREMENTS AND PROCEDURES FOR THE PROTECTION OF NATO CLASSIFIED INFORMATION AND MEETINGS

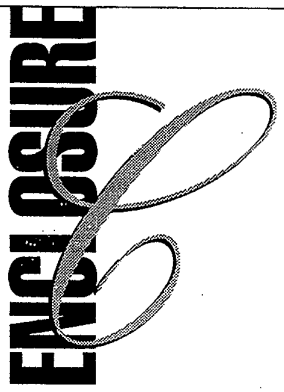
TABLE OF CONTENTS

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - Jan. 99

ANNEXES TO ENCLOSURE "C"

(*) Appendices 3 and 4 will be released to non-NATO recipients as required



SECURITY REQUIREMENTS AND PROCEDURES FOR THE PROTECTION OF NATO CLASSIFIED INFORMATION AND MEETINGS

INTRODUCTION

1. The requirements and procedures in this document are designed to protect NATO classified information(1).

2. The term "NATO classified information" used throughout this document embraces all classified information, military, political and economic, circulated within NATO, whether such information originates in NATO commands and agencies(2) or is received from member nations or from other international organizations.

3. NATO classified information may be circulated, in accordance with the need-to-know principle and without reference to the originator, within NATO. It should be emphasized that the information itself remains the property of the originator and may not be given to any non-NATO nations or to any other international organization except by the originator or as set out in Annexes I and II.

(1) Throughout these instructions :

(a) information means knowledge that can be communicated in any form;

(b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

(c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

(d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

(2) Except where specifically noted otherwise, the terms "NATO command and agency" and "NATO command or agency" used throughout C-M(55)15(Final) include the following: the NATO Military Committee, International Military Staff, Major NATO Commands, NATO military agencies, NATO International Staff, NATO civil agencies.

4. Although NATO UNCLASSIFIED information does not require security protection, it may only be released to non-NATO nations, organizations and individuals when such release would not be against the interests of the North Atlantic Treaty Organization. Any procedures considered necessary for such release will be decided independently by member nations and NATO commands and agencies.

5. The requirements and procedures have been set out in convenient sections so that all persons who are required to handle NATO classified information may be readily aware of their responsibility in fulfilling their particular function. It is not possible, however, in this document to allow for national and local conditions, and member nations and NATO commands and agencies may require to supplement these procedures with more detailed regulations of their own.

SECTION I

AGENCIES RESPONSIBLE FOR THE CONTROL AND CO-ORDINATION OF SECURITY

NATO SECURITY COMMITTEE

6. The NATO Security Committee is established at the Headquarters of the Council and is composed of representatives from each member nation, who should be experienced in security matters in their own nation. The NATO Security Committee will be responsible directly to the Council. A representative of the NATO Military Committee (NAMILCOM) will be present at the meetings of the NATO Security Committee. Representatives of Major NATO Commands and NATO agencies may also be present on matters of interest to them.

7. The Committee is responsible directly to the Council for:

   (a) examining questions concerning NATO security policy;

   (b) considering security matters referred to it by the Council, a member nation, the Secretary General, the NAMILCOM, a Major NATO Commander and the heads of NATO military and civil agencies;

   (c) preparing appropriate recommendations to Council.

NATO OFFICE OF SECURITY (NOS)

8. The NATO Office of Security (NOS) is established within the NATO International Staff. It will be composed of personnel experienced in security matters in both military and civil spheres. The Office will maintain close liaison with the National Security Authority (NSA) of each member nation, and with each NATO command and agency. The Office may also, as required, request member nations and NATO commands and agencies to provide additional security experts to assist it for limited periods of time when full-time additions to the Office would not be justified. The Director, NOS, serves as Chairman to the NATO Security Committee.

9. The NOS is responsible for:

   (a) the examination of any questions affecting NATO security;

   (b) devising methods whereby NATO security might be improved;

   (c) the overall coordination of security for NATO among member nations and NATO commands and agencies;

   (d) ensuring the implementation of NATO security decisions, including the provision of such advice as may be requested by member nations and NATO commands and agencies either in their application of the basic principles and minimum standards of security described in Enclosure "B" or in the implementation of the specific requirements of NATO security systems;

(e) informing, as appropriate, the NATO Security Committee, the Secretary General and the Chairman of the Military Committee of the state of security within NATO, and the progress made in implementing Council decisions regarding security;

(f) carrying out periodic surveys of NATO security systems for the protection of NATO classified information in member nations and NATO commands and agencies;

(g) coordinating with NSAs and NATO commands and agencies, the investigation into cases of lost, compromised or possibly compromised NATO classified information;

(h) devising security measures for the protection of NATO Headquarters and ensuring their correct implementation (paragraph 17 also refers);

(i) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the North Atlantic Council and under its authority, responsibilities for supervising the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding Atomic Information -C-M(64)39 - and the Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding ATOMAL Information - C-M(68)41(5th revise).

NATO MILITARY COMMITTEE, MAJOR NATO COMMANDS AND NATO MILITARY AGENCIES

10. As the highest military authority in NATO, the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is consequently responsible for all security matters within the NATO military structure. In accordance with previously agreed policy and in compliance with its Terms of Reference in paragraph 9 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

11. Major NATO Commanders, and heads of NATO military agencies established under the aegis of the NAMILCOM, are responsible for all security matters within their commands or agencies. This includes responsibility for ensuring that a security organization and security system are set up, that security programmes are devised and executed in accordance with NATO security policy and that the security arrangements are inspected periodically at each command level. In cases of organizations holding COSMIC TOP SECRET or ATOMAL information, security inspections are to be made at least once every 18 months unless, during that period, an inspection has been carried out by the NOS.

12. The NAMILCOM may authorize the establishment (or disestablishment) of one COSMIC central registry. Each major NATO Commander may authorize the establishment (or disestablishment) of one COSMIC central registry within his command. The fact that a COSMIC central registry has been established (or disestablished) will be notified to the NOS.

13. The NAMILCOM may authorize the establishment (or disestablishment) of COSMIC registries in NATO military agencies responsible to it. A Major NATO Commander may authorize the establishment (or disestablishment) of COSMIC registries within his command. The NAMILCOM or a Major NATO Commander may delegate this authority to the Control Officer of a COSMIC central registry. The fact that COSMIC registries have been established (or disestablished) will be notified to the NOS.

14. The NAMILCOM will be responsible for communications security within NATO and will ensure that the provisions of its implementing regulations relating to physical, information and personnel security are compatible with the terms of the regulations contained in this document and in the documents pertaining to the "Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information". Any cases of incompatibility will be referred to the NOS within the terms of paragraph 20 below.

NATO INTERNATIONAL STAFF AND NATO CIVIL AGENCIES

15. The Secretary General may authorize the establishment (or disestablishment) of a COSMIC central registry within the International Staff.

16. The Secretary General may authorize the establishment (or disestablishment) of COSMIC registries within the International Staff and in NATO civil agencies (this authority may be delegated to the Control Officer of a COSMIC central registry). The fact that COSMIC registries have been established (or disestablished) will be notified to the NOS.

17. The NATO International Staff and NATO civil agencies will be responsible to the Council for the maintenance of security within their establishment. They will set up an appropriate security organization in accordance with current NATO security regulations. This organization will include an inspection system applicable at all levels.

MEMBER NATIONS

18. Each member nation will establish an NSA responsible for the security of NATO classified information.

19. This NSA is responsible for:

    (a) the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad;

    (b) authorizing the establishment (or disestablishment) of national COSMIC central registries to a maximum of two. The fact of the establishment (or disestablishment) of a COSMIC central registry will be notified to the NOS;

    (c) authorizing the establishment (or disestablishment) of national COSMIC registries (this authority may be delegated to the Control Officer of a COSMIC central registry). The establishment (or disestablishment) of COSMIC registries will be notified to the NOS;

    (d) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organizations at all levels both military and civil to determine that such arrangements are adequate and in accordance with current NATO security regulations. In the case of organizations holding COSMIC TOP SECRET or ATOMAL information, security inspections will be made at least once every 18 months unless, during that period, they are carried out by the NOS;

    (e) ensuring that a security determination of eligibility has been made in respect of all nationals who are required to have access to NATO information classified CONFIDENTIAL and above, in accordance with the provisions of C-M(55)15(Final);

    (f) ensuring that such national emergency security plans as are necessary to prevent NATO classified information from falling into unauthorized or hostile hands have been prepared.

GENERAL

20. Any NATO security problem necessitating coordination between NSAs of member nations, and NATO commands and agencies, will be referred to the NOS. In cases where such reference is by military authorities, this will be made through command channels. Any unresolved differences arising in the course of such coordination will be submitted by the NOS to the NATO Security Committee for consideration.

21. Any proposals by member nations and NATO commands and agencies involving modification of NATO security procedures will be referred in the first instance to the NOS. Any proposals made by the military authorities will be transmitted through command channels. If the NATO security problems giving rise to such proposals cannot be resolved except by modification of NATO security procedures, the proposals will be referred to the NATO Security Committee, and if necessary, by it to the North Atlantic Council (NAC).

SECTION II

DEFINITIONS OF SECURITY CLASSIFICATIONS AND COSMIC AND NATO MARKINGS

SECURITY CLASSIFICATIONS(1)

TOP SECRET

22. This security classification will be applied only to information and material, the unauthorized disclosure of which would result in exceptionally grave damage to the NATO.

SECRET

23. This security classification will be applied only to information and material, the unauthorized disclosure of which would result in grave damage to NATO.

CONFIDENTIAL

24. This security classification will be applied to information and material, the unauthorized disclosure of which would be damaging to the interests of NATO.

RESTRICTED

25. This security classification will be applied to information and material, the unauthorized disclosure of which would be disadvantageous to the interests of NATO.

MARKINGS

COSMIC

26. This word is a qualifying marking(2) which, when applied to a document, signifies that:

    (a) the document is the property of NATO and the information contained therein remains the property of the originator and may not be passed outside NATO without the consent of the originator. The Council may, however, authorize the transmission of COSMIC documents without reference to the originator, to other international organizations of NATO nations specifically designated by the Council;

    (b) the document is subject to the special handling arrangements outlined in Sections IV and VII of these procedures.

(1) For the term "UNCLASSIFIED", see paragraph 4.

(2) The marking COSMIC should prefix the classification on the document to which it relates.

27. All TOP SECRET documents prepared for circulation within NATO (and all copies of such documents) will carry the marking COSMIC TOP SECRET and be subject to COSMIC control procedures, except when emergency operational needs require that units not served by a COSMIC registry should receive or originate TOP SECRET documents. In such cases, the COSMIC marking (but not the classification) should be omitted, but the documents must be given so far as is practicable equivalent security protection and must be incorporated into the COSMIC system as soon as possible. COSMIC markings and procedures will be used only for TOP SECRET documents.

NATO

28. This word is a qualifying marking(1) which, when applied to a document, signifies that the document is the property of NATO and that the information contained therein remains the property of the originator, and if bearing a security classification, may not be passed outside the Organization except under the conditions laid down in paragraph 3 and that it is subject to the security protection outlined in these procedures.

29. The marking NATO will be applied to all copies prepared for circulation within the North Atlantic Treaty Organization of SECRET, CONFIDENTIAL and RESTRICTED documents. The marking NATO may also be applied to UNCLASSIFIED documents.

(1) The marking NATO should prefix the classification on the document to which it relates.

SECTION III

CLASSIFICATION MANAGEMENT

GENERAL

Definition

30. Classification management is a discipline which seeks to ensure that information(1) is appropriately classified, clearly identified, and remains classified only as long as required.

Responsibility

31. The responsibility for determining whether official information should be marked NATO UNCLASSIFIED or be given a particular level of security classification rests exclusively with the originating member nation or NATO command or agency.

32. Each element, as appropriate, of member nations and NATO commands and agencies will ensure that its personnel are advised regarding the correct application of classification, downgrading and declassification procedures.

CLASSIFICATION

General

33. If it is determined that a security classification is warranted, a conscious decision will be made by the originator in selecting a level of classification consistent with the sensitivity as defined in paragraphs 22 to 25. To assist originators in selecting the appropriate level of classification, each element of member nations and NATO commands and agencies in which NATO classified information is handled should, when considered useful and practicable, prepare and distribute within the element a security classification guide applicable to the topics handled by it.

34. Both overclassification and underclassification should be avoided in the interests of meaningful security as well as efficiency. The classification assigned determines the physical security given to the information in storage and transmission, its circulation, and the security clearance required for access.

35. Information or material will be classified according to its own content and not according to the classification of the file on which it is based or of information to which it refers (e.g. although a document may be classified COSMIC TOP SECRET, a corrigendum to the document will be classified according to its own content or not classified as the case may be).

(1) Note definition list contained in footnote (1) to paragraph 1.

ENCLOSURE "C" to
C-M (55) 15 (Final)

0216-97 - October 97

36. References to classified information will not be classified unless the reference itself contains or reveals classified information. However, owing to the risk of compromising classified information, only the minimum reference details should be given.

37. When collating information, it shall be reviewed for overall classification since it may require a higher classification than its component parts owing to the greater intelligence value which, on occasion, a comprehensive picture may contain.

38. The overall classification of information must be at least as high as that of its most highly classified component. However, a covering document must also conspicuously show the security classification, if any, it warrants when separated from the information it accompanies.

39. In order to ensure that NATO classifications are accurate and precise, clearly identifiable portions of complex documents such as sections, enclosures, annexes and appendices which are of various levels of classification or of no classification, will be marked accordingly. This procedure, which facilitates the further use of individual portions under their own classification, will also be applied, as appropriate, to individual segments such as titles and paragraphs. Particularly when a document derives a high level of classification from a relatively small and easily identified portion of its text, that portion will be identified. The classification which the document will require when that portion is not included shall be stated in a footnote to the overall classification marking on the first page of the document.

40. Cases of apparent overclassification or underclassification should be brought to the attention of the originator by the recipient. If the originator decides to reclassify the document, he will so inform all addressees.

41. Wherever practicable, the originator should, when issuing a document, indicate whether it can be declassified or downgraded to a specified level on a certain date or on the happening of a specific event. The date or event shall normally not exceed ten years unless the information contained in the document needs longer protection.

Special requirements for COSMIC TOP SECRET and NATO SECRET

42. The number of persons who can authorize the original allocation of the COSMIC TOP SECRET classification will be limited to the minimum number absolutely required for efficient administration. A similar policy will be adopted, where practicable, with regard to NATO SECRET information.

43. Where practicable therefore, each member nation and NATO command and agency will designate, in writing, by position for use within that organization, those persons empowered to authorize the original allocation of the COSMIC TOP SECRET classification and, where considered advisable and practicable, the NATO SECRET classification.

DOWNGRADING AND DECLASSIFICATION

44. NATO classified documents may be downgraded or declassified only by, or with the consent of, the originating nation, office, successor organization or higher authority, and only after the interested member nations or NATO commands or agencies have been consulted.

45. Each member nation will establish a system to ensure that TOP SECRET information which it has originated and released to NATO is reviewed every two years to ascertain whether the TOP SECRET classification still applies. Such a review is not necessary in those instances where the originating member nation has predetermined that specific TOP SECRET information will be automatically downgraded after two years and the material has been so marked. Each NATO command and agency will establish a similar system to review COSMIC TOP SECRET information which it has originated.

46. When COSMIC TOP SECRET information is downgraded, the marking NATO must precede the new classification.

47. Each member nation will establish a periodic or other effective system for review of all SECRET information and, where practicable, of all CONFIDENTIAL and RESTRICTED information which it has originated and released to NATO, to ensure that the original security classification still applies.

48. Each NATO command and agency will establish a similar system in respect of NATO SECRET information and, where practicable, of NATO CONFIDENTIAL information which it has originated. This information will be systematically reviewed for timely downgrading, with NATO RESTRICTED as the downward limit. Classified information originated by a NATO command or agency will be systematically reviewed for declassification only when it is at least 30 years old.

49. A contributor to collated information originated by a NATO command or agency who, when consulted in the course of a review for the declassification of 30-year old information, objects to the declassification of specific information, will indicate the earliest date on or around which he will either agree to its declassification or review it again for declassification.

50. The originator of information downgraded or declassified will ensure that recipients of this information are notified promptly of its downgrading or declassification. Those recipients who have given further dissemination to this information will be responsible for ensuring that the further recipients are informed promptly that this information has been downgraded or declassified. In all cases, action to re-mark information will be taken immediately by the recipients of that information for which a downgrading or declassification notice has been received.

SECTION IV

PHYSICAL SECURITY

GENERAL

51. This Section lays down the policy and minimum standards for physical security measures for the protection of NATO classified information. The object of physical security measures is to prevent an unauthorized person from gaining access to NATO classified information.

SECURITY REQUIREMENTS

52. All premises, areas, buildings, offices, rooms, etc. in which NATO classified information and material is stored and/or handled must be protected by appropriate physical security measures.

53. In deciding what degree of physical security protection is necessary, account must be taken of all relevant factors such as:

    (a) the level of classification and category of information;

    (b) the amount and form of the information (hard copy/computer storage media) held;

    (c) the security clearance and need-to-know of the staff; and

    (d) the locally-assessed threat from intelligence services which target the Alliance and/or its member nations, sabotage, terrorist and other subversive and/or criminal activities.

54. The physical security measures achieved must be designed to:

    (a) deny surreptitious or forced entry by an intruder;

    (b) deter, impede and detect actions by disloyal personnel (the spy within); and

    (c) allow for segregation of staff in their access to NATO classified information in accordance with the need-to-know principle.

PHYSICAL SECURITY MEASURES

Security Areas

55. Areas where information classified NATO CONFIDENTIAL or higher is handled and stored must be organized and structured so as to correspond to one of the following:

    (a) **Class I Security Area:** an area where NATO CONFIDENTIAL information or higher of any category is handled and stored in such a way that entry into the area constitutes, for all

practical purposes, access to classified information, e.g. document registries and operations centres. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) a control of entry system which admits only those appropriately cleared and specially authorized to enter the area;

(iii) specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;

(b) **Class II Security Area**: an area where NATO CONFIDENTIAL information or higher of any category is handled and stored in such a way that it can be protected by controls established internally from access by unauthorized persons, e.g. premises containing offices in which information classified NATO CONFIDENTIAL and higher is regularly handled and stored. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) a control of entry system which admits unescorted only those cleared and specially authorized to enter the area. For all other persons, provision is to be made for escorts or equivalent controls, to prevent unauthorized access to NATO classified information and uncontrolled entry to areas subject to technical security inspections.

Those areas which are not occupied by duty personnel on a 24-hour basis will be inspected immediately after normal working hours to ensure that NATO classified information is properly secured.

Administrative Zone

56. Around or leading up to Class I or Class II security areas an Administrative Zone of lesser security may be established. Such a zone requires a visibly defined perimeter within which possibility exists for control of personnel and vehicles. Only NATO RESTRICTED information will be permitted to be handled and stored in Administrative Zones.

Entry and Exit Controls

57. Entry into Class I and Class II security areas will be controlled by a pass or personal recognition system governing the regular staff. A system of control of visitors designed to deny unauthorized access to NATO classified information must also be established. Whenever possible, a pass should not show in clear text or symbols the identity of the issuing organization and/or the place to which its holder is allowed entry. Pass systems may be supported by automated identification, which should be regarded as a supplement to, but not a total replacement for, guards. If the laws and regulations of NATO member nations so allow, random briefcase searches (including packages, bags and anything that could contain classified information and material) should be conducted on entry to and exit from a Class I or Class II security area when prevailing security conditions so require. Such entry and exit searches will be conducted at NATO commands and agencies.

Guards

58. When guards are used to ensure the integrity of security areas and NATO classified information, they must be appropriately cleared, qualified by training, and supervised.

59. Patrols of Class I and Class II security areas should take place outside normal working hours and on non-working days at intervals to be determined by the security authority in the light of the local threat. The patrols shall ensure that NATO classified information is properly protected and that there is no sign of any untoward incident.

60. In order to improve general guard coverage and, for security areas where in the interests of security it has been determined that members of the guard force may not have direct entry, intruder detection by means of devices such as closed circuit television, alarm system or visual inspection ports should be provided. The former devices may also be employed as substitutes for patrols.

61. The response force required is to provide a minimum of two guards to any point of a security disorder on the site without weakening site protection elsewhere. Guard response to alarms or emergency signals shall be tested and must be within a time limit evaluated as capable of preventing an intruder's access to the NATO classified information being protected.

Security Containers and Strong Rooms

62. Containers used for storage of NATO classified information are divided into three classes:

- **Class A**: containers nationally approved for storage of COSMIC TOP SECRET information within a Class I or a Class II security area;
- **Class B**: containers nationally approved for storage of NATO SECRET and NATO CONFIDENTIAL information within a Class I or a Class II security area;
- **Class C**: office furniture suitable for storage of NATO RESTRICTED information only.

63. For strong rooms constructed within a Class I or a Class II security area, and for all Class I security areas where information classified NATO CONFIDENTIAL and higher is stored on open shelves or displayed on charts, maps, etc., the walls, floors and ceilings, door(s) with lock(s) must be certified by the NSA to offer equivalent protection to the class of security container approved for the storage of the NATO classified information involved.

Locks

64. Locks used with security containers and rooms in which NATO classified information is stored shall meet the following standards:

- **Group A**: nationally approved for Class A containers;
- **Group B**: nationally approved for Class B containers;
- **Group C**: suitable for Class C office furniture only.

Control of keys and combinations

65. Keys of security containers should not be taken out of the office building. Combination settings of security containers will be committed to memory by persons needing to know them. Spare keys and a written record of each combination setting for use in an emergency should be held in sealed opaque envelopes by the government department or NATO command or agency concerned. Working and spare security keys should be kept in separate containers. The record of each combination should be kept in a separate envelope. The keys and the envelopes should be given security protection no less stringent than the material to which they give access.

66. Knowledge of combination settings of security containers will be restricted to the smallest possible number of persons. Settings will be changed:

(a) whenever a change of personnel occurs;

(b) whenever a compromise has occurred or is suspected;

(c) at intervals of preferably six months and not exceeding 12 months.

Intrusion Detection Devices

67. When alarm systems, closed circuit television and other electric devices are used in the protection of NATO classified information, electricity must be provided through permanently connected external mains supply with a rechargeable standby battery. Another basic requirement is that a malfunction in or tampering with such systems shall result in an alarm or other definitive warning to the monitoring personnel.

Approved Equipment

68. NSAs will maintain, from their own or from bilateral resources, lists of equipment which they have approved for the direct or indirect protection of NATO classified information under various specified circumstances and conditions. NATO commands and agencies will consult with their host nation before purchasing such equipment.

Physical Protection of Copying and Telefax Machines

69. Copying machines and telefax machines must be physically protected to the extent necessary to ensure that only authorized persons can use them and that all classified products are properly controlled.

PROTECTION AGAINST OVERLOOKING AND EAVESDROPPING

Overlooking

70. When NATO classified information is at risk from overlooking, appropriate measures must be taken to counter this risk under daylight as well as artificial light conditions.

Eavesdropping

71. Offices or areas in which information classified NATO SECRET and above is regularly discussed must be protected against passive and active audio eavesdropping attacks where the risk warrants it. The responsibility for determining the risk is to be coordinated and decided by the appropriate security authority after consultation, as necessary, with technical specialists.

72. Protection against passive eavesdropping attacks - the leakage of classified information via insecure communications or by overhearing directly - may involve seeking technical security advice as described in paragraph 74 below and may involve soundproofing walls, doors, floors and ceilings of designated sensitive areas.

73. Protection against active eavesdropping - the leakage of classified information by wired microphones, radio microphones or other implanted devices - will require a technical and/or physical security inspection of the fabric of the room, its furnishings and fittings and its office equipment, including office machines (mechanical and electric) and communications, etc. These inspections should be undertaken by the appropriate security authority.

Technically Secure Areas

74. Areas to be protected against audio eavesdropping are to be designated as technically secure areas and entry to them must be specially controlled. Rooms must be locked and/or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas must be subject to regular physical and/or technical inspections which will also be undertaken following any unauthorized entry or suspicion of such and entry by external personnel for maintenance work, redecoration, etc. No item of furnishings or equipment should be allowed into these areas until it has been thoroughly examined physically for eavesdropping devices by trained security staff. Telephones should not

normally be installed in areas which are technically secure. However, where their installation is unavoidable, they must be provided with a positive disconnect device if the nature of the telephone system makes this acceptable.

75. Regular technical security inspections may need to be carried out in areas where exceptionally sensitive conversations are held in order to supplement physical searches for quick plant devices and to investigate a telephone system or an electrical or other service which could be used as an attack medium. They may also be necessary to determine the vulnerabilities of sensitive areas, including vulnerabilities arising from the local threat from intelligence services which target the Alliance and/or its member nations.

Examination of electric/electronic office equipment

76. Before being used in those areas where meetings are held or work is being performed which involves information classified NATO SECRET and above, and in circumstances where the risk is assessed as high, communications equipment and electric or electronic office equipment of any kind should be examined by technical or communications security experts to ensure that no intelligible information is inadvertently or illicitly transmitted by such equipment beyond the perimeter of the appropriate security area. A record of the type, serial and inventory numbers should be maintained of equipment and furniture moved into and out of these technically secure areas which should be kept locked by an approved method when not occupied and any keys treated as security keys.

SECTION V

ACCESS TO NATO CLASSIFIED INFORMATION

NEED-TO-KNOW

77. Access to NATO classified information will be confined to those whose duties make such access essential. No person is entitled solely by virtue of rank or appointment or security clearance to have access to NATO classified information. In each and every case the need-to-know will be established.

PERSONNEL SECURITY

78. Each member nation will be responsible for security clearing all its nationals before they are authorized access to NATO information classified TOP SECRET, SECRET or CONFIDENTIAL either in member nations or NATO commands or agencies.

79. Each member nation will, at the request of the NATO command or agency at which a person is to take up duty, provide a completed copy of the NATO security clearance certificate (copy at Annex III) certifying that the person has been security cleared. If any information about one of its nationals serving with a NATO command or agency is received by a member nation which in its opinion would affect the security of NATO, that nation will either communicate such information to the security authority of the NATO command or agency concerned, insofar as national security permits, or withdraw that person's security clearance. If the latter course of action is taken, the security authority of the NATO command or agency will similarly be informed. Where such information has been obtained by a member nation in respect of a national of another member nation or by a NATO command or agency in respect of a member of its staff, the nation concerned should be advised.

80. The security clearance certificate provided under the terms of paragraph 79 for an individual on initial appointment to NATO will be based on an investigative action which was completed:

    (a) in the case of personnel seconded from the armed forces or civil services, not more than five years before the date of the appointment;

    (b) in the case of personnel not seconded from the armed forces or civil services, not more than nine months before the date of the appointment.

    In either case, the date of expiry appearing on the certificate will in no case be more than five years from the date of the last investigative action. After the issue of the initial security clearance certificate and provided the staff member has unbroken service with NATO, the certificate will be reviewed for revalidation at intervals not exceeding five years with effect from the date of the last investigative action on which it was based.

BRIEFING

81. Before having access to COSMIC TOP SECRET information, all persons will be briefed on NATO security procedures and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorized hands either by intent or through negligence. Persons with access to NATO SECRET, NATO CONFIDENTIAL and NATO RESTRICTED information will be made aware of the appropriate NATO security regulations and of the consequences of negligence.

82. It is important that persons who are required to handle NATO classified information are initially made aware, and periodically reminded, of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the press, and the threat presented by the activities of intelligence services which target the Alliance and its member nations. Such persons will be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre giving rise to suspicions of an intelligence background or any unusual circumstances relating to security.

83. All persons normally exposed to frequent contact with representatives of countries whose intelligence services target the Alliance and its member nations must be given a briefing on the techniques known to be employed by various intelligence services.

84. There are no NATO security regulations concerning private travel to any destination by personnel cleared for access to NATO classified information. NSAs will, however, acquaint their nationals serving in NATO commands and agencies with travel regulations that may exist in their parent nation, and to which they may be subject.

ACCESS TO NATO CLASSIFIED INFORMATION

85. Each individual in possession of NATO classified information is responsible for ensuring that persons to whom it is passed are authorized to have access to information of at least that specific classification.

86. The responsibility for authorizing access to NATO classified information, and for the briefing of personnel on NATO security procedures, rests with the responsible officials of the government department or NATO command or agency in which the person is to be employed.

87. Member nations and the Heads of NATO commands and agencies sponsoring delegates to conferences and meetings away from their parent organizations will transmit certification to the appropriate authorities that such delegates are authorized to have access to NATO classified information of the appropriate level. Exceptionally, such certification may be hand-carried by the delegates concerned. A copy of the certificate of security clearance to be used for all visits, except repeated visits or visits to facilities in more than one member country to be made under the terms of Section VI of Enclosure "D", is at Annex IV. Where applicable, a consolidated list of names giving the details required by Annex IV is acceptable.

88. Persons outside regular government or NATO employment on NATO or national business requiring access to NATO classified information do so under the sponsorship of their own government and will be security cleared and briefed as to their responsibility for security.

ACCESS TO COSMIC TOP SECRET INFORMATION

89. Access to COSMIC TOP SECRET information must be specially controlled. Those who are required to have such access will be specifically authorized by the head of the government department or the NATO command or agency concerned or by a designated senior official. Persons who are authorized access will be recorded in the appropriate COSMIC registry or control point.

90. All persons to be authorized access to COSMIC TOP SECRET information will sign a certificate to the effect that they have been briefed on NATO security procedures and that they fully understand their special and continuing responsibility for safeguarding COSMIC TOP SECRET information, and the consequences of unauthorized disclosure of classified information either by intent or through negligence.

91. The names of all persons ceasing to be employed in duties requiring access to COSMIC TOP SECRET information will be removed from the COSMIC list. All persons will be reminded of their special and continuing responsibility for the safeguarding of COSMIC TOP SECRET information and will sign a certificate to the effect that they understand this. Should any such person be re-employed on duties requiring access to COSMIC TOP SECRET information, the procedures in paragraphs 80-83, 89 and 90 above will be completed by the new department in which the person is to be employed.

ACCESS TO NATO CRYPTO INFORMATION

92. Security clearance procedures for establishing a person's eligibility to have access to NATO classified information are equally applicable for eligibility to have access to NATO crypto information. In addition, individuals who in the normal course of their duties are required to have access to NATO high grade keying material or crypto information of a sensitive nature must be specifically authorized by the head of the NATO command or agency, responsible officials of national employing organizations, and/or by NSAs, as appropriate, in accordance with the procedures set forth in NATO crypto security instructions which have been promulgated by the NAMILCOM.

INTERIM ACCESS TO NATO CLASSIFIED INFORMATION IN AN EMERGENCY

93. In wartime or in periods of mounting international tension or in peacetime during on-call/exercise duty when emergency measures require it, member nations and heads of NATO commands and agencies may in exceptional circumstances grant by a written authorization access to NATO classified information to persons who do not possess the requisite security clearance, provided that such authorization is absolutely necessary and there are no reasonable doubts as to the trustworthiness of the person concerned.

94. In the particular case of COSMIC TOP SECRET information, this emergency access will be confined wherever possible to those personnel whose clearances already afford them access to NATO SECRET or NATO CONFIDENTIAL information. In peacetime, emergency access to NATO SECRET and above will be limited to personnel who have been cleared for NATO CONFIDENTIAL and above.

95. Whenever such emergency access is granted, a record of the authorization will be made by the authority concerned who will, as soon as possible, institute the procedures necessary to fulfil the normal clearance requirements.

SECTION VI

COSMIC REGISTRIES AND CONTROL POINTS AND NATO REGISTRIES

GENERAL

96. Registries are responsible for the control of NATO classified information. With regard to accountable NATO classified information, registries should be able at all times to establish the location of this information.

97. COSMIC registries and control points and registries (secretariats) handling NATO SECRET information and below may be co-located and operated by the same registry personnel. COSMIC TOP SECRET information, however, will be physically compartmentalized and administratively separated from NATO SECRET information and below. In NATO member nations, registry personnel handling national classified information may, if properly cleared, also be responsible for COSMIC TOP SECRET and NATO SECRET information and below.

COSMIC REGISTRIES AND CONTROL POINTS

98. The purpose of COSMIC registries and control points is to ensure the correct recording, handling and distribution of COSMIC TOP SECRET information. The head of the COSMIC registry or control point is designated, the "COSMIC Control Officer". Alternate COSMIC control officers should be designated as necessary. An alternate COSMIC control officer may perform some of the duties of the COSMIC control officer on a permanent basis and will assume all authority and responsibility during the latter's absence.

99. Central registries act as the main receiving and despatching authority for the member nation or NATO command or agency within which they have been established. Central registries may also act as registries where appropriate.

100. Registries are responsible for the internal distribution of COSMIC TOP SECRET information and for keeping records of the location of each document held on the registry's charge. When issued on temporary loan to other than a control point, such records will include the individual custody.

101. A COSMIC control point is an administrative means for assisting in the control of COSMIC TOP SECRET information below the registry level. Its primary purpose is to provide facilities for the receipt, routing, and custody of COSMIC TOP SECRET documents received from the registry under which it operates, and when authorized from other COSMIC central registries, registries or control points, and to control such documents when they are on temporary loan to individual users.

102. COSMIC control points may be established in accordance with regulations issued by the appropriate NSA, the Secretary General, the NAMILCOM or Major NATO Commanders. Infrequent and temporary access to COSMIC TOP SECRET information does not necessarily require the establishment of a COSMIC control point, provided procedures ensure that the information remains under the control of the appropriate COSMIC registry or existing control points.

103. In exceptional circumstances, control points may be authorized to exchange COSMIC TOP SECRET documents directly with other registries and control points, provided that the transmission and receipt is recorded in the registries responsible for holding the documents on charge.

104. Control points are responsible for keeping up-to-date records of the individual custody of all COSMIC TOP SECRET documents in their charge.

105. In order to expedite NATO business, and for administrative economy, registries and control points may be authorized by the appropriate authority of the member nation or NATO command or agency to transmit COSMIC TOP SECRET information direct to other registries and control points within the same member nation or NATO command or agency.

106. COSMIC TOP SECRET documents may only be issued outside a registry or control point on temporary loan to an individual, who is responsible for their custody. The individual custody of COSMIC TOP SECRET documents will not be transferred except through the responsible registry or control point and such documents will be returned as early as possible.

107. COSMIC TOP SECRET documents consigned to an addressee in another member nation or NATO command or agency may be transmitted direct from one central registry, registry or control point to another when authorized by the appropriate authority of the member nation or NATO command or agency.

COSMIC CENTRAL REGISTRIES

108. The control officer of a COSMIC central registry is responsible for:

(a) transmission of COSMIC TOP SECRET information in accordance with the regulations contained in Section VII;

(b) maintaining an up-to-date list of all COSMIC registries within the member nation or NATO command or agency and of those control points established directly under the central registry together with names and signatures of the appointed control officers and their authorized alternates;

(c) obtaining receipts from registries and control points for all COSMIC TOP SECRET documents distributed by the central registry;

(d) maintaining a record of COSMIC TOP SECRET documents held, distributed or destroyed by the central registry;

(e) maintaining an up-to-date list of all COSMIC registries and control points within other member nations and NATO commands and agencies, and those control points not mentioned in paragraph (b) above with which he/she normally corresponds, together with the names and signatures of their appointed control officers and alternates;

(f) physical safeguarding of all COSMIC TOP SECRET information held within the registry in accordance with regulations contained in Section IV.

COSMIC REGISTRIES AND CONTROL POINTS

109. The control officer of a COSMIC registry or control point will be responsible for:

(a) transmission of COSMIC TOP SECRET information in accordance with regulations contained in Section VII;

(b) maintaining an up-to-date list of all persons authorized to have access to COSMIC TOP SECRET information within the government department or NATO command or agency served;

(c) distribution of COSMIC TOP SECRET documents in accordance with the instructions of the government department or NATO command or agency served;

(d) before despatch, ensuring that all addressees are authorized to have access to COSMIC TOP SECRET information;

(e) obtaining receipts for all COSMIC TOP SECRET documents distributed;

(f) maintaining an up-to-date record of all COSMIC TOP SECRET documents held or circulating within the government department or NATO command or agency or passed to other COSMIC registries or control points and, in the case of a registry, maintaining records of destruction;

(g) ensuring that COSMIC TOP SECRET documents are returned from a control point to the responsible registry when no longer required;

(h) maintaining an up-to-date list of COSMIC registries and control points with whom he/she is authorized to exchange COSMIC TOP SECRET information together with the names and signatures of their control officers and alternates;

(i) the physical safeguarding of all COSMIC TOP SECRET documents held on charge in accordance with the regulations laid down in Section IV.

ANNUAL MUSTERS

110. At least once every 12 months, each COSMIC registry will carry out a muster of all COSMIC TOP SECRET documents for which it is accountable. A document is deemed to have been accounted for if:

(a) it is physically sighted; or

(b) a receipt is held from the COSMIC registry to which it has been transferred; or

(c) a destruction certificate for the document is held; or

(d) a downgrading or declassifying order is held.

111. Registries will forward to the appropriate central registry as soon as possible a certificate to the effect that this annual muster has been completed.

112. Results of annual musters of all COSMIC central registries will be reported by the security authorities concerned to the NOS by 1st April of each year.

SECTION VII

PREPARATION, DISSEMINATION, TRANSMISSION AND DESTRUCTION OF NATO CLASSIFIED INFORMATION

PREPARATION

113. Information marked COSMIC or NATO is subject to the control and protection set forth in NATO security procedures and information management directives. Neither marking should be applied to a national document, except to copies which are specifically for circulation within NATO.

114. Information classified NATO CONFIDENTIAL and above will be handled, processed, translated and reproduced only by those persons authorized access to NATO information of at least that level of security classification.

115. All documents, including permanently bound books and pamphlets or reproduction thereof, will have their overall classification conspicuously stamped, marked, typed, printed or written at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, on the back page and on the outside of the back cover (if any). Each other written or printed page will bear at the top and bottom the overall security classification of the component section of the document (i.e. main document, annex, appendix, etc.) of which it forms a part. Where applicable, within the provisions of paragraph 39 where titles and paragraphs are classified separately or have no classification, the appropriate initials, e.g. CTS, NS, NC, NR or NU will be inserted within parentheses immediately following the title or the numerical designation of the paragraph. The following additional rules apply in respect of:

(a) Charts, maps and drawings

The classification of charts, maps and drawings will also be marked under the legend, titleblock or scale and on the outside when folded.

(b) Photographic Material

Photographs, films, including negatives and positives, and their spools and containers, shall be marked in such a manner as to ensure that any recipient or viewer will know that classified information of a specified level is involved.

(c) Tape Recordings

The spools containing tapes, including video tapes, on which classified information has been recorded must be clearly marked with the highest classification of information ever recorded thereon. This classification will remain on the spool until the tape has been degaussed by a method nationally approved for declassification of the type of tape involved. When recording, the appropriate classification should be quoted at the beginning and end of each passage. Each end of classified tapes will be visibly marked with its classification in case the tapes become detached from their spools. Recordings shall be kept in containers or on spools that bear conspicuous classification markings.

(d) Other Material

The assigned security classification and, where appropriate, downgrading and declassification instructions shall be conspicuously stamped, printed, written, painted or affixed by means of a tag, sticker, decal or similar device on classified material other than that described above.

116. The security classification and the marking will be kept separate from all other reference markings wherever they appear on a document. The letters used for security classifications and markings shall, wherever possible, be of a different type or reproducible colour and larger than those used in the text of a document and in no case shall they be smaller.

117. When a document is downgraded or declassified by an originator, the original NATO classification on the first page will be lined through and the new classification or NATO UNCLASSIFIED, as the case may be, will be shown immediately above or under it, together with the authority for such action as well as the date and initials of the person effecting the amendment. The serving registry must be informed of any such changes.

118. All NATO classified documents will bear a reference number and date on the first page. Each COSMIC TOP SECRET and NATO SECRET document will bear the reference number on each page and a copy number on the first page.

119. A new annex or appendix added to a COSMIC TOP SECRET or NATO SECRET document or designed to replace a portion of an existing COSMIC TOP SECRET or NATO SECRET document will state on the first page:

(a) the reference number of the original document with its date of issue; and

(b) the purpose of the new text, e.g. addition or substitution.

120. The originating date of a COSMIC TOP SECRET or NATO SECRET document should be retained even though amendments are made to it unless or until it is the subject of fundamental revision and re-issue.

121. The first page of a NATO classified document or its index or table of contents will include a complete list of annexes and appendices.

122. Each written or printed page of a document will be page numbered. The total number of pages of COSMIC TOP SECRET and NATO SECRET documents will be stated on the first page. To facilitate the checking of the completeness of a COSMIC TOP SECRET and NATO SECRET document when it consists of more than one component (e.g. enclosures, annexes, appendices, etc.) a list of effective pages must be included in the document.

DISTRIBUTION

Dissemination

123. Dissemination of NATO classified information will be on a need-to-know basis. Information classified NATO CONFIDENTIAL and above will be restricted to persons currently cleared and authorized to have access to such information.

124. The initial dissemination of information classified NATO CONFIDENTIAL and above should be specified by the originator. The addressee may authorize such wider distribution as may be required in accordance with the principle laid down in paragraph 123 above.

125. Dissemination of COSMIC TOP SECRET information will be through registry channels except

125. Dissemination of COSMIC TOP SECRET information will be through registry channels except as provided for in paragraph 103. COSMIC TOP SECRET documents on loan outside a registry or control point will be returned when no longer required.

EXTRA COPIES, TRANSLATIONS AND EXTRACTS

126. If an addressee requires extra copies of a COSMIC TOP SECRET document, these should normally be obtained, except in the case of a signal/message, from the originating member nation or NATO command or agency. It is recognized, however, that it may be necessary in exceptional cases for an addressee to make copies or translations of COSMIC TOP SECRET documents. In such cases reproductions or translations of COSMIC TOP SECRET documents and signals/messages must:

(a) be authorized by the control officer of a COSMIC central registry. This authorization may be delegated to a control officer of a COSMIC registry, but in such cases a report of such reproduction or translation will be reported to the COSMIC central registry which will monitor such reproductions and translations and record the copies made. In the case of a signal/message, the officer in charge of the signal office primarily concerned may authorize the production of those copies and translations necessary to make initial distribution. Thereafter the authority for reproduction and translation of signals/messages will be the same as for other COSMIC TOP SECRET documents;

(b) bear the reference and copy number of the original document together with the name of the originating authority and that of the reproducing element;

(c) be marked with an identifying copy number locally assigned by the element making the reproduction or translation;

(d) display the COSMIC TOP SECRET marking and classification and all other markings according to the original document;

(e) be translated, typed or otherwise reproduced by persons authorized to have access to COSMIC TOP SECRET information;

(f) be recorded and distributed by the appropriate COSMIC registry.

127. If the originator of a COSMIC TOP SECRET document wishes to retain exclusive control of its reproduction, it will contain a prominent and suitable note to that effect, for example:

"Reproduction of this document, in whole or in part, is prohibited unless authorized by the originator."

or

"Reproduction of paragraphs ... to ... annexes ... and ... is prohibited unless authorized by the originator."

These special restrictions should be applied with discrimination and as infrequently as possible.

128. Notwithstanding these reproduction prohibitions, addressees whose national language is not that of the document may translate the document in one copy provided the provisions of paragraph 126 have been met and the translation includes any statement about limitations on reproduction. Such translations will, additionally, be reported to the originator.

129. Reproductions and translations of documents classified NATO SECRET and below may be produced by the addressee under strict observation of the need-to-know principle. Security measures laid down for the original document will be applied to such reproductions and/or translations. If classified NATO SECRET they must be marked with identifying copy numbers. The number of reproductions and/or translations of NATO SECRET documents and their copy numbers must be recorded.

130. Extracts of NATO classified documents may be included, if necessary, in documents which need to be seen by persons in member nations or NATO commands or agencies who have not been authorized access to NATO classified information, provided they have national security clearance to the level of the classification of the extracted information.

131. In order to ensure that the extracts are properly protected, such papers will be given an appropriate security classification and will be distributed on a need-to-know basis. An extract from a classified document shall bear the classification of the document or component thereof (if individually classified) from which it is taken unless it is obvious that it justifies another classification. Otherwise it will be referred to the original or higher classification authority for determination of a less restrictive classification. If, however, in exceptional circumstances, the originator of a COSMIC TOP SECRET document desires to control the further dissemination of information contained therein, the originator will indicate the restrictions specified in paragraph 127 above. The provisions of paragraph 128 above are not applicable under these circumstances.

MICROFILMING, STORAGE ON OPTICAL DISK OR MAGNETIC MEDIA

132. For emergency purposes or to minimize storage problems, NATO classified documents may be microfilmed, stored on optical disks or magnetic media provided:

(a) the microfilm or storage process is undertaken by personnel who possess a current and appropriate NATO clearance;

(b) the microfilms, optical disks or magnetic storage media are afforded the same security protection as the original document and any microfilms and optical disks containing more than one classification will be afforded the security protection of the highest classification appearing on the microfilm, optical disk or magnetic storage media;

(c) in the case of NATO SECRET documents, a record of the microfilming, storage on optical disk or magnetic media is made;

(d) in the case of COSMIC TOP SECRET documents:

(i) the microfilming, storage on optical disk or magnetic media is authorized by the control officer of the registry concerned;

(ii) the microfilming, storage on optical disk or magnetic media of the documents is brought under registry and inventory control applicable to COSMIC TOP SECRET documents and reported in the annual muster along with other COSMIC TOP SECRET documents held.

(iii) the control officer of a registry authorizing microfilming or storage on optical disk reports the fact to the control officer of the COSMIC central registry.

REPRODUCTION FROM MICROFILM, OPTICAL DISK OR MAGNETIC STORAGE MEDIA

133. Copies from microfilm, optical disk or magnetic storage media may be produced provided:

(a) the process is undertaken by personnel who possess a current and appropriate NATO clearance;

(b) copies bear the full original classification and marking of the original document, plus, in the case of COSMIC TOP SECRET and NATO SECRET information, a designation to identify the document as such (i.e. Reproduction Copy No. 1, Reproduction Copy No. 2, etc.);

(c) in the case of NATO SECRET information the document produced will be properly recorded;

(d) copies no longer required will be destroyed in accordance with the regulations set forth in paragraphs 149 and 150 below;

(e) additionally, in the case of COSMIC TOP SECRET information:

(i) the control officer of a registry holding COSMIC TOP SECRET microfilm, optical disk or magnetic storage media has authorized the reproduction;

(ii) copies when produced are brought under registry and inventory control applicable to COSMIC TOP SECRET documents and reported in the annual muster along with other COSMIC TOP SECRET documents held;

(iii) the control officer of a registry authorizing reproduction from microfilm, optical disk or magnetic storage media reports the number of copies made to the control officer of the COSMIC central registry.

TRANSMISSION

Packaging

134. Documents classified NATO CONFIDENTIAL and above will be transmitted under double opaque and strong cover. The inner cover will be secured, will be stamped with the appropriate NATO classification and bear the full designation and address of the addressee. When necessary the inner envelope may be marked "To be opened only by ...". The inner cover will be enclosed in a secure outer cover. The outer cover will bear a designation (but not a name) and address and a package number for receipting purposes and will not indicate the classification of the contents or the fact that it contains classified information. If documents are transmitted under double cover by courier, the outer cover should be clearly marked, e.g. "by courier only". A locked pouch or box or a sealed diplomatic pouch may be considered as the outer cover.

135. When NATO classified documents are carried between offices of the same building or enclosed group of buildings by officials (other than messengers), they will be covered in such a way as to prevent observation of their contents. If they are carried by messengers they will be enclosed so that the messenger does not have access.

Document Control

136. A receipt will be enclosed in the inner cover of COSMIC TOP SECRET and NATO SECRET documents. NATO CONFIDENTIAL documents will be receipted for only if required by the originator/transmitter. The receipt will be immediately returned to the sender after having been dated and signed. COSMIC TOP SECRET documents transmitted between registries and control points will be opened and receipted for only by a COSMIC control officer. In exceptional circumstances, the inner cover of a COSMIC TOP SECRET document may be addressed to an individual through a COSMIC control officer, in which case only that individual will open and receipt for the documents. The receipt and disposal of such documents will be recorded in the usual manner.

137. A continuous receipt system is required for COSMIC TOP SECRET documents. For transmission of NATO SECRET documents within member nations and NATO commands and agencies, each member nation or NATO command or agency concerned will establish internal controls, to include periodic inspections and such other appropriate measures as will ensure that NATO SECRET documents are controlled and their movements recorded.

138. A receipt, which requires no security classification, will quote only the reference number, date, copy number and language of the document but not its title, if classified.

139. For NATO CONFIDENTIAL and above, couriers and messengers will obtain receipts against package numbers. Receipts for packages containing NATO CONFIDENTIAL documents are only required if carried outside the confines of a building or enclosed group of buildings.

National Transmission

140. National transmission of documents classified NATO CONFIDENTIAL and above will be by authorized messenger service or courier. Additionally, NATO SECRET and NATO CONFIDENTIAL documents may be transmitted by a postal service under conditions fixed by national regulations.

141. Whenever a messenger service is used for the carriage of documents classified NATO CONFIDENTIAL and above outside the confines of a building or an enclosed group of buildings, the packaging and receipting provisions contained in paragraphs 134, 136 and 139 above will be complied with. The personal carriage of documents classified NATO CONFIDENTIAL and above may be permitted within a member nation under conditions no less stringent than national regulations permit for the personal carriage of national documents of equivalent classification and provided the relevant provisions of paragraph 145 are complied with.

International Transmission

142. The international transmission of material classified NATO CONFIDENTIAL and NATO SECRET will be by diplomatic pouch, military courier, registered mail through postal services approved by the NATO Security Committee, or personal carriage subject to compliance with paragraph 145. Material classified up to and including NATO SECRET that cannot be transmitted by one of the foregoing methods and that are relevant to the industrial domain may be transmitted by other means subject to compliance with the relevant provisions in Enclosure "D". The international transmission of COSMIC TOP SECRET material will be by diplomatic pouch or military courier.

Transmission of NATO RESTRICTED Documents

143. NATO RESTRICTED documents will be transmitted nationally or internationally by such means as are authorized by the appropriate NSA. In the case of NATO commands and agencies, the rules concerning such transmissions will be set by the head of the command or agency, after agreement with the NSA of the member nation in which the material is despatched.

Security of Courier and Messenger Personnel

144. All couriers and messengers employed to carry documents classified NATO CONFIDENTIAL and above will be security cleared by the appropriate national authority. Couriers and messengers will be instructed on their duties for protecting the documents entrusted to them.

Personal Carriage

145. Each member nation and NATO command and agency will prepare instructions covering the personal carriage of documents classified NATO CONFIDENTIAL and above by hand of persons other than couriers and messengers, based on these regulations. These instructions will make it clear that:

(a) in no circumstances may COSMIC TOP SECRET documents be carried internationally;

(b) the bearer must be cleared for access to at least the level of classification of the documents carried;

(c) a record must be kept in the appropriate registry in the case of COSMIC TOP SECRET documents, and in the appropriate offices in the case of NATO SECRET or CONFIDENTIAL documents, of all documents carried. The receipt for the documents or the actual documents, if returned, must be checked against this record;

(d) the documents will be carried in a locked container which will bear a label with an identification and instructions to the finder;

(e) the documents must not leave the possession of the bearer unless they are housed in accordance with the provisions for safe custody contained in Section IV, i.e. the documents must not be left unattended (e.g. in hotels, and vehicles) or stored in hotel safes or luggage lockers;

(f) the documents must not be read in public places (e.g. in aircraft, trains, etc.); and, when international carriage is involved, that:

(g) the container or document package will be covered by an official seal, or likewise protected under procedures designed to prevent or discourage customs examination;

(h) the bearer must carry a courier certificate (copy at Annex V) recognized by all NATO nations authorizing him to carry the package as identified;

(i) the bearer's travel arrangements with regard to destinations, routes to be taken and means of transportation to be used, will be in accordance with NATO regulations (Annex VII refers) or - if national regulations with respect to such matters are more stringent - in accordance with such regulations.

The bearer will be required to read and sign these instructions.

ELECTRICAL TRANSMISSION

146. Communications security measures have been devised to ensure the secure electrical transmission of NATO classified information. Only authorized communications centres and/or terminals may effect transmission of information classified NATO CONFIDENTIAL and above. The detailed rules for the electrical transmission of NATO classified information are laid down in current NATO communications security instructions.

147. Only cryptographic systems specifically authorized by the NAMILCOM will be used for the encryption of information, however transmitted (e.g. voice, data or telegraph), classified NATO SECRET and above. Cryptographic systems approved by a member nation or by the

NAMILCOM will be used for the encryption of NATO CONFIDENTIAL and below. When speed is of paramount importance and means of encryption are not available, information classified NATO RESTRICTED may be transmitted in clear text.

148. Under certain exceptional circumstances, such as during impending or actual terrorist activities or during impending or actual hostilities, when speed of delivery is so essential that time cannot be spared for encryption and it is considered that the transmitted information cannot be acted upon by the opposition in time to influence current operations, NATO RESTRICTED, NATO CONFIDENTIAL and NATO SECRET information may be transmitted in clear text, provided each occasion is individually authorized by the head of the originating organization.

DESTRUCTION OF NATO CLASSIFIED INFORMATION

Routine Destruction

149. To prevent unnecessary accumulation, superseded information and information no longer needed will be destroyed as soon as practicable. It is not necessary to await destruction instructions from the originator. Holders of NATO classified information will maintain a continuing review of documents to determine whether they can be destroyed.

150. Surplus or superseded classified information, including all classified waste such as spoilt copies, working drafts, shorthand notes, carbon paper, etc., will be destroyed under appropriate security regulations and supervision into an unrecognizable form and beyond reconstruction.

(a) except as provided for in paragraph (c) all COSMIC TOP SECRET documents for destruction will be returned to the registry which holds them on charge. Each COSMIC TOP SECRET document will be listed on a certificate of destruction which is to be signed by the COSMIC control officer and by the official witnessing the destruction, who must be authorized to have access to COSMIC TOP SECRET information. Destruction certificates of COSMIC TOP SECRET documents which have been microfilmed, stored on optical disk or magnetic media should indicate that fact;

(b) destruction certificates and control records for COSMIC TOP SECRET documents will be retained for a minimum period of 10 years in a registry. Copies need not be forwarded to the originator or the appropriate central registry unless specifically requested;

(c) the NSA may authorize the responsible control officer of any deployed or isolated military unit to destroy COSMIC TOP SECRET documents which are no longer needed, provided properly executed destruction certificates are furnished to the registry which holds them on charge;

(d) the destruction of documents classified NATO SECRET will be recorded and such record will be signed by destruction and witnessing officials both being appropriately cleared and authorized to have access to NATO SECRET information. Destruction records and document control records will be retained in the office performing the destruction for a period specified by individual member nations and NATO commands and agencies, but not less than three years;

(e) the recording of the destruction and the retaining of control records of NATO CONFIDENTIAL or NATO RESTRICTED documents will be in accordance with procedures established by member nations and NATO commands and agencies;

(f) classified waste destroyed immediately after the material is produced need not have its destruction recorded. However, where the process of production includes some form

of certification and/or accounting arrangement, certification of destruction will be in accordance with procedures established by member nations and NATO commands and agencies in respect of the classification of the material involved.

EMERGENCY PLANNING

151. Each member nation and NATO command and agency will prepare plans based on local conditions for safeguarding NATO classified information in case of emergency, including destruction and evacuation plans where applicable, and will promulgate within their respective organizations such instructions as are considered necessary to prevent NATO classified information falling into hostile hands.

152. Emergency safeguarding and/or destruction of NATO SECRET and NATO CONFIDENTIAL material must not interfere with the safeguarding and/or destruction of COSMIC TOP SECRET material, including crypto material, which will always retain priority over any other NATO material. Specific rules governing emergency safeguarding and destruction of crypto material are promulgated by the NAMILCOM.

SECTION VIII

SECURITY MEASURES FOR MINISTERIAL AND OTHER CLASSIFIED MEETINGS

153. Security measures commensurate with the level of the meeting and the sensitivity of the information to be discussed must be taken by the member nation or NATO command or agency convening the meeting. Such measures will be based upon the information, physical and personnel security requirements of this document and such other meeting security requirements as deemed necessary by the responsible authorities.

SECTION IX

BREACHES OF SECURITY AND COMPROMISES OF NATO CLASSIFIED INFORMATION

GENERAL

154. The protection of NATO classified information depends on the design of appropriate security regulations to give effect to approved security policy and guidance, and on the effective implementation of these regulations by education and supervision backed up by disciplinary and, in extreme cases, legal sanctions.

DEFINITIONS

155. Breach of Security: a breach of security is an act or omission contrary to existing NATO general or local security regulations, the results of which may endanger or subject to compromise NATO classified information.

156. Compromise: NATO classified information is compromised when knowledge of it has, in whole or in part, passed to unauthorized persons, i.e. individuals without appropriate NATO security clearance or authority to have such access, or when it has been subject to risk of such passing(1).

ACTION ON BREACHES OF SECURITY

157. All breaches of security must be reported immediately to the appropriate security authority(2). Each reported breach of security will be investigated by persons who have security and investigative experience, if possible, and who are independent of those persons immediately concerned with the breach, to determine:

(a) whether NATO classified information has been compromised;

(b) if so, whether all the unauthorized persons who have or could have had access to the information have at least some NATO security clearance and are known from existing records to be of such reliability and trustworthiness that no harm to NATO will result from the compromise; and

(c) what remedial, corrective or disciplinary (including legal) action is recommended.

---

(1) (i) classified information lost, even temporarily, outside a security area is to be presumed compromised;

(ii) classified information lost, even temporarily, inside a security area, including that in documents which cannot be located at periodic inventories, is to be presumed compromised until investigation proves otherwise.

(2) Security authorities will, in cases of breaches involving ATOMAL information, comply with the procedures detailed in C-M(68)41(5th revise).

158. Where the investigation yields positive answers to both 157(a) and (b) the administrative authority is to take steps to brief and/or indoctrinate the individuals concerned, as appropriate, to the classification and category of the information to which they have had inadvertent access. The administrative authority can close such cases without reporting to the NOS. Where the investigation yields a positive answer to 157(a) and a negative answer to either part of 157(b) the compromise is reportable to the NOS as described below.

Records of Breaches of Security

159. Heads of NATO commands and agencies are to arrange for records of breaches of security regulations, including reports of investigation and remedial and corrective actions, to be kept for three years and to be available during security inspections.

Reporting of Compromises

160. When a compromise of NATO classified information has to be reported under the terms of paragraph 158, the report is to be forwarded through the NSA or the head of the NATO command or agency concerned to the NOS. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances.

161. Initial reports are to be forwarded immediately to the NOS in cases where it has been determined that:

(a) COSMIC TOP SECRET or NATO SECRET information is involved; or

(b) there are indications or suspicions of espionage (provided the report would not hamper the investigations in hand).

162. Initial reports should contain the following information:

(a) a description of the information involved, including its classification and marking reference and copy number, date, originator, subject and scope;

(b) a very brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise and, if known, the number and/or category of unauthorized persons who have or could have had access;

(c) whether the originator has been informed.

163. Further reports are to follow as developments warrant. Reports on compromise of NATO CONFIDENTIAL information are to be forwarded when the investigation has been completed and should contain information as requested in paragraph 162(a), (b) and (c). Cases involving NATO RESTRICTED information need be reported only when they present unusual features. In all cases of reportable compromise the final report, or a progress report, of the investigation will be with the NOS within 90 days of the initial report.

RELIEF FROM ACCOUNTABILITY FOR LOST ACCOUNTABLE DOCUMENTS

164. When the final report of investigation shows that an accountable document has been irretrievably lost rather than mislaid, the NSAs or the head of the NATO command or agency may grant relief from accountability.

ACTION BY THE ORIGINATING NATO COMPONENT

165. The main purpose of reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimize the damage. Reports of the damage assessment and minimizing action taken should be forwarded to the NOS.

ACTION BY THE NATO OFFICE OF SECURITY (NOS)

166. The NOS will:

(a) coordinate enquiries where more than one security authority is concerned;

(b) coordinate, if necessary, with the originators and the security authorities concerned the final assessment of the damage done to NATO and any minimizing action to be taken;

(c) recommend to, and/or conduct in agreement with the security authority concerned, further investigations whenever it considers them necessary;

(d) inform the Secretary General of NATO, whenever the gravity of damage to the Alliance so warrants.

ACTION BY THE SECRETARY GENERAL OF NATO

167. The Secretary General of NATO may request the appropriate authorities to make further investigations and to report.

COMPROMISES OF CRYPTOGRAPHIC MATERIAL

168. Separate provisions relating to the compromise of cryptographic material have been issued by the NAMILCOM to communications security authorities of member nations and NATO commands and agencies.

SECTION X

PROTECTION OF NATO CLASSIFIED INFORMATION STORED, PROCESSED OR TRANSMITTED IN AUTOMATIC DATA PROCESSING (ADP) SYSTEMS AND NETWORKS

INTRODUCTION

169. Within this Section, the specific element of the Security Authority, responsible for ensuring compliance with NATO security policy in respect of Automatic Data Processing (ADP) systems or networks, is referred to as the Security Accreditation Authority (SAA).

170. The security policy and requirements in this Section shall apply to all ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above.

171. ADP systems and networks storing, processing or transmitting information with the highest classification of NATO RESTRICTED shall also require security measures to ensure the protection of the information, and to control disclosure of, and access to, the information, based on need-to-know. The security measures, to be determined by the appropriate Security Accreditation Authority, shall be commensurate with the policy stated in this document and the current NATO communications security policy.

172. Protection of weapon or sensor systems containing embedded ADP systems shall be determined and specified in the general context of the systems to which they belong using applicable provisions of this Section to the extent possible.

173. Definitions of the following terms used in this Section are included in paragraphs 270 to 285 : Security modes of operation (Dedicated, System High and Multi-Level), ADP security, Computer security (COMPUSEC), COMPUSEC product, Communications security (COMSEC), Evaluation, Certification, Accreditation, ADP system, ADP system security features, ADP network, ADP network security features, ADP area, and Remote Terminal/Workstation Area. The definition of information category designations is included at paragraph 268.

THREATS TO, AND VULNERABILITIES OF, ADP SYSTEMS AND NETWORKS

174. In general terms, a threat can be defined as a potential for the accidental or deliberate compromise of ADP system or network security (loss of confidentiality, loss of integrity, or loss of availability). A vulnerability can be defined as a weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency; and may be technical, procedural or operational in nature.

175. Where NATO classified information is stored, processed or transmitted in ADP systems and networks, in a concentrated form designed for rapid retrieval, communication and use, this information may be vulnerable to unauthorised or denied user access, and to unauthorised disclosure, corruption, modification or deletion. Furthermore, the complex and sometimes fragile equipment is expensive and often difficult to repair or replace rapidly. These ADP systems and networks are therefore attractive targets for intelligence-gathering operations and sabotage, especially if security measures are thought to be ineffective.

SECURITY MEASURES

176. The security measures stated in this Section provide protection against the unauthorised disclosure of information (the loss of confidentiality). To achieve adequate security protection of an ADP system or network storing, processing or transmitting information classified NATO CONFIDENTIAL and above, the appropriate standards of conventional security shall be specified, along with appropriate special security procedures and techniques particularly designed for each ADP system or network.

177. A balanced set of security measures (physical, personnel, procedural, computer and communication) shall be identified and implemented to create a secure environment in which an ADP system or network operates.

178. Computer security measures (hardware and software security features) shall be required to implement the need-to-know principle, and to prevent or detect the unauthorised disclosure of information. The extent to which computer security measures are to be relied upon shall be determined during the process of establishing the security requirement. The process of accreditation shall determine that an adequate level of assurance is present to support this reliance on computer security measures.

179. The integration of the ADP system and a communications system shall also require that the communications security aspects be assessed as part of the overall security.

SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT (SSRS)

180. For all ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above, a System-Specific Security Requirement Statement (SSRS) shall be required to be produced by the ADP System Operational Authority (ADPSOA) or appropriate project staffs, and approved by the SAA.

181. The SSRS shall be formulated at the earliest stage of a project's inception and shall be developed and enhanced as the project develops, fulfilling different roles at different stages in the project and system's life cycle.

182. The SSRS shall form the binding agreement between the ADP SOA and the SAA against which the ADP system or network is to be accredited.

183. The SSRS is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met. It is based on NATO security policy and a risk assessment, or imposed by parameters covering the operational environment such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation or user requirements. The SSRS is an integral part of project documentation submitted to the appropriate authorities for technical, budgetary and security approval purposes. In its final form, the SSRS constitutes a complete statement of what it means for the ADP system or network to be secure.

SECURITY MODES OF OPERATION

184. All ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above shall be accredited to operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation, or their national equivalent :

(a) dedicated;

(b) system high; and

(c) multi-level.

185. The Information Category Designation, US-SIOP, shall only be processed in the dedicated mode.

186. The definition and requirements for each security mode of operation are stated in paragraphs 270 to 272.

SECURITY RESPONSIBILITY

[*Note - paragraphs 187 to 191 shall apply only to NATO commands and agencies.*]

187. The NATO Security Committee (NSC), with the advice of the NC3 Board, is responsible for advising the North Atlantic Council (NAC) regarding security policy for ADP systems or networks. The NOS and the NHQC3S act as secretariats for these Committees.

188. Any problem regarding security of an ADP system or network which is not resolved by the authorities in the normal military chain of command or civilian hierarchy, shall be referred to the NOS and/or to the NHQC3S for appropriate action.

189. Major NATO Commanders, heads of NATO military and civil agencies are required to establish appropriate security organizations at all international command and agency levels for the maintenance of security in accordance with NATO security procedures (paragraphs 11 and 17, Section I).

190. Where NATO ADP systems or networks are involved, some aspects of security require specialist knowledge of ADP hardware and software, communications security and counter-intelligence services; proper co-operation between these different elements should be assured in the security organization.

191. The Major NATO Commander or head of the NATO military or civil agency shall also designate a security authority responsible overall for the security organization in accordance with Section I. In addition, he shall designate an ADP Authority to provide guidance to the security authority on the implementation and control of special security features designed as part of ADP systems or networks.

Security Accreditation Authority (SAA)

192. The SAA shall be responsible for granting approval to an ADP system or network to store, process or transmit NATO classified information, to a defined classification level (including, where appropriate, special category(ies), in its operational environment.

193. The SAA shall be a National Security Authority (NSA), Major NATO Commander (MNC) or the NOS, or their delegated / nominated organizations or representatives, dependent upon the ADP system or network to be accredited.

194. The SAA shall exercise responsibility for security on behalf of the head of an organization, an MNC or the head of a NATO military or civil agency, and in all but the most exceptional cases its responsibility for security and its authority to enforce security standards throughout an organization, an MNC or an agency is final.

195. The SAA shall establish an Accreditation Policy or Strategy, as part of its overall security policy, clearly stating the conditions under which it shall be called upon to accredit an ADP system or network (see paragraph 252).

ADP System Operational Authority (ADPSOA)

196. The ADPSOA (which either acts as or appoints a System Manager/Management) is the person or unit delegated the responsibility from the ADP Authority, for the implementation and operation of the ADP system or network. This responsibility extends throughout the life cycle of the ADP system or network from the project concept stage, through system specification, installation testing, accreditation, operation, modification, to final disposal. In some circumstances, the role of the ADPSOA may be passed from one part of an organization to another during the various phases of the life cycle. It is important that the role be identified and allocated at an early stage, and be continuous throughout the life cycle.

197. The ADPSOA should act as the co-ordinator for the co-operation of the Security Accreditation, ADP and Communications Authorities wherever an organization :

(a) plans to develop or acquire an ADP system or network;

(b) proposes to make changes to an existing equipment configuration;

(c) proposes to interconnect an ADP system or network with another ADP system or network;

(d) proposes to make changes to the security mode of operation of an existing ADP system or network;

(e) proposes to make any changes to existing, or to adopt new, software which may have an impact on ADP system or network security (see paragraphs 242 to 245);

(f) proposes to undertake work of a higher security classification than the one for which an existing ADP system or network has been accredited; and

(g) plans, proposes or intends to undertake any other activity that may affect the security of an accredited ADP system or network (for example, increasing substantially the size of the user population).

198. The ADPSOA, as directed by and in co-operation with the Security Accreditation and ADP Authorities, should decide on the security standards and practices to be employed by the supplier to his development, installation and testing of the ADP system or network. In addition, the ADPSOA should be responsible for the justification, selection, implementation and control of those technical security features designed as part of the overall ADP system or network. From the very conception of the requirement for an ADP system or network, or the update or modification of such ADP systems or networks, the required security and ADP management structure, with appropriate responsibilities, should be put in place for the implementation and supervision of security throughout the life cycle of the ADP system or network.

ADP System Security Officer

199. An ADP System Security Officer shall be appointed by the ADPSOA, to be responsible for the supervision of the development, implementation and maintenance of the security measures within the ADP system, including the preparation of Security Operating Procedures (SecOP's) (see paragraphs 240 and 241). In addition, for larger ADP systems and networks, it may be appropriate to nominate additional persons (for example, for specific areas,

divisions or directorates of an organization) who carry out these duties according to the conditions set out by the ADP System Security Officer in the Security Operating Procedures (SecOps).

ADP Network Security Officer

200. When two or more ADP systems are interconnected, or for a single large networked ADP system, an ADP Network Security Officer responsible for co-ordinating network security arrangements shall be appointed, who shall liaise with those responsible for communications security (see paragraphs 230 to 231, and 240 to 241). The parties concerned shall mutually agree on the person nominated to hold the post of ADP Network Security Officer.

ADP Site Security Officer

201. An ADP Site Security Officer shall be appointed by the appropriate NSA (or their nominated representative), or the MNC Security Authority (or their nominated representative), or the head of the NATO Military or Civil Agency, to be responsible for ensuring the implementation and maintenance of the security measures applicable to the site.

202. The site may be a particular location, or group of locations where they are allocated to an ADP system or network. The security responsibility for each remote terminal/workstation area shall also be clearly identified. The duties of the ADP Site Security Officer may be covered by an organization, HQ's or Unit's Security Officer as part of that person's overall duties.

Users

203. Under the direction of the ADP System/Network Security Officer(s), all ADP system or network users have a responsibility for their ADP system or network's security. With all users briefed and conscientious about their security duties, an increase in the overall effectiveness of the security regime can be obtained.

ADP Security Training

204. ADP security education and training shall be available at various levels, and for various personnel, as appropriate, within an organization : senior level management, ADP system/network development staff, Security Authority staff, ADP Site/System/Network Security Officer(s), and users.

PERSONNEL SECURITY

205. Users of the ADP system or network shall be cleared and have a need-to-know, as appropriate for the classification (including caveats/categories) and content of the information stored, processed or transmitted within their particular ADP system or network.

206. Because of the vulnerability of information to unauthorised or denied access, and to disclosure, corruption, modification or deletion, particular care should be taken in regard to the training and supervision of personnel, including development staff, who have access to the ADP system or network. The SAA should, in consultation with either the project manager or the ADP SOA, designate, during the project inception stage of each ADP system or network, all sensitive positions and specify the level of clearance and supervision required for all personnel occupying them.

207. ADP systems and networks should be specified and designed in a way that facilitates the allocation of duties and responsibilities to ADP personnel so as to prevent one person having complete knowledge or control of the system security keys (for example, passwords and Personal Identification Devices (PID's)) and software. Procedures should be established for each ADP system or network to segregate programming and system or network operation. As far as practicable, personnel should be prohibited from both programming and operating a given system and procedures should be established to detect such activity. The aim should be that collusion between two or more individuals would be necessary for alteration or intentional degradation of the system or network to take place. The SSRS should clearly state those situations where the "two-man rule" is to be implemented.

208. In order to ensure that security measures are sensibly devised and implemented, ADP and security staff with responsibility for ADP security should be trained and briefed to the extent necessary to understand each other's problems.

PHYSICAL SECURITY

209. ADP and remote terminal / workstation areas (as defined in paragraphs 284 and 285) in which information classified NATO CONFIDENTIAL and above is presented, stored, processed or transmitted by ADP means, or where potential access to such information is possible, shall be established as NATO Class I or Class II security areas (paragraph 55) or national equivalent, as appropriate (see also paragraph 212).

210. The following measures are applicable to ADP and remote terminal/workstation areas where information classified NATO CONFIDENTIAL or above is processed :

(a) entry of both people and material to, and their departure from, ADP and remote terminal/ workstation areas shall be controlled by positive means (paragraph 55);

(b) ADP and remote terminal/workstation areas in which the security of the ADP system or network can be modified should never be occupied by only one authorised employee; and

(c) individuals requiring temporary or intermittent access to these areas should be authorised entry as visitors by the responsible ADP Site Security Officer. Visitors should be supervised at all times to ensure that they are denied unauthorised access to NATO classified information and that they do not gain access to the ADP equipment for illicit purposes.

211. Dependent upon the risk to security, and depending on the classification of the information being processed, there may be a requirement for the two-man rule to be applied to areas other than the ADP area. Such areas should be determined during the project inception stage and specified in the SSRS.

212. When an ADP system is to be operated in a stand-alone mode, permanently disconnected from another ADP system or network (for example, word processor, microcomputer, minicomputer, etc.) then, taking account of the physical environment, other procedural or technical security measures present, the hardware architecture and the part played by the ADP system in the overall function, it may be possible for the SAA to waive the aspect addressed in paragraph 210(b). In such cases, the SAA should prescribe rules appropriate to the composition of the ADP system, the level of classified information being processed and the special features identified.

CONTROL OF ACCESS TO AN ADP SYSTEM OR NETWORK

213. All information and material which controls access to an ADP system or network, for example passwords, shall be controlled and protected under arrangements commensurate with the highest classification and the category designation of the information to which it may give access.

214. When no longer utilised for this purpose, the access control information and material should be destroyed pursuant to Section VII.

SECURITY OF INFORMATION

215. It is incumbent upon the originator of the information to identify and classify, or indicate as unclassified, all information-bearing documents, whether they be in the form of hard-copy output or computer storage media. Each page of hard-copy output shall be marked, at the top and bottom, with the classification. Output, whether it is in the form of hard-copy or computer storage media shall have the same classification as the highest classification of the information used for its production, or be classified at the highest classification of a System High or Dedicated ADP system or network, unless the originator or higher authority for release of information has agreed, after review, to a different classification.

216. It is incumbent upon an organisation and its information owners to consider the problems of aggregation of individual elements of information, and the inferences that can be gained from related elements, and determine whether or not a higher classification is appropriate to the totality of the information.

217. The fact that the information may be a brevity code, transmission code or in any form of binary representation does not provide any security protection and should not, therefore, influence the classification of the information.

218. Prior to release from the ADP or remote terminal/workstation area, information-bearing documents classified NATO CONFIDENTIAL and above shall be controlled in accordance with the appropriate security regulations.

219. When information is transferred from one ADP system or network to another the information shall be protected during transfer and in the receiving ADP system or network in the manner commensurate with the original classification and category of the information.

220. All computer storage media shall be stored in a manner commensurate with the highest classification of the stored information or the media label, and at all times shall be appropriately protected.

221. Re-usable computer storage media used for recording NATO classified information shall retain the highest classification for which they have ever been used until that information has been properly downgraded or declassified and the media reclassified accordingly, or the media declassified or destroyed by an approved NATO or national procedure (see paragraphs 227 to 229).

CONTROL AND ACCOUNTABILITY OF INFORMATION

222. Automatic (audit trails) or manual logs shall be kept as a record of access to information classified NATO SECRET and above. These records shall be retained for a period to be agreed with the SAA. In respect of information classified COSMIC TOP SECRET or Special Category, the minimum retention period is 10 years; for information classified NATO SECRET, the minimum retention period shall be determined by NSAs, the MNC Security Authority or the NOS, but shall not be less than 3 years.

223. Classified outputs held within the ADP area may be handled as one classified item and need not be registered with the central (or other) document registry, provided the material is identified, marked with its classification and controlled within the ADP area until destroyed, reduced to record copy, or placed on permanent file. Appropriate records and control of classified material shall be maintained within the ADP area until the material is brought under formal document accountability control or destroyed.

224. Where output is generated from an ADP system or network storing, processing or transmitting NATO classified information, and transmitted to a remote terminal/workstation area from an ADP area, positive procedures, agreed by the SAA, shall be established for controlling the remote output. For NATO SECRET and above, such procedures shall include specific instructions for accountability of the information.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

225. All removable computer storage media classified NATO CONFIDENTIAL and above shall be properly identified and controlled (for NATO UNCLASSIFIED and NATO RESTRICTED, the local security regulations, approved by the NSA, the MNC Security Authority or the NOS, shall apply). The identification and controls shall include, as a minimum :

(a) for NATO CONFIDENTIAL and above, a means of identification (serial number and classification marking) for each separate medium (noting that the classification marking shall indicate the highest classification ever stored on the medium, unless downgraded according to approved procedures); fixed procedures for issue and receipt and for the final disposal of the computer storage media by destruction or other methods; records, manual or by computer printout, of the general content and classification and category designation of the information;

(b) for NATO SECRET and above, the details of removable computer storage media, including their general contents and classification, shall be maintained within an appropriate Registry; and

(c) spot checking and mustering of removable computer storage media, to ensure consistency with the identification and control procedures in place :

(i) for NATO CONFIDENTIAL, removable computer storage media shall be periodically spot-checked for their physical presence and contents (to ensure that a higher classification is not stored on the media);

(ii) for NATO SECRET, all removable computer storage media shall be periodically mustered , and spot-checked for their physical presence and contents (to ensure that a higher classification is not stored on the media); and

(iii) for COSMIC TOP SECRET and Special Category information, all removable computer storage media shall be mustered, on an annual basis, and shall be periodically spot checked for their physical presence and contents (to ensure that an inappropriate Special Category is not stored on the media).

226. Users shall take the responsibility for ensuring that NATO classified information is stored on media with the appropriate classification marking and protection. Procedures should be established to ensure that, for all levels of NATO information, the storage of information on computer storage media is being carried out in accordance with the security regulations.

DE-CLASSIFICATION AND DESTRUCTION OF COMPUTER STORAGE MEDIA

227. NATO classified information electromagnetically or otherwise recorded on re-usable computer storage media, shall only be erased in accordance with current approved procedures.

228. When a computer storage medium comes to the end of its useful life, it should be de-classified whereupon it may be released and handled as unclassified. If the medium cannot be de-classified, it shall be destroyed by an approved procedure. Computer storage media which have held COSMIC TOP SECRET or Special Category information, for example ATOMAL and US-SIOP, may be destroyed but shall not be de-classified and re-used.

229. NATO classified information in non-reusable form (i.e. hard-copy printout, punched cards, punched tape, etc.) shall be destroyed by procedures approved for the destruction of NATO classified material as laid down in Section VII.

COMMUNICATIONS SECURITY

230. Any means used for the electromagnetic transmission of NATO classified information shall follow the current NATO communications security instructions, set out in Military Committee communications security policy documents and supporting policy guidance documents. In addition, the electrical transmission of information shall comply with the policy set out in Section VII (See paragraphs 146 to 148).

231. An ADP system or network shall have the capability of positively denying access to NATO classified information at any or all of its remote terminal / workstations, when required, either by physical disconnection or by special software features approved by the SAA.

INSTALLATION AND RADIATION SECURITY

232. Initial installation of ADP systems or networks and any major change thereto should be so specified that installation is carried out by security-cleared installers under constant supervision of technically qualified personnel who are cleared for access to NATO classified information to the level equivalent to the highest classification which the ADP system or network is expected to store, process or transmit.

233. All equipment shall be installed in accordance with current policy as stated in "NATO Policy on Control of Compromising Emanations", MC 315. This policy references AMSG-719, "Installation of Electrical Equipment for the Processing of Classified Information" as the applicable document for systems and facility installations. National directives of technical equivalence may also be used.

234. ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above shall be appropriately protected from security vulnerabilities caused by compromising emanations, the study and control of which is referred to as "TEMPEST".

235. MC 315 determines the TEMPEST countermeasure requirements which are then implemented by the application of emanation control standards, such as AMSG 720 ("Compromising Emanations Laboratory Test Standard"), AMSG 784B ("Laboratory Test Standard for

Tactical Mobile Equipment/Systems (Vol. I); Test Procedures for Tactical Mobile Platforms (Vol. II)"), AMSG 788 ("Compromising Emanations Laboratory Test Standards for Protected Facility Equipment"), and AMSG 799 ("NATO TEMPEST Zoning Concept and Evaluation Procedures") for specific facilities based on the sensitivity of the information and the threat.

236. TEMPEST countermeasures for NATO assets shall be reviewed and approved by the NOS or the MNCs. For national assets which store, process or transmit NATO information, approval authority is the recognised national TEMPEST approving authority.

SECURITY DURING PROCESSING

237. All processing shall be carried out in accordance with the SecOps detailed in paragraphs 240 to 241 below.

238. Release of information classified NATO CONFIDENTIAL and above to unmanned facilities shall be prohibited unless special arrangements approved by the SAA Authority are in force, and have been specified in the SecOps.

239. In the case of ADP systems or networks that have potential or authorised users not possessing a security clearance, the storing, processing and transmitting of information classified COSMIC TOP SECRET or Special Category information shall not be permitted.

SECURITY OPERATING PROCEDURES (SecOps)

240. SecOPs are a description of the implementation of the security policy to be adopted, the operating procedures to be followed, and personnel responsibilities.

241. The SecOPs shall be prepared by the ADP System/Network Security Officer, in consultation with the ADP SOA, the ADP Authority and the SAA, who shall co-ordinate with other security elements concerned. The SAA shall approve the SecOPs before authorizing the storing, processing or transmitting of information classified NATO CONFIDENTIAL and above.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

242. The ADP SOA shall establish controls that shall ensure that master copies of all software (general-purpose operating systems, subsystems and software packages) in use are protected in conditions commensurate with the classification of the information which they are to process. Security protection of applications programs shall be determined on the basis of an assessment of the security classification of the program itself rather than of the classification of the information it is to process.

243. The software versions in use should be verified at regular intervals to ensure their integrity and correct functioning. New or modified versions of software should not be used for the processing of information classified NATO CONFIDENTIAL and above, until the security-relevant/security-enforcing features of the software have been tested and approved by the ADP System Security Officer, and, depending upon the re-accreditation conditions stated in the SSRS, approved by the responsible SAA. Software which provides new or altered systems capabilities, and which does not contain any security-relevant/security-enforcing features, should not be used until verified by the ADP SOA.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/ COMPUTER VIRUSES

244. Checking for the presence of malicious software/computer viruses shall be carried out in accordance with the requirements of the SAA.

245. New or modified versions of software (operating systems, subsystems, software packages and applications software), presented on computer storage media, and information-bearing floppy diskettes or other removable computer storage media arriving in an organization should be checked, in a stand-alone environment (whenever possible), for the presence of any malicious software or computer viruses, before being introduced to the ADP system or network. In addition, periodic checks should be made on installed software; these checks should be made more frequently if the ADP system or network is connected to another ADP system or network, or if connected to a public telephone/data transmission network.

MAINTENANCE

246. Contracts and procedures for scheduled and on-call maintenance of ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above, shall specify requirements and arrangements for maintenance personnel and their associated equipment entering an ADP area, and especially for maintenance personnel who may require access to NATO classified information in the course of their maintenance duties.

247. The requirements shall be clearly stated in the SSRS and the procedures shall be clearly stated in the SecOPs. Contractor maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under stringent security control, and only with the approval of the SAA.

PROCUREMENT

[*Note - paragraphs 248 to 251 shall apply only to NATO commands and agencies.*]

248. Procurement of ADP systems or networks should be limited, in so far as practicable, to ADP systems or networks designed and manufactured in a NATO member nation; hardware or software developed or manufactured in non-NATO member nations should be procured only after approval by the appropriate SAA.

249. For ADP systems and networks storing, processing or transmitting information classified NATO SECRET and above, and/or Special Category information, the ADP system/network or the baseline computer security products (for example, general purpose operating system products, security-relevant/security-enforcing limited functionality products and network products) to be procured should either have been evaluated and certified, or currently be under evaluation and certification, against the NATO criteria (AC/35-D/1012(revised) refers) or national equivalent, by an appropriate NATO/National Evaluation or Certification Authority/Agency.

250. For ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL, substantial consideration should be given to those products referred to in paragraph 249 above.

251. In deciding whether equipment, particularly computer storage media, should be leased rather than purchased, it should be borne in mind that such equipment, once used for storing or processing NATO classified information, cannot be released outside an appropriately secure environment without first being de-classified to the approval of the SAA and that such approval may not always be possible.

ACCREDITATION

252. All ADP systems and networks, prior to storing, processing or transmitting information classified NATO CONFIDENTIAL and above, shall be accredited, based upon information provided in the SSRS, SecOPs and any other relevant documentation, by the SAA. Sub-systems and remote terminals/ workstations shall be accredited as part of all the ADP systems or networks to which they are connected. Where an ADP system or network supports both NATO and national organizations, the NATO and National Security Authorities (NSAs) shall mutually agree on the accreditation.

EVALUATION AND CERTIFICATION

253. Prior to accreditation, in certain instances, the multi-level security mode of operation shall require the hardware, firmware and software security features of an ADP system or network to have been evaluated and certified, based on NATO criteria (or national criteria which have been approved by the national evaluation or certification authority), as being capable of safeguarding information of mixed classification and information category designation, and of discriminating between users on the basis of their authorised access to the system.

254. The requirements for evaluation and certification shall be included in system planning, and clearly stated in the SSRS, as soon as the security mode of operation has been established.

255. The instances where evaluation and certification shall be required, within the multi-level security mode of operation, are as follows :

(a) ADP systems or networks storing, processing or transmitting information classified COSMIC TOP SECRET, and/or Special Category information; and

(b) ADP systems and networks storing, processing or transmitting information classified NATO SECRET, where:

(i) the ADP system or network is interconnected with another ADP system or network (for example, under another ADPSOA); or

(ii) the ADP system or network has a potential user population which cannot be specifically defined, for example, where directly or indirectly connected to a public network.

256. The evaluation and certification processes shall be carried out in accordance with approved guidelines and by independent and impartial teams of technically qualified and appropriately cleared personnel acting on behalf of the appropriate SAA. The SAA shall be involved in the selection of the appropriate teams to carry out the evaluation and certification processes.

257. The teams may be provided from a Host nation evaluation or certification authority or its nominated representatives, for example, a competent and cleared contractor, or from the Communications and Information Systems Security and Evaluation Agency (SECAN).

258. The evaluation and certification processes shall establish the extent to which the design and implementation of a particular ADP system or network meets specified security requirements, as stated in the SSRS. Relevant sections of the SSRS may require to be updated following evaluation and certification. The evaluation and certification processes should commence at the ADP system or network specification stage and continue through the implementation stage.

259. The degree of the evaluation and certification processes involved may be lessened (for example, only involving integration aspects) where ADP systems or networks are based on existing nationally evaluated and certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

260. For all ADP systems and networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above, the ADP SOA shall establish control procedures which shall ensure that all ADP system or network changes are reviewed for their security implications.

261. The types of change that would give rise to re-accreditation, or that require the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure which could have affected the security features of the ADP system or network, the ADP SOA shall ensure that a check is made to ensure the correct operation of the security features. Continued accreditation of the ADP system or network shall normally depend on the satisfactory completion of the checks.

262. All ADP systems or networks storing, processing or transmitting information classified NATO CONFIDENTIAL and above shall be inspected or reviewed on a periodic basis by the SAA. In respect of ADP systems or networks storing, processing or transmitting COSMIC TOP SECRET or Special Category information, the inspections shall be carried out not less than once annually.

SECURITY OF MICROCOMPUTERS/PERSONAL COMPUTERS

263. Microcomputers/Personal Computers (PCs) with fixed hard discs (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices (for example, portable PCs and electronic "notebooks") with fixed hard discs, shall be considered as information storage media in the same sense as floppy discs or other removable computer storage media.

264. This equipment shall be afforded the level of protection, in terms of access, handling, storage and transportation, commensurate with the highest classification level of information ever stored or processed (until downgraded or declassified in accordance with approved procedures).

USE OF PRIVATELY-OWNED ADP EQUIPMENT FOR OFFICIAL NATO WORK

265. The use of privately-owned removable computer storage media, software and ADP hardware (for example, PCs and portable computing devices) with a storage capability shall be prohibited for storing, processing and transmitting information classified NATO CONFIDENTIAL and above. For NATO UNCLASSIFIED and NATO RESTRICTED information, the appropriate national, MNC or agency regulations shall apply.

266. Privately-owned hardware, software and media shall not be brought into any Class I or Class II area where NATO classified information is stored, processed or transmitted without the permission of the head of the organiszation.

USE OF CONTRACTOR-OWNED OR NATIONALLY-SUPPLIED ADP EQUIPMENT FOR OFFICIAL NATO WORK

267. The use of contractor-owned ADP equipment and software in organizations in support of official NATO work may be permitted by the Head of an organisation. The use of nationally-provided ADP equipment and software by employees in a NATO command or agency may also be permitted; in this case, the ADP equipment shall be brought under the control of the appropriate organization's inventory. In either case, if the ADP equipment is to be used for storing, processing or transmitting NATO classified information, then the appropriate SAA

shall be consulted in order that the elements of ADP security that are applicable to the use of that equipment are properly considered and implemented.

INFORMATION CATEGORY DESIGNATIONS

268. Information Category Designations currently apply to ATOMAL, US-SIOP-ESI, Crypto, information designated EXCLUSIVE FOR, or any other NATO-recognised special handling designators, as these designations require limited distribution and special handling in addition to that designated by the security classification.

DEFINITIONS

269. The definitions provided in the subsequent paragraphs are the preferred NATO definitions, and may, in some cases, differ from national definitions.

SECURITY MODES OF OPERATION

DEDICATED

270. A mode of operation in which ALL individuals with access to the ADP system or network are cleared to the highest classification level of information stored, processed or transmitted within the ADP system or network, and with a common need-to-know for ALL of the information stored, processed or transmitted within the ADP system or network.

Notes :

(1) The common need-to-know indicates there is no mandatory requirement for computer security features to provide separation of information within the ADP system or network; and

(2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information stored, processed or transmitted within the ADP system or network.

SYSTEM HIGH

271. A mode of operation in which ALL individuals with access to the ADP system or network are cleared to the highest classification level of information stored, processed or transmitted within the ADP system or network, but NOT ALL individuals with access to the ADP system or network have a common need-to-know for the information stored, processed or transmitted within the ADP system or network.

Notes :

(1) The lack of common need-to-know indicates that there is a requirement for computer security features to provide selective access to, and separation of, information within the ADP system or network;

(2) Other security features (for example, physical, personnel and procedural) shall conform to the requirements for the highest classification level and all category designations of the information stored, processed or transmitted within the ADP system or network; and

(3) All information stored, processed or being available to an ADP system or network under this mode of operation, together with any output generated, will be protected as potentially of the information category designation and of the highest classification level being

stored, processed or transmitted until determined otherwise, unless there is an acceptable level of trust that can be placed in any labelling functionality present.

MULTI-LEVEL

272. A mode of operation in which NOT ALL individuals with access to the ADP system or network are cleared to the highest classification level of information stored, processed or transmitted within the ADP system or network, and NOT ALL individuals with access to the ADP system or network have a common need-to-know for the information stored, processed or transmitted within the ADP system or network.

Notes :

(1) This mode of operation permits, concurrently, the storing, processing or transmitting of information of different classification levels and of mixed information category designations; and

(2) The lack of all individuals being cleared to the highest level, associated with a lack of common need-to-know, indicates that there is a requirement for computer security features to provide selective access to, and separation of, information within the ADP system or network.

ADP SECURITY

273. The application of security measures to ADP systems or networks, in order to protect against, or prevent, exploitation, modification (including destruction) or denial of service through interception, unauthorised electronic access, or related technical intelligence threat.

Note :

Such measures include computer and communications security, and also procedural, physical, personnel and document security.

COMPUTER SECURITY (COMPUSEC)

274. The application of hardware, firmware and software security features to a computer system in order to protect against, or prevent, the unauthorised disclosure, manipulation, modification/deletion of information or denial of service.

COMPUTER SECURITY PRODUCT

275. A generic computer security item which is intended for incorporation into an ADP system for use in enhancing, or providing for, confidentiality, integrity or availability of information stored, processed or transmitted.

COMMUNICATIONS SECURITY (COMSEC)

276. The application of security measures to telecommunications in order to deny unauthorised persons information of value which might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

Note :

Such measures include crypto, transmission and emission security; and also include procedural, physical, personnel, document and computer security.

EVALUATION

277. The detailed technical examination, by an appropriate authority, of the security aspects of an ADP system or network, or computer security product.

Notes :

(1) The evaluation investigates the presence of required security functionality, the absence of compromising side-effects from such functionality and assesses the incorruptibility of such functionality; and

(2) The evaluation determines the extent to which the security requirements of an ADP system or network, or the security claims of a computer security product, are satisfied and establishes the assurance level of the ADP system or network, or the computer security product's trusted function.

CERTIFICATION

278. The issue of a formal statement, supported by an independent review of the conduct and results of an evaluation, of the extent to which an ADP system or network meets the security requirement, or a computer security product meets pre-defined security claims.

ACCREDITATION

279. The authorisation and approval granted to an ADP system or network to process NATO classified information in its operational environment.

Note :

Such accreditation should be made after all appropriate security procedures have been implemented and a sufficient level of protection of the system resources has been achieved. Accreditation should normally be made on the basis of the SSRS, including the following :

(a) a statement of the objective of accreditation for the system; in particular, what classification level(s) of information is/are to be handled and what system or network security mode(s) of operation is/are being proposed;

(b) production of a risk management review to identify the threats and vulnerabilities and measures to counter them;

(c) a detailed description of the proposed operations (e.g., modes, services, to be provided), including a description of the ADP system and ADP network security features which shall form the basis of accreditation;

(d) the plan for the implementation and maintenance of the security features;

(e) the plan for initial and follow-on system security or network security test, evaluation and certification; and

(f) certification, where required, together with other elements of accreditation.

ADP SYSTEM

280. Assembly of equipment, methods and procedures, and if necessary, personnel, organized to accomplish information processing functions.

Notes :

(1) This is taken to mean an assembly of facilities, configured for storing, processing and transmitting information within the system;

(2) Such systems may be in support of consultation, command, control, communications, scientific or administrative applications including word processing;

(3) The boundaries of a system will generally be determined as being the elements under the control of a single ADP SOA; and.

(4) An ADP system may contain subsystems, some of which are themselves ADP systems.

ADP SYSTEM SECURITY FEATURES

281. The ADP system security features comprise all hardware/firmware/software functions, characteristics, and features; operating procedures, accountability procedures, and access controls, the ADP area, remote terminal/workstation area, and, the management constraints, physical structure and devices, personnel and communications controls needed to provide an acceptable level of protection for classified information to be stored or processed in an ADP system.

ADP NETWORK

282. Organization, geographically disseminated, of ADP systems interconnected to exchange data, and comprising the components of the interconnected ADP systems and their interface with the supporting data or communications networks.

Notes :

(1) An ADP network can use the services of one or several communications networks; several ADP networks can use the services of one common communications network; and

(2) An ADP network is called "local" if it links several computers together in the same site.

ADP NETWORK SECURITY FEATURES

283. The ADP network security features include the ADP system security features of individual ADP systems comprising the network together with those additional components and features associated with the network as such (for example, network communications, security identification and labelling mechanisms and procedures, access controls, programs and audit trails) needed to provide an acceptable level of protection for classified information.

ADP AREA

284. An area which contains one or more computers, their local peripheral and storage units, control units and dedicated network and communications equipment.
Note :

This does not include a separate area in which remote peripheral devices or terminals/ workstations are located even though those devices are connected to equipment in the ADP area.

REMOTE TERMINAL / WORKSTATION AREA

285. An area containing some computer equipment, its local peripheral devices or terminals/ workstations and any associated communications equipment, separate from an ADP area.

ANNEX I

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO INTERNATIONAL ORGANIZATIONS OUTSIDE THE NORTH ATLANTIC TREATY ORGANIZATION (NATO) COMPOSED ONLY OF SOME OR ALL NATO NATIONS

1. Any member nation or NATO command or agency considering it would be advantageous to NATO to release to an international organization, outside the North Atlantic Treaty Organization (NATO), composed only of some or all NATO member nations NATO classified information up to and including COSMIC TOP SECRET but excluding that orginated by one or more of the nations participating in a NATO Production and Logistics Organization (NPLO) or other organization granted a charter under the terms of C-M(62)18 or generated within such an organization and pertaining to it - see paragraph 3 below - will submit an application for its release to the NATO Military Committee or NATO civil committee most concerned with the information *(1)*.

2. The authority to release such NATO classified information will rest exclusively with either the Council or the relevant committee. In the case of information referred to a NATO civil committee, that committee will authorize its release, provided it is unanimous that the information may be released and provided the information is not classified higher than NATO CONFIDENTIAL. If the information is classified COSMIC TOP SECRET or NATO SECRET, the NATO civil committee, having agreed that the information should be released, will seek the approval of Council, for its dissemination. Normally, such approval will be sought case-by-case but where there is a need to release a certain type of information on a continuing basis, Council may authorize the NATO civil committee to act on its behalf. (If the originator of the information, for which release is desired, is not a member of the relevant committee, that committee must first seek the originator's consent to the release, if the originator or originators cannot be established the relevant committee will assume the responsibility of the originator.)

3. In the case of NATO classified information originated by one or more of the nations participating in an NPLO or other organization granted a charter under the terms of C-M(62)18 or generated within that organization and pertaining to it, the application for release - see paragraph 1 above - will be submitted to the Board of Directors (or to any other body designated by higher authority) of the NATO organization concerned. Provided it unanimously agrees that the information should be released, the Board of Directors (or any other body designated by higher authority) will seek the approval of the national security authorities of the nations participating in the NATO organization programme for its dissemination. If approval is given, the information will be passed in accordance with the procedures referred to in paragraph 4 below. The NATO organization concerned will maintain records of all NATO classified information passed under these procedures, together with the written confirmation mentioned in paragraph 4 below. These records will be subject to examination by the NATO Office of Security (NOS) during their annual inspections.

(1) For ease of reference, hereafter in this Annex the term "relevant committee" will be used in lieu of the expression "as appropriate, either to the NATO Military Committee or to the NATO civil committee most concerned with the information".

4. When approval for release has been given and before any NATO classified information is passed to such an international organization, that organization will confirm, in writing, to the security authority of the member nation or NATO command or agency or NPLO (or other) Management Agency making the release, with a copy to the NOS, that the relevant paragraphs of the Security Regulations set out in the attached Appendix will be implemented at all times. Normally, this written confirmation will be required only before NATO classified information is passed to the international organization for the first time. Subsequent confirmation may be required as a result of an inspection by the NOS.

APPENDIX to ANNEX I

SECURITY REGULATIONS TO ENSURE THE PROTECTION OF NATO CLASSIFIED INFORMATION PASSED BY THE NATO TO AN INTERNATIONAL ORGANIZATION COMPOSED ONLY OF SOME OR ALL NATO NATIONS

PERSONNEL

1. The number of officials of the international organizations who will have access to NATO classified information must be strictly confined to those whose duties make such access essential according to the need-to-know principle. It will be the responsibility of the NATO Military Committee or the NATO civil committee most concerned with the information to be passed, or of the Board of Directors (or of any other body designated by higher authority) in respect of information pertaining to NATO Production and Logistics Organizations (NPLO) and other organizations governed by the terms of C-M(62)18, to obtain assurances from the recipient organization that the individuals of that organization who will be given access to the NATO information, hold NATO security clearances, at the appropriate level, issued by their parent governments and that the number of such individuals is kept as low as possible consistent with the efficient use of the information.

2. Security clearance certificates for the individuals concerned must be provided to the NATO Protective Security Branch (PRB), or to the security authority of the NPLO or other organization concerned before such individuals can have access to NATO classified information.

DOCUMENTS

3. The selection of NATO documents to be transmitted to the international organization rests exclusively with the NATO Military Committee or the NATO civil committee or the Board of Directors (or any other body designated by higher authority), as appropriate, referred to in paragraph 1 above.

Despatching

4. NATO documents selected in accordance with paragraph 3 above will be forwarded to the international organization through approved channels as laid down in Section VII of Enclosure "C".

Packaging

5. The double cover system will be used. The inner cover will be marked "NATO", together with the security classification. A receipt form will be enclosed for each NATO classified document. The receipt form, which requires no security classification, should quote only the reference number, date, copy number and language of the document and not its title.

6. The inner cover will be enclosed in an outer cover which will bear a package number for receipting purposes. Under no circumstances will any security classification appear on the outer envelope.

7. Messengers will always obtain receipts against package numbers.

Registration on Arrival

8. As soon as a NATO classified document is received, it will be listed in a special register, held by the organization, the pages of which will bear columns indicating the date received, the

date of the document, its serial number, its copy number, its security classification, its title, the date when the receipt is returned and the date the document, when no longer required, is sent back to NATO.

Custody and Security Protection

9. When not in use, documents will be stored in a security container which is approved for the storage of national documents of the same classification as the NATO document. Such containers will bear no indication of their contents, which will be accessible only to those authorized to have access to NATO classified information. In the case of combination locks, the combination will be known only to the officials of the international organization authorized access to NATO classified information and will be changed every six months, or sooner in case of transfer of an authorized official, or when compromise is suspected.

10. NATO classified documents may only be removed from the security container in which they are housed, by members of the international organization who are authorized to have access to the documents. The person removing a document from the security container will be responsible for ensuring its safe custody at all times until it is replaced it in the container. In particular, he must ensure that no one, who is not authorized to see the document, has access to it.

11. No copies or extracts of NATO classified documents will be made.

12. Plans for the destruction in an emergency of NATO classified documents should be prepared.

Breaches of Security

13. When a breach of security involving a NATO classified document occurs or is suspected, the following action should be taken immediately:
    (a) discover the circumstances of the breach of security;
    (b) notify the NOS;
    (c) minimize the damage done;
    (d) devise measures to prevent recurrence;
    (e) implement any recommendations made by the NOS to prevent a recurrence.

PHYSICAL

14. When not in use, any security container used for the storage of NATO classified documents will at all times be kept securely locked.

15. When maintenance personnel or cleaners are required to enter or remain in the room in which the security container is located, they must at all times be escorted by a member of the international organization's security section.

16. Outside office hours (at night, week-ends and holidays) protection of the security container will be provided either by a watchman or by an automatic alarm system.

INSPECTIONS

17. The NOS will be permitted to carry out inspections of the security measures in force to protect NATO classified information within the international organization.

REPORTS

18. So long as the international organization holds NATO classified information it will submit an annual report, to reach the NOS by 31st January each year, to confirm the above security regulations are being implemented.

ANNEX II

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO AND THE EXCHANGE OF CLASSIFIED INFORMATION WITH NON-NATO NATIONS AND INTERNATIONAL ORGANIZATIONS INCLUDING SUCH NATIONS

GENERAL

1. Classified information entrusted to or generated by NATO in order to enable it to perform its rôle is an asset which is disseminated and protected in accordance with agreed NATO security policy and procedures. This Annex and its Appendices set out the policy and procedures required for the release of NATO classified information to, and the exchange of classified information with, non-NATO nations and international organizations including such nations (hereinafter referred to as non-NATO recipients). These arrangements cover information classified up to and including NATO SECRET contained in documents issued by the NAC, or by any other NATO committee, command or agency (hereinafter referred to as NATO bodies). Appendix 2 sets out additional provisions pertaining to the release of information by a NPLO classified up to and including NATO SECRET originated by and belonging to one or more of the nations participating in the NPLO.

2. The release of NATO classified information to non-NATO recipients will follow the procedures outlined in Appendix 1 (these may differ for NPLOs - see Appendix 2). The release of NATO classified information to, and the exchange of classified information with, non-NATO recipients will take place in the context of cooperative activities approved by the NAC. Any request for the release of NATO classified information to non-NATO recipients outside such cooperative activities will be examined and approved on a case-by-case basis.

PRINCIPLES FOR AUTHORIZING THE RELEASE OF NATO CLASSIFIED INFORMATION

3. Authorization to release will always be subject to the consent of the originator(s). The decision to release will be based on the following principles :

   (a) for NATO classified information to be released under cooperative activities approved by the NAC:

      (i) the subject matter must be included in the general work plan for the activity or in the practical measures established for cooperation;

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - October 97

(ii) the release of NATO classified information must be required for initiating cooperation on a specific subject or for the continuance and further development of cooperation within the approved activity;

(iii) a security agreement, signed by the Secretary General on behalf of NATO and by a representative duly-mandated by the non-NATO recipient, must have been concluded;

(b) for NATO classified information to be released on special request from either NATO member nations or NATO bodies (the Sponsor) to non-NATO recipients outside NAC-approved cooperative activities:

(i) the Sponsor shall be responsible for obtaining a written assurance to NATO from the non-NATO recipient that any information received will be appropriately protected;

(ii) the Sponsor must forward this written assurance to the relevant committee, together with the release request;

(iii) the request must demonstrate the advantage which would accrue to NATO.

RELEASE AUTHORITY[1]

4. The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated:

(a) to the relevant committee for information classified up to and including CONFIDENTIAL;

(b) to the NAMILCOM for information classified up to and including SECRET which has been originated by the NAMILCOM and bodies subordinate to it;

(c) to the NPLO, for NATO classified information originated by and belonging to one or more of the nations participating in the NPLO.

Authority for release will only be delegated to a committee on which the originator(s) is/are represented. If the originator(s) or originators cannot be established, the relevant committee will assume the responsibility of the originator. Authority for release should be delegated to the lowest committee level best suited to evaluate the importance of the classified information.

MINIMUM STANDARDS FOR THE HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION RELEASED TO AND OF CLASSIFIED INFORMATION EXCHANGED WITH NON-NATO RECIPIENTS

5. Appendix 3 contains the minimum standards required for the handling and protection of NATO classified information released to, and of classified information exchanged with, non-NATO recipients. This document will be furnished to all non-NATO recipients with whom NATO concludes a security agreement in the context of cooperative activities approved by the NAC.

[1] Throughout this Annex and its Appendices, the NAC, delegated committee or NPLO will be referred to as the "Release Authority".

ADMINISTRATIVE ARRANGEMENTS FOR THE IMPLEMENTATION OF THE SECURITY AGREEMENT

6. Appendix 4 contains the administrative arrangements necessary for the implementation of the security agreement. The completion of the administrative arrangements will be confirmed by a security survey carried out by the NOS of the relevant agencies of the non-NATO recipient.

7. The security survey will establish the ability of the non-NATO recipient to comply with the provisions of the security agreement and with the minimum standards contained in Appendix 3. The NOS will produce a report of the survey and transmit a copy to the Security Authority of the non-NATO recipient. The original report will be filed in the NOS. The conclusion drawn from the survey as to the ability of the non-NATO recipient to protect NATO classified information will be communicated by the NOS to the relevant NATO bodies and, if requested, to NATO member nations.

CLASSIFICATION SYSTEM

8. Details are contained in Appendix 1.

APPENDIX 1 to ANNEX II

PROCEDURES FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO RECIPIENTS

REQUESTS FOR RELEASE

1. Release authorization will be based on the principles stated in paragraph 3 of Annex II to this document.

2. Requests for release will be sent to the relevant addressee as follows:

   (a) the Executive Secretary, NATO International Staff, for NATO classified information issued by the NAC and bodies subordinate to it;

   (b) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and bodies subordinate to it;

   (c) the Head of an NPLO.

3. Requests for release will include the following information :

   (a) for cooperative activities approved by the NAC:

      (i) reference to the relevant subject in the overall work plan for the cooperative activity;

      (ii) purpose and justification for the release (initiating cooperation, progress in cooperation, exercise, etc);

      (iii) identification of document(s) containing the NATO classified information (reference number, date and NATO classification);

      (iv) description of the NATO classified information which should be released (the whole document(s), part of the document or excerpt from the document);

      (v) if appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents, etc., stating maximum classification and any other limitations regarding the possible future release).

   (b) for release outside cooperative activities approved by the NAC, the document containing the NATO classified information must be identified and the information requested in (a)(ii),(iii) and (iv) above must be given.

ACTIONS UPON THE RECEIPT OF A RELEASE REQUEST

4. Addressees receiving a request for release of NATO classified information will determine that:

   (a) the justification given in the release request is adequate;

   (b) the NATO classified information concerned is properly identified and described;

   (c) in the case of cooperative activities approved by the NAC, a security agreement has been concluded between NATO and the non-NATO recipient and that the required security survey has been carried out by the NOS with a positive result;.

   (d) in the case of a request for release outside cooperative activities, the non-NATO recipient has provided, through its Sponsor, a written assurance to NATO that it will provide appropriate protection to any information released; and

   (e) the request is sent to the appropriate committee for a decision.

5. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g. a military document prepared by NAMILCOM and approved by the Defence Planning Committee (DPC) and issued under the latter's reference), it is the responsibility of the initial addressee to coordinate the response to the request.

ACTIONS BY THE RELEASE AUTHORITY

6. Based on the information contained in the request, the Release Authority will approve or disapprove the release.

7. National members of the Release Authority are responsible for obtaining any clearance which may be required from national authorities.

8. Approval, whether obtained in committee or under the silence procedure, will be recorded in writing.

9. The Release Authority may approve generic release of NATO classified information issued under its authority. Such approval must state the specific subject areas or series of documents of the NATO classified information and the level of classification authorized for release and may stipulate any other limitations regarding possible future release.

10. Should a request for release of NATO classified information not be approved by a delegated Release Authority, the request, together with the latter's reason for not approving it, may be presented to the next level and ultimately to the NAC for final decision. This action will only be taken in cases when sought by the requesting NATO member nation(s) or NATO body or when the delegated Release Authority decides that such action is appropriate.

CLASSIFICATION SYSTEM

11. The classifications are as follows : RESTRICTED, CONFIDENTIAL and SECRET. Classification will be used to indicate the sensitivity of the classified information and thus the security measures and procedures which will apply for its protection. It is the prerogative of the originator of the information to classify and to downgrade or declassify it.

12. The following procedures will be used for marking classified information:

(a) classified information originating from NATO which is released to non-NATO recipients will retain its NATO classification. In addition, the cover or first page of any document released will be marked with the name of the Release Authority, the date the release decision was taken and any related terms or conditions;

(b) (i) where classified information is generated within a cooperative activity approved by the NAC, the classification shall be preceded by NATO and either by the designation of the activity or by the name(s) of the international organization(s) or participating nation(s) :

NATO and NAME OF ACTIVITY or
NAME OF NATION(S) or
INTERNATIONAL ORGANIZATION(S) CONFIDENTIAL

Examples :

NATO/EAPC/PfP RESTRICTED

NATO/RUSSIA CONFIDENTIAL

NATO/OSCE RESTRICTED

(ii) If, in addition, an originator deems it necessary to limit the distribution of classified information, a marking showing the parties allowed access will be added below the line as, for example

NATO and NAME OF ACTIVITY or
NAME OF NATION(S) or
INTERNATIONAL ORGANIZATION(S) CONFIDENTIAL
NAME OF NATION(S) or EXERCISE ..... ONLY

N.B. : Exercise name used here rather than spelling out names of all participants.

Examples :

NATO/PfP CONFIDENTIAL
HUNGARY/POLAND ONLY

NATO/PfP RESTRICTED
EXERCISE COPPERPLATE ONLY

TRANSFER OF NATO CLASSIFIED INFORMATION AUTHORIZED FOR RELEASE

13. All NATO classified information released to non-NATO recipients will be forwarded under appropriate cover. All transfers will be effected through a NATO registry to the registry of the non-NATO recipient participating in a cooperative activity approved by the NAC. Transfer to non-NATO recipients not participating in cooperative activities will be by agreed official channels.

14. NATO bodies will keep complete, separate records of all NATO classified information which they have released to non-NATO recipients and will send details of the reference number, title and release date to the NATO Central Registry, Brussels. On request, national authorities can obtain details through the NATO Central Registry, Brussels.

APPENDIX 2 to ANNEX II

NATO PRODUCTION AND LOGISTICS ORGANIZATIONS (NPLOs)

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION BELONGING TO AN NPLO OR OTHER ORGANIZATION GRANTED A CHARTER UNDER THE TERMS OF C-M(62)18

1. NATO classified information originated by one or more of the nations participating in an NPLO or other organization granted a charter under the terms of C-M(62)18, or generated within such an organization and pertaining to it, may be the subject of an application for release to a non-NATO recipient by any member nation, or NATO body considering that it would be advantageous to NATO.

2. The application will be submitted to the Head of the NATO organization concerned, who will pass it on to the Board of Directors for a decision. It must specify the document(s) or the class of information to be released, the proposed recipient's need for access to the information, and the purpose for which it will be used.

3. Provided that the Board unanimously agrees that the NATO classified information should be released, it will ask the NSA of the nations participating in the NATO organization's programme to satisfy themselves that adequate security arrangements for the protection of the NATO classified information intended to be released exist or are created.

4. Such arrangements will include a security agreement approved by the nations participating in the NPLO and, on behalf of the intended recipient(s), by an authority competent to commit them to undertake to give the NATO classified information released at least that measure of security protection already afforded to it within NATO. A summary of the relevant provisions is set out in Appendix 3, which may be provided to the intended recipient(s). NSAs will also take whatever steps they consider appropriate to ensure that the intended recipient(s) are competent to comply with the provisions of this security agreement.

5. Release will be administered by the Board of Directors of the NATO organization concerned. Records will be kept of all NATO classified information passed under these procedures. These records will be subject to examination by the NOS during its periodic inspections of the organization.

APPENDIX 3 TO ANNEX II

MINIMUM STANDARDS FOR THE HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION RELEASED TO AND CLASSIFIED INFORMATION EXCHANGED WITH NON-NATO RECIPIENTS

GENERAL

1. All NATO classified information which is released to another party is for official use only. It will, therefore, only be disseminated to bodies and individuals with a need-to-know. The minimum standards provided in this document will apply to all NATO classified information released to non-NATO recipients and will also be applied to all classified information exchanged within the context of cooperative activities approved by the NAC.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

2. Before an individual is granted access to information classified CONFIDENTIAL or SECRET, he/she will be subject to a security clearance procedure designed to determine whether he/she is loyal and trustworthy. When the result of such a procedure is positive, a Security Clearance Certificate will be issued for the individual by his/her Security Authority.

3. Before an individual is authorised access to classified information, he/she will be briefed on the security regulations relevant to the classification of the information released and the legal and disciplinary consequences of breaches of these regulations.

4. When an individual who has been security cleared is designated as a representative of his/her organization to a meeting in which classified information is involved or the venue for the meeting is within a secure area, his/her Security Authority, when requested, will send a Certificate of Security Clearance to the organization convening the meeting. The requirements for escorting individuals who do not hold a NATO security clearance remain valid if the meeting takes place in NATO secure areas.

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

5. A registry system will be established by the recipient for the receipt, despatch, control and storage of classified information. Sub-registries may be established as necessary. The registry (or sub-registry) will be responsible for :

   (a) the recording of the receipt and despatch of all classified information;

   (b) the distribution and control of classified information within the nation/organization served;

   (c) the storage of the classified information; and

(d) the final disposal of the classified information, including the maintenance of:

(i) destruction certificates for all information classified SECRET;

(ii) log books or document registers for information classified RESTRICTED or CONFIDENTIAL.

CLASSIFICATION SYSTEM

6. The classifications are as follows : RESTRICTED, CONFIDENTIAL and SECRET. Classification will be used to indicate the sensitivity of the classified information and thus the security procedures and measures which will apply for its protection. It is the prerogative of the originator of the information to classify and to downgrade or declassify when appropriate.

7. The following procedures will be used for marking classified information:

(a) classified information originating from NATO which is released to non-NATO recipients will retain its NATO classification. In addition, the cover or first page of any document released will be marked with the name of the Release Authority, the date the release decision was taken and any related terms or conditions;

(b) (i) where classified information is generated within a cooperative activity approved by the NAC, the classification shall be preceded by NATO and either by the designation of the activity or by the name(s) of the international organization(s) or participating nation(s) :

NATO and NAME OF ACTIVITY or CONFIDENTIAL
NAME OF NATION(S) or
INTERNATIONAL ORGANIZATION(S)

Examples :

NATO/EAPC/PfP RESTRICTED

NATO/RUSSIA CONFIDENTIAL

NATO/OSCE RESTRICTED

(ii) If, in addition, an originator deems it necessary to limit the distribution of classified information, a marking showing the parties allowed access will be added below the line as, for example:

NATO and NAME OF ACTIVITY or CONFIDENTIAL
NAME OF NATION(S) or
INTERNATIONAL ORGANIZATION(S)
NAME OF NATION(S) or EXERCISE ..... ONLY

N.B. : Exercise name used here rather than spelling out names of all participants.

Examples :

NATO/PfP CONFIDENTIAL
HUNGARY/POLAND ONLY

NATO/PfP RESTRICTED
EXERCISE COPPERPLATE ONLY

REQUIREMENTS FOR THE HANDLING, STORAGE, AND TRANSMISSION OF NATO CLASSIFIED INFORMATION

8. These are as follows :

(a) NATO RESTRICTED information shall be handled and stored (in locked containers) in areas that are not accessible to unauthorized personnel. Documents may be sent through postal channels by such means as are authorized by the appropriate NSA. Cryptographic systems approved by a NATO member nation or by the NAMilCom shall be used for the encryption of NATO RESTRICTED infor-mation transmitted by electrical means. In exceptional circumstances, when speed is of paramount importance and means of encryption are not available, information classified NATO RESTRICTED may be transmitted electrically in clear text over public systems. Reproductions and translations of documents classified NATO RESTRICTED may be produced by the addressee under strict observation of the need-to-know principle;

(b) NATO CONFIDENTIAL information will be handled and stored in areas to which access is strictly controlled. Access will be restricted to designated personnel who have been appropriately cleared and have an established need for access for official purposes. Documents will be stored in containers with nationally-approved locks, the keys or combinations to which will be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Cryptographic systems approved by a NATO member nation or by the NAMILCOM will be used for the encryption of NATO CONFIDENTIAL information transmitted by electrical means. Reproductions and translations of documents classified NATO CONFIDENTIAL may be produced by the addressee under strict observation of the need-to-know principle;

(c) NATO SECRET information will be handled and stored in areas to which access is strictly controlled. Access will be limited to designated, appropriately cleared personnel with an established need for access for official purposes. NATO SECRET documents will be stored in security containers with nationally-approved locks, the keys or combinations to which will be held only by designated security cleared personnel needing access to the stored information to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag. Only cryptographic systems specifically authorized by the NAMILCOM will be used for the encryption of information, however transmitted (e.g. voice, data or telegraph), which is classified NATO SECRET. Reproductions and translations of documents classified NATO SECRET may be produced by the addressee under strict observation of the need-to-know principle. Copies of documents classified NATO SECRET must be marked with identifying copy numbers. The number of reproductions and/or translations of NATO SECRET documents and their copy numbers must be recorded by the registry (or sub-registry).

ADP SECURITY

9. To achieve adequate security protection of an ADP system or network, the appropriate standards of conventional security shall be specified, along with appropriate special security procedures and techniques particularly designed for each ADP system or network.

10. A balanced set of security measures (physical, personnel, procedural, computer and communication) shall be identified and implemented to create a secure environment in which an ADP system or network operates.

11. Computer security measures (hardware and software security features) shall be required to implement the need-to-know principle, and to prevent or detect the unauthorized disclosure of information. The extent to which computer security measures are to be relied upon shall be determined during the process of establishing the security requirement and the ability of such measures to provide the required level of security will be verified.

12. The integration of an ADP system and a communications system shall also require that the communications security aspects be assessed as part of the overall security.

BREACHES OR COMPROMISES OF SECURITY

13. Whenever a breach/compromise of security affecting classified information is discovered:

(a) a report giving details of the breach/compromise must be sent immediately to the NOS and to the Release Authority who will inform the originator(s) as required.

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, will be taken.

INSPECTIONS

14. A non-NATO participant in a cooperative activity approved by the NAC who is in receipt of classified information will facilitate periodic inspections by the NOS to ensure that the security environment is adequate for the retention of classified information.

APPENDIX 4 TO ANNEX II

ADMINISTRATIVE ARRANGEMENTS FOR THE IMPLEMENTATION OF THE SECURITY AGREEMENT BETWEEN NATO AND NON-NATO RECIPIENTS PARTICIPATING IN COOPERATIVE ACTIVITIES APPROVED BY THE NORTH ATLANTIC COUNCIL

1. Non-NATO recipients participating in these cooperative activities will appoint a Security Authority to be responsible for the implementation of security arrangements and procedures under the security agreement and will identify this Authority to the NOS which is the equivalent Security Authority for NATO. The NOS will establish liaison with the Security Authority of the non-NATO recipient to facilitate implementation of these security arrangements and procedures.

2. In accordance with the provisions contained in the security agreement, the NOS and the Security Authority of a non-NATO recipient must establish to their satisfaction that the recipient party will protect the classified information it receives as required by the originator.

3. Based on the minimum standards referred to previously which are derived from C-M(55)15(Final), the administrative arrangements will cover, as required, the establishment of:

   (a) a Security Authority which will implement and oversee the security measures for the protection of classified information released and classified information exchanged in the cooperative activity;

   (b) a registry system, including sub-registries, if required, by the non-NATO recipient;

   (c) procedures for the recording, control and destruction of classified information;

   (d) standards of security containers used for the storage of classified information;

   (e) channels of transmission;

   (f) personnel security clearance procedures; and

   (g) a system and procedures for the investigation of breaches of security.

4. After signature of the security agreement and the completion of the administrative arrangements described in paragraph 3 above, and before the exchange of classified information begins, the NOS will, and non-NATO recipients may, carry out a survey of the preparations made by an intended non-NATO recipient or NATO respectively for the handling and storage of the classified information to be exchanged. A copy of the NOS survey report will be provided to the intended non-NATO recipient.

5. NATO and non-NATO recipients will exchange details of the addresses to be used for the distribution of classified information, together with details of courier or messenger services for the transmission of classified information.

ANNEX III

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO THE WESTERN EUROPEAN UNION (WEU)

GENERAL

1. The release and exchange of information classified RESTRICTED and above between NATO and WEU is regulated by the Security Agreement between the Parties. This Annex and its Appendices set out the policy, procedures and regulations required for the release of NATO classified information to WEU.

ELIGIBILITY FOR RECEIPT BY WEU OF NATO CLASSIFIED INFORMATION

2. NATO members in WEU are eligible to receive information classified up to and including COSMIC TOP SECRET, via WEU. Non-NATO members in WEU must have completed all security formalities and signed a security agreement with WEU to be eligible to receive information classified up to and including NATO SECRET.

RELEASE AUTHORITY

3. The North Atlantic Council (NAC) is the ultimate authority for the release of NATO classified information to WEU. Except for information classified up to and including COSMIC TOP SECRET which has been originated by the NATO Military Committee (NAMILCOM) (see paragraph 4(b) below), the release of information classified COSMIC TOP SECRET will always rest with the NAC. A committee may agree on the advantage of disseminating such information to WEU, however, seeking the NAC's approval for its release.

4. The NAC has delegated release authority to:

   (a) the relevant committee for information classified up to and including NATO CONFIDENTIAL;

   (b) the NAMILCOM for information classified up to and including COSMIC TOP SECRET which has been originated by the NAMILCOM and bodies subordinate to it;

   (c) the Board of Directors of a NATO Production and Logistics Organization (NPLO), for information classified up to and including NATO SECRET originated by and belonging to one or more of the states participating in the NPLO.

5. Authority for release will only be delegated to a committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the relevant committee will assume the responsibility of the originator(s).

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - Jan 99

RELEASE PROCEDURES

6. Appendix 1 establishes the procedures for the release of NATO classified information to WEU.

SECURITY REGULATIONS

7. Appendix 2 establishes security regulations for the handling and protection of NATO classified information released to WEU.

REQUESTS FROM NATO FOR RELEASE OF WEU CLASSIFIED INFORMATION

8. Appendix 3 contains a request form, a copy of which should be completed and sent to the Secretary General, WEU by agreed channels.

APPENDIX 1 to ANNEX III

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO WEU

REQUESTS FOR RELEASE

1. Requests from WEU for release of NATO classified information (stating their requirement and giving details of intended recipients) will be sent to the relevant addressee as follows:

   (a) the Executive Secretary, NATO International Staff, for NATO classified information issued by the NAC and bodies subordinate to it;

   (b) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and bodies subordinate to it;

   (c) the Head of an NPLO for classified information originated by and belonging to one or more of the states participating in that NPLO.

ACTIONS UPON THE RECEIPT OF A RELEASE REQUEST

2. The addressee will task relevant NATO staffs to prepare required documents for the appropriate committee (or, in the case of an NPLO, for the Board of Directors or any other body designated to authorize release) for a decision on release. These documents will contain the following information:

   (a) identity of state(s) eligible for receipt under the terms of the request;

   (b) in the case of release requests to non-NATO member states of WEU, written confirmation that WEU has completed security formalities and has signed a security agreement with those non-NATO member states: this will be provided through the NATO Office of Security (NOS);

   (c) identification of document(s) containing the NATO classified information (reference number, date and NATO security classification);

   (d) description of the NATO classified information which could be released (the whole document(s), part of the document(s) or excerpt from the document(s)).

REQUESTS FOR GENERIC RELEASE

3. Requests for generic release will also include, as appropriate, details of specific subject areas, defined series of documents, anticipated future documents or series of documents

and anticipated requirements for internal release, etc., stating maximum classification. Upon approval, the appropriate committee (or Board of Directors) will state any other limitations regarding future release.

PROCESSING RELEASE REQUESTS

4. The request will be sent to the appropriate committee (or Board of Directors) for a decision, which will entail obtaining the approval of the originator(s). National members of the relevant committee are responsible for obtaining any clearance which may be required from their national authorities. The Board of Directors of an NPLO, having agreed on the release of classified information originated by and belonging to one or more of the states participating in the NPLO, will then seek the approval of the national security authorities of the nations participating in the NPLO for its dissemination.

5. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g. a military document prepared by NAMILCOM and approved by Defence Planning Committee (DPC) and issued under the latter's reference), it is the responsibility of the initial addressee to coordinate the response to the request.

CLASSIFICATION MARKINGS

6. Classified information originating from NATO which is released to WEU will retain its NATO ownership label and security classification. A caveat will be added below the line to denote releasability:

Either:	NATO (Security Classification) RELEASABLE TO NATO MEMBER WEU NATIONS ONLY
Or:	NATO (Security Classification) RELEASABLE TO NATO MEMBER WEU NATIONS AND NAME(S) OF COUNTRY(IES)ONLY
E.g.:	NATO (Security Classification) RELEASABLE TO NATO MEMBER WEU NATIONS AND ROMANIA AND HUNGARY ONLY

7. In addition, the cover or first page of any document released will be marked with the name of the committee (or Board of Directors) which has authorized the release, the date the release decision was taken and any related terms.

RECORDS

8. NATO bodies will keep complete, separate records of all NATO classified information which they have released to WEU and will send details of the reference number, title and release date to the NATO Central Registry, Brussels.

APPENDIX 2 to ANNEX III

SECURITY REGULATIONS FOR THE HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION RELEASED TO WEU

GENERAL

1. All NATO classified information which is released to WEU is for official use only. It will, therefore, only be disseminated to individuals in WEU with a need-to-know and in accordance with stipulated release caveats. Within WEU, NATO classified information will be handled in accordance with WEU security regulations, which are based on NATO regulations.

PERSONNEL SECURITY CLEARANCE AND AUTHORIZATION FOR ACCESS

2. All individuals who have a need-to-know and require access to information classified NATO CONFIDENTIAL and above must have a valid WEU security clearance granted by their National Security Authority.

3. Before being given access to NATO classified information, the individual must be briefed on the protective security regulations relevant to the classification of the NATO information released, his/her liability to disciplinary action and that such action will not prejudice legal action.

CLASSIFICATION SYSTEM

4. Classification markings will be used to indicate the sensitivity of the NATO classified information and thus the security procedures and regulations which will apply for its protection. The classifications are as follows: RESTRICTED, CONFIDENTIAL, SECRET and COSMIC TOP SECRET. These correspond to WEU classifications of "RESTRICTED", "CONFIDENTIAL", "SECRET" and "FOCAL TOP SECRET".

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

5. A Registry system will be established by WEU for the receipt, despatch, control and storage of NATO classified information. Sub-registries may be established as necessary. The registry (or sub-registries) will be responsible for:

   (a) recording of receipt and despatch of all NATO classified information;

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - Jan 99

(b) distribution and control of NATO classified information within WEU;

(c) storage of NATO classified information; and

(d) the final disposal of NATO classified information including the maintenance of:

(i) destruction certificates for all information classified NATO SECRET and above;

(ii) log books or document registers for information classified NATO RESTRICTED or NATO CONFIDENTIAL.

ELECTRICAL TRANSMISSION

6. The electrical transmission of classified information between NATO and WEU shall be in accordance with agreed NATO/WEU mechanisms/procedures, which assure its protection.

BREACHES OR COMPROMISES OF SECURITY

7. Whenever a breach/compromise of security affecting NATO classified information is discovered or suspected:

(a) a report giving details of the breach/compromise must be sent immediately to the NATO Office of Security (NOS) and to the NATO Release Authority who will inform the originator(s) as required.

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the NOS. At the conclusion of the investigation, remedial or corrective action, where appropriate, must be taken.

REPORTS

8. As long as WEU holds NATO classified information it will submit an annual report, to reach the NOS by the 31st January every year, to confirm the above security regulations are being implemented.

INSPECTIONS

9. The NOS is responsible, on behalf of NATO, for security arrangements for the protection of classified information and material exchanged between NATO and WEU. It will therefore carry out regular inspections in WEU of the security measures in force to protect NATO classified information released to WEU.

APPENDIX 3 to ANNEX III

	NATO RESTRICTED
	NATO CONFIDENTIAL
	NATO SECRET
	COSMIC TOP SECRET

NORTH ATLANTIC TREATY ORGANIZATION

FROM : (DIVISION/OFFICE)

REQUEST FOR RELEASE OF WEU CLASSIFIED INFORMATION

TO : SECRETARY GENERAL, WEU INFO. : REFS. :	FILE : NO :
1. IDENTIFICATION OF DOCUMENT(S) (WHERE KNOWN)	

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - Jan 99

2. RATIONALE FOR THE REQUEST

3. INTENDED RECIPIENTS IN NATO

4. (Describe here if the whole document is needed or which part or except is requested)

Date :

Signature :

ANNEX IV

SECURITY ARRANGEMENTS FOR THE RELEASE AND PROTECTION OF NATO CLASSIFIED INFORMATION TO A NATO-LED COMBINED JOINT TASK FORCE (CJTF) OR SIMILAR FORMATION AND THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION WITH NON-NATO NATIONS/ORGANIZATIONS PARTICIPATING IN A NATO-LED CJTF OR SIMILAR FORMATION

1. The CJTF concept of deployable multinational, multi-service formations involving NATO and non-NATO nations/organizations generated and tailored for specific contingency operations was endorsed at the NATO Summit of January 1994 and is being implemented through PO(96)63 and MC 389. It reflects NATO's determination to give full and practical effect to its new roles, to strengthen the European defence capability of the Alliance and to enhance the development of the Partnership for Peace (PfP) programme.

2. Participation in a NATO-led CJTF presumes that NATO and non-NATO nations will release/exchange and protect classified information required for the conduct of the CJTF, principally to maintain the security of the forces involved and the effectiveness of the mission.

3. This Annex and its Appendices set out the security requiremements for the release and protection of NATO classified information to a NATO-led CJTF and the exchange and protection of classified information with non-NATO nations/organizations participating in a NATO-led CJTF; it draws on existing NATO policy and procedures for the release and protection of NATO classified information outside NATO.

4. The following principles will apply:

   (a) political and military endorsement of the CJTF mission will have been obtained and any legal requirements satisfied before classified information can be released to/ exchanged within a CJTF;

   (b) security formalities[1] must have been completed between NATO and non-NATO nations/ organizations to enable the latter to receive NATO classified information released to a CJTF;

   (c) NATO security policy and procedures for the handling and protection of classified information will apply to all nations/organizations participating in the CJTF;

   (d) the originator will be the sole authority for deciding the level of security classification, the release status of the classified information and any caveats/restrictions on dissemination;

[1] These include Security Agreements with Euro-Atlantic Partnership Council (EAPC) nations and Security Assurances with non EAPC nations. A copy of the Security Assurance is attached at Appendix 2.

ENCLOSURE "C" to C-M (55) 15 (Final)

0216-97 - Jan 99

(e) (i) non-NATO members participating in the CJTF will be eligible to receive information classified up to and including NATO SECRET released to the CJTF in accordance with NATO procedures;

(ii) ATOMAL information of any classification may not be released to any nation participating in the CJTF which is not a party to C-M(64)39 and C-M(68)41(5th Revise).

(f) all classified information released/exchanged will be disseminated under strict observance of the need-to-know principle and will only be used for the accomplishment of the CJTF mission;

(g) the CJTF Commander will balance the requirement to protect classified information with the need to maintain the security of the forces involved and the effectiveness of the CJTF mission;

(h) for the CJTF operation and after NAC decision on which non-NATO nations will join, and once the latter have signed the appropriate documents (including security agreements/security assurances), in order to ensure the security of forces and the effectiveness of the mission, authority for the release/exchange of all classified information of an operational nature, such as support of combined combat operations, may be delegated by the NATO Military Committee (NAMILCOM) to the level best suited to evaluate the importance of that information and the need for its immediate release. This should be specified in the promulgating NATO Operations Order (OPORD). The guiding principle will be that classified information of an operational nature that has the potential to affect the lives of CJTF personnel should be withheld only in the most exceptional circumstances. Such release of information not marked by the originator as releasable to the CJTF will be reported promptly to the NAMILCOM which will decide what limitations should be imposed on the continuing release of such information and inform the appropriate commander(s).

APPENDIX 1 to ANNEX IV

SECURITY REGULATIONS AND PROCEDURES FOR THE RELEASE AND PROTECTION OF NATO CLASSIFIED INFORMATION TO A COMBINED JOINT TASK FORCE (CJTF) OR SIMILAR FORMATION AND THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION WITH NON-NATO NATIONS/ORGANIZATIONS PARTICIPATING IN A CJTF OR SIMILAR FORMATION

1. As stated at Annex IV, a political and military mandate for the mission will be required, any legal requirements satisfied, and security formalities (see footnote 1 to Annex IV) completed before any classified information can be released to or exchanged within a CJTF.

2. A security organization and security authorities will be established in the promulgating NATO Operations Order at the inception of the CJTF and responsibilities clearly identified and defined in that OPORD. These will include:

   (a) regulating and coordinating all physical, personnel, document and information systems security (INFOSEC) issues;

   (b) clearly identifying release authorities for classified information which will be established in accordance with agreed NATO policy;

   (c) overseeing and monitoring the security régime;

   (d) contingency planning for emergency access and destruction of classified information.

SECURITY REGULATIONS - GENERAL

3. NATO civil and military bodies participating in the CJTF will comply with NATO security regulations and procedures for the handling and protection of NATO classified information. National/other organization classified information released to the CJTF will be handled and protected to the same standard as NATO classified information unless other procedures are required by the originator. Non-NATO personnel will be denied access to any NATO or national classified information that has not been authorized for release by the appropriate authority. Physical controls and security procedures will be established in order to maintain separation between NATO classified information which is not releasable to the CJTF and NATO classified information released to the CJTF.

4. This régime will be achieved by:

   (a) establishing separate NATO facilities for the collation and screening of NATO classified information prior to release. These facilities will be at the lowest level consistent with the security and effectiveness of the CJTF;

(b) permitting access to NATO secure areas by non-NATO personnel only when escorted;

(c) prohibiting access by non-NATO personnel to primary sources of NATO classified information or to IT systems and networks processing NATO classified information;

(d) permitting access by non-NATO personnel to meetings/briefings only after NATO classified information to be used in them has been approved for release;

(e) providing non-NATO nations with copies of this Annex and its Appendices and any other relevant NATO security documents to enable them to handle and protect classified information to NATO standards.

SECURITY REGULATIONS : DETAIL

5. *(a) Physical Security*

(i) areas containing NATO and other classified information must be selected to provide both effective security and for operational efficiency;

(ii) NATO classified information will be stored and controlled separately from other classified information;

(iii) NATO-only and CJTF areas must be separated and clearly identified;

(iv) access to these areas will be permitted to authorized personnel only, who have a valid and appropriate security clearance and possess a pass issued by the authorities controlling these areas;

(b) Personnel Security

(i) access to classified information will only be permitted to individuals who have a valid and appropriate security clearance issued by their national security authority or other competent national body;

(ii) it is the CJTF commander's responsibility to ensure: that all individuals participating in the CJTF are informed of the security régime and of current security regulations and procedures; that these individuals are aware of their personal responsibility for the protection of classified information to which they have access; and that these individuals receive appropriate security education and training.

(c) Document Security

(i) **RESTRICTED** information is to be handled, displayed and stored in areas to which the public is denied access. Transmission is to be achieved through secure means. Transmission by public telecommunications is to be avoided unless speed of delivery is essential to CJTF force security and mission success. Copies may be reproduced by recipients;

(ii) **CONFIDENTIAL** information is to be handled by appropriately cleared personnel with authorized access to the subject matter. When not in use, CONFIDENTIAL information is to be stored in security containers located in controlled areas. Displays of CONFIDENTIAL information will only take place within appropriately controlled areas. Transmission is to be via diplomatic couriers or military messenger services or secure telecommunications. Copies may be reproduced by recipients provided that dissemination is made under the need-to-know principle;

(iii) **SECRET** information is to be handled by appropriately cleared personnel with authorized access to the subject matter. When not in use, SECRET information is to be stored in security containers. The area in which the container is located

is to be under guard at all times and a control of entry system is to be established which only permits authorized individuals to enter the area. SECRET information is to be transmitted by diplomatic courier, secure messenger services or secure telecommunications. Copies may only be made after receipt of written approval from the originator. All copies are to be registered and controlled in the same manner as the original. All transactions involving SECRET information are to be covered by a continuous chain of receipts;

(iv) **COSMIC TOP SECRET (CTS)** - Regulations and procedures for information classified CTS are to be found in this document;

(v) Recipients are to maintain records of all information classified NATO SECRET/ NATIONAL or (other) ORGANIZATION SECRET and above released to the CJTF. Information no longer required is to be destroyed by secure means and a destruction certificate completed containing the signatures of two appropriately cleared individuals having witnessed the destruction.

(vi) Should a compromise of information classified CONFIDENTIAL and above take place, an investigation of the circumstances will be carried out by the appropriate security authority and the originator informed. CJTF participants, whether NATO or non-NATO, will cooperate in the investigation as required. Remedial or corrective action will be taken to correct any deficiency in procedures that caused the compromise. A report on the compromise and on action taken will be forwarded to the NATO Office of Security (NOS) by the investigating security authority.

(d) INFOSEC

(i) identification and authentication/access control - only authorized users, who have been uniquely and reliably identified and authenticated, shall have access to relevant classified information, whether this is national, other organization, NATO or CJTF;

(ii) accounting/audit - authorized users shall be individually accountable for their access (read, write, modify and delete) and actions (transmit/receive) with regard to classified information within the CJTF. Measures will be implemented by the CJTF security authority/ies (as specified in the OPORD) to detect and prevent users or bodies (inside or outside the CJTF) from breaching or attempting to breach the security environment;

(iii) confidentiality - confidentiality measures shall be taken to make it impossible to intercept or re-direct data communications links that carry classified information within the CJTF;

(iv) integrity - the integrity of all classified information stored, processed or transmitted within the CJTF shall be maintained; and

(v) availability - classified information within the CJTF shall be available to authorized users when required.

OWNERSHIP AND SECURITY CLASSIFICATIONS MARKINGS

6. (a) There will be a requirement to release/disseminate classified information from the planning/preparatory stages of the CJTF onwards. Originators should, therefore, designate as much classified information as possible as releasable to the CJTF. CJTF commanders and others involved in the CJTF should seek to anticipate classified information requirements at the earliest possible stage and seek approval for its release/dissemination as outlined in paragraph 7 below. Separate compartments for NATO only and for NATO classified information released to the CJTF must be created in order to provide a mechanism to control the circulation of classified information within the CJTF.

(b) The ownership and security classification marking of information is as follows. All information will:

(i) carry an ownership marking - NATO, national or other organization;

(ii) be classified according to NATO security regulations - RESTRICTED, CONFIDENTIAL, SECRET;

(iii) carry a release designator where appropriate:

Either : NATO SECRET
Releasable to (name of CJTF)

or : NATIONAL or (other) ORGANIZATION SECRET
Releasable to e.g. NATO only or (name of CJTF); and

(iv) contain any caveats regarding further dissemination:

NATO SECRET
Releasable to (name of CJTF) - Name/Names of Country(ies) only

For proprietary/legal reasons, there are only three possible ownership markings for information within the CJTF : either NATO, national or (other) organization. For example, a CONFIDENTIAL document can only be NATO CONFIDENTIAL, NATIONAL or (other) ORGANIZATION CONFIDENTIAL, **BUT NOT** NATO/ CJTF CONFIDENTIAL.

(c) Component parts of documents classified CONFIDENTIAL upwards should be marked and classified (including by paragraph) by the originator to allow further dissemination of appropriate sections. Original security classification markings/ caveats must be retained when information is used to prepare composite documents or briefings.

RELEASE AUTHORITY

7. These authorities are as follows, based on the source/originator of the classified information :

(a) National/(other) Organization: National/(other) Organization classified information may be provided to NATO and/or to the CJTF. Classified information provided exclusively to NATO can only be further released on the authority of the providing nation/organization.

(b) NATO: The NAC is the ultimate authority for the release of NATO classified information to non-NATO nations/organizations participating in the CJTF. This authority adheres to the principle of originator consent and is delegated to the lowest level consistent with operational and security requirements, and in particular to:

(i) the relevant committee for information classified up to and including NATO CONFIDENTIAL;

(ii) the NAMILCOM for information classified up and including NATO SECRET for information which has been originated by the NAMILCOM and bodies subordinate to it.

The above will also apply to all NATO classified information previously contributed by NATO nations where the national originator cannot be determined. Classified information originated within elements of the CJTF as NATO-only may subsequently be authorised for release to the CJTF by the originator.

(c) CJTF : classified information generated within the CJTF should generally be caveated as CJTF-releasable, and may therefore be released, when necessary, throughout the CJTF based on the security clearance and on the need-to-know of the recipients. Classified information generated within the CJTF which is not considered releasable, for whatever reason, to the CJTF, will be handled as either national or NATO classified, and is subject to release as described above. For the secure and effective conduct of operations, CJTF commanders of OF-6 rank or above may authorize the release of information already released to the CJTF to individuals or organizations beyond the CJTF on a need-to-know basis for CJTF force security and mission success purposes only.

8. In all cases, any classified information of an operational nature that has the potential to affect the lives of CJTF personnel, should be withheld only in the most exceptional circumstances.

APPENDIX 2 to ANNEX IV

SECURITY ASSURANCE

The (country or organization) represented by (name and function) in the furtherance of (name of the CJTF) agrees:

(a) to protect classified information provided to it by (name of the CJTF) in a manner equivalent to that used to protect its own classified information of an equivalent or higher level;

(b) to provide such classified information only to appropriately cleared individuals under its jurisdiction with a need-to-know;

(c) to use such information only for the purposes for which it was provided;

(d) not to transfer such information to a third party without the prior written approval of the originator of the information; and

(e) to continue to abide by these security requirements even after completion of (name of the CJTF).

ANNEX V

NATO SECURITY CLEARANCE CERTIFICATE

1. Certification is hereby given that:

Full Name: .....

Date and Place of Birth: .....

has been granted a security clearance by the Government of

.....

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

.....

.....

.....

.....

2. The validity of this certificate will expire not later than(2)

.....

Signed:

Title: Official government stamp

Date:

---

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

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

(2) Date of expiry of this certificate must conform with the provisions of paragraph 4 of the Supplement to C-M(55)15(Final)

0216-97 - Jan 99

ENCLOSURE "C" to C-M (55) 15 (Final)

ANNEX VI

CERTIFICATE OF SECURITY CLEARANCE

Issued by .....
(member nation or NATO command or agency)

Date and Place of Issue

.....

..... Valid until .....

This is to certify that:

Full Name .....

Date of Birth .....

Place of Birth .....

Nationality .....

Where employed .....

Purpose and Duration of Visit .....

.....

.....

.....

Holder of Passport/Identity Card No. .....

Issued at ..... Dated .....

Military Rank and Number (where applicable) .....

.....

has been cleared for access to NATO information classified up to and including

..... in accordance with

current NATO security regulations and has been briefed accordingly by

.....

Signed:

Title: Official government stamp

Date:

NOTE: This certificate must be handled in accordance with the provisions of paragraph 87 of Enclosure "C" to C-M(55)15(Final)

ENCLOSURE "C" to

0216-97-Jan 99

ANNEX VII

COURIER CERTIFICATE

Valid until .....

1. This is to certify that the bearer ....., holder of Passport/
(name and rank where applicable)

Identity Card No. ..... is a member of .....
(parent organization)

2. On the journeys detailed overleaf, the bearer is travelling in the execution of his official functions and is designated as an official NATO courier. He is authorized to carry ..... (number) of packages of official NATO documents, the seals on which correspond to the specimen seal appearing against the appropriate journey.

3. All customs and immigration officials concerned are, therefore, requested to extend to the official correspondence and documents being carried under official seal by the bearer, the immunity from search or examination conferred by the Agreement on the Status of the North Atlantic Treaty Organization National Representatives and International Staff, and the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces.

Signature of Authorizing Official:

Designation:
(Name and rank in capitals)

Official stamp of NATO member nation or NATO command or agency

Date:

ORDRE DE MISSION D'UN COURRIER

Valable jusqu'au .....

1. Il est certifié par la présente que le porteur ....., détenteur
(nom et grade, le cas échéant)

du Passeport/Carte d'identité n°. ..... est membre de .....
(organisme d'appartenance)

2. Au cours des voyages mentionnés au verso, le porteur voyage en exécution de ses fonctions officielles et est accrédité comme un courrier officiel de l'OTAN. Il est autorisé a transporter ..... (nombre) paquets contenant des documents officiels de l'OTAN, dont les sceaux correspondent au modèle du sceau apposé en regard du voyage indiqué.

3. Tous les fonctionnaires des services de douanes et de l'immigration sont, en conséquence, priés d'appliquer à la correspondance et aux documents officiels transportés sous sceau officiel par le porteur, l'immunité prévue en matière de visite et de contrôle douanier par la Convention sur le Statut de l'Organisation du Traité de l'Atlantique Nord, des Répresentants nationaux et du Personnel international et la Convention entre les Etats parties au Traité de l'Atlantique Nord sur le Statut de leurs Forces.

Signature du fonctionnaire responsable:

Désignation:
(nom et grade en majuscules)

Sceau officiel du pays membre de l'OTAN ou du commandement ou organisme de l'OTAN

Date:

ENCLOSURE "C" to
C-M (55) 15 (Final)

0216-97 - Jan 99

DETAILS OF ITINERARY DETAILS DE L'ITINERAIRE		SPECIMENS OF SEAL USED MODELE DU SCEAU UTILISE
From De	to à	See note below Voir note ci-dessous
From De	to à	See note below Voir note ci-dessous
From De	to à	See note below Voir note ci-dessous
From De	to à	See note below Voir note ci-dessous

NOTE: In addition to an impression of the seal, the officer affixing the seal must print his name, rank and the name and address of his department, command, agency or facility.

En complément à l'impression du sceau, le fontionnaire apposant le sceau doit mentionner en majuscules, son nom et grade ainsi que le nom et l'adresse de son service, commandement, organisme ou établissement.

ANNEX VIII

LIST OF INFORMATION, PHYSICAL AND PERSONNEL SECURITY GUIDANCE DOCUMENTS

REFERENCE	DATE	CL	TITLE
AC/35-D/1000	08.03.72	NR	Review of NATO Security Committee documents in the AC/35-D series
AC/35-D/1001(Revised) + Supp 1, 2 & 3 Supp 4 & 5 Supp 6 & 7 Supp 8, 9, 10, 11(a),(b) & (c) Supp 12, 13 & 14 Supp 15 & 16	07.08.75 05.02.76 17.06.76 05.05.77 29.08.79 03.04.80 07.05.81	NC/ NR/ NU	Security Education
AC/35-D/1002(Revised)	07.02.77	NU	NATO security classifications with their national equivalents
AC/35-D/1003(Revised)	09.04.79	NU	Personal carriage of NATO classified documents
AC/35-D/1004 (3rd revise)	09.06.95	NR	Security clearance procedures for NATO staff
AC/35-D/1005(Revised)	28.07.83	NR	Guidance on policy and minimum standards for the physical measures for the protection of NATO classified information
AC/35-D/1006(Revised)	05.07.76	NR	Guidance on the conduct of inspections by NATO components' security authorities
AC/35-D/1007(2nd revise)	28.02.86	NR	Guidance on planning for the security protection of NATO commands and agencies
AC/35-D/1008(4th revise)	28.03.90	NR	CANCELLED (Security briefings of individuals exposed to contact with nationals of countries with special security risks)
AC/35-D/1009(4th revise)	09.12.94	NR	Security of Automatic Data Processing Systems (ADPS)
AC/35-D/1010	23.06.76	-	CANCELLED (Secure Voice System)
AC/35-D/101(2nd revise)	10.03.87	NU	SUPERSEDED and replaced by the NATO Security Awareness Catalogue

REFERENCE	DATE	CL	TITLE
AC/35-D/1012(Revised)	28.05.90	NU	NATO Trusted Computer System Evaluation Criteria
AC/35-D/1013	15.12.88	NR	CANCELLED (AC/35-N/235 - 20.01.95) NATO microcomputer security policy guidance
AC/35-D/1014	23.07.90	NR	Guidelines for the structure and content of security operating procedures for ADP systems and networks
AC/35-D/1015(Revised)	15.11.96	NR	Guidelines for the development of a security requirement statement
AC/35-D/1016	19.10.90	NU	Guidelines for conducting an ADP inspection/review - an aide mémoire
AC/35-D/1017(Revised)	17.11.93	NR	Guidelines for ADP security risk analysis
AC/35-D/1018(Revised)	26.04.95	NU	Guidelines for the specification of computer security features in procurement documentation
AC/35-D/1019	03.08.92	NU	Guidelines for the evaluation and certification of ADP systems and networks and computer security (COMPUSEC) products
AC/35-D/1020(2nd Revise)	23.07.96	NC	Review of the nature and extent of the threats to, and vulnerabilities of, ADP systems and networks
AC/35-D/1021(Revised)	03.02.97	NR	Guidelines for the accreditation of ADP systems and networks
AC/35-D/1022	20.01.93	NU	Provisional security policy guidance on the interconnection of networks
AC/35-D/1023	23.04.93	NR	Guidelines for the assessment of computer seccurity functionality classes and assurance levels in specific environments
AC/35-D/1024	09.07.93	NR	Establishment, update and maintenance of a NATO computer security products list and a NATO computer security "products under evaluation" list
AC/35-D/1025	20.05.94	NU	Guidelines for the organization and management of ADP security

ANNEX IX

RESTRICTIONS GOVERNING THE INTERNATIONAL CARRIAGE OF CLASSIFIED DOCUMENTS OR MATERIAL

1. The following regulations concern the destinations, routes to be taken and means of transportation to be used by persons other than couriers and messengers, when carrying documents and material classified NATO CONFIDENTIAL and NATO SECRET.

2. The bearer must not travel to, through or over non-NATO countries to which one or more of the criteria listed below are applicable.

   (a) the government of the country:

   - gives evidence by word or deed of an attitude hostile to NATO and/or its member nations;
   - is not able to give a generally agreed level of protection to the life and/or personal belongings of its residents and/or visiting foreigners;
   - has given evidence not to respect at all times the immunity of a diplomatic seal;

   (b) the intelligence services of the country target the Alliance and/or its member nations;

   (c) the country is at war, or subject to serious civil strife.

   For the choice of the means of transportation, these criteria equally apply.

3. In choosing the means of transportation, the bearer will exclude any carrier registered in a non-NATO country to which any one of the criteria listed above applies.

4. Exceptionally, the above restrictions need not apply, if urgent operational requirements cannot be met otherwise.

ENCLOSURE "D"

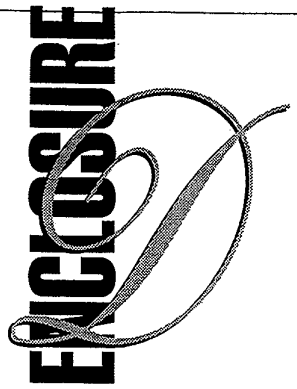
INDUSTRIAL SECURITY

TABLE OF CONTENTS

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

ANNEXES TO ENCLOSURE "D"



INTRODUCTION

1. This document deals with the security aspects in relation to NATO classified information issued to industry and to NATO classified contracts with industry, taking into consideration the major principles set forth in Enclosure "B" and at paragraphs 1 to 5 of Enclosure "C".

2. **Section I** : provides the definitions of all specific terms used in the present Enclosure.

3. **Section II** : sets out the responsibilities of the security authorities, at all levels, involved in NATO classified contracts and in the release of NATO classified information to industry.

4. **Section III** : describes the security procedures to be enforced in the negotiation and the letting of NATO classified contracts.

5. **Section IV** : sets out the general rules for issuing NATO Facility Security Clearances to facilities and NATO Personnel Security Clearances to the personnel involved in NATO classified contracts.

6. **Section V** : provides the security procedures to be enforced during the international transportation of NATO classified material.

7. **Section VI** : describes the security procedures to be followed for the control of international visits to facilities, agencies involved in a NATO classified programme.

ENCLOSURE "D" to
C-M (55) 15 (Final)

0216-97 - October 97

SECTION I

DEFINITIONS

GENERAL

NATO Classified Contract

1. Any contract issued by NATO or a NATO member nation in support of a NATO - funded or administered project/programme that will require access to NATO classified information.

Classified Information

2. Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorized disclosure which has been so designated by security classification.

NATO Classified Information

3. All classified information, military, political and economic, circulated within NATO, whether such information originates in NATO commands and agencies or is received from member nations or from other international organizations.

Material, Equipment/Components, Document

4. (a) The word "material" includes documents and equipment/components.

   (b) The words "equipment/components" designate any item of machinery or equipment or weapons either manufactured or in the process of manufacture.

   (c) The word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproduction by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

GLOSSARY SECTION II

Designated Security Authority (DSA)

5. An authority subordinate to the National Security Authority (NSA) to be responsible for :

   - communicating to industry the national security policy in all matters of NATO industrial security policy;

   - providing direction and assistance in its implementation.

   In some countries, the function of a DSA may be carried out by the NSA.

Facility

6. An installation, plant, factory, laboratory, office, university or other educational institution or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.

NATO Production and Logistics Organization (NPLO)

7. A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which the North Atlantic Council grants clearly - defined organizational, administrative and financial independence.

It shall comprise:

- a board of directors; and
- an executive body, composed of a General Manager and its staff.

NATO Project Management Agency

8. The executive body of a NPLO.

NATO Project Management Office

9. The office of any non-NPLO NATO agency or command, responsible for the management of a NATO classified project or contract.

Project Manager

10. The manager responsible for any NATO project/programme or contract.

GLOSSARY SECTION III

Infrastructure

11. The NATO term denoting all those installations which are necessary for the deployment and operations of modern armed forces, for example: airfields, signals, communications, military headquarters, fuel tanks and pipelines, radar warning and navigational aid systems, port installations and so forth.

Contracting Officer

12. The duly appointed representative of a government department, or agency of a member nation, or a NATO Military Command, or NATO Project Management Agency/Office who has the authority to negotiate, let and administer NATO prime contracts on behalf of the member nation or NATO.

Prime Contractor

13. An industrial, commercial or other entity of a member nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential subcontractors as approved.

Contractor

14 An industrial, commercial or other entity of a member nation which has already contracted with another industrial, commercial or other entity primarily involved in a NATO project and

which wants to let a sub-contract with a potential sub-contractor to perform a service, or manufacture a product, in the framework of the same NATO project.

Contract Manager

15. The duly appointed representative of a facility already engaged in a NATO. related project who has the authority to negotiate or let and administer on behalf of the facility sub-contracts for a NATO classified project.

Sub-Contractor

16. An industrial, commercial, educational, or other entity of a member nation which has sub-contracted, with a contractor or with another sub-contractor to perform a service or manufacture a product, as part of a NATO classified contract.

Negotiations

17. The term encompasses all aspects of awarding a contract or sub-contract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.

Security Aspects Letter (SAL)

18. A document issued by the appropriate authority as part of any NATO classified contract or sub-contract, identifying the security requirements or those elements thereof requiring security protection for a NATO classified contract.

Security Classification Check List

19. A listing of the NATO information connected with the various aspects of a NATO classified contract that should be classified and of the classification levels to be assigned thereto. That listing may be annexed to, or incorporated in, a "Security Aspects Letter".

Project Security Instructions (PSI)

20. In major projects, a document prepared and issued by the NATO Project Management Agency/Office, approved by the responsible NSAs/DSAs of the participating nations, annexed to the prime contract and, if appropriate, to sub-contracts. The PSI describes the compulsory security provisions required for the performance of the contract and the methods by which NATO project information and material will be classified, marked, handled, processed, transmitted and safeguarded. The PSI (which includes a Project Security Classification Guide) shall be developed under the terms agreed in the Project Agreement.

Project Security Classification Guide

21. A document similar to the "Security Classification Check List", but for major projects, established by the Security Classification Board of the NATO Project Management Agency/Office and annexed to the PSI.

GLOSSARY SECTION IV

NATO Facility Security Clearance (NFSC)

22. A determination by an NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO classified information of a specified classification or below, and its personnel who require access to NATO classified information have been properly cleared and briefed on NATO security requirements necessary to fulfil on the NATO classified prime or sub-contract.

Host Nation

23. The nation designated by an official body of NATO to act as the governmental agency to contract for the execution of a NATO prime contract. Nations in which sub-contracts are executed are not referred to as host nations.

Nation of Origin of Contractor

24. The nation in which the contractor is registered or incorporated and which characterizes the nationality of the facility which fulfils the contract.

GLOSSARY SECTION V

Classified Material as Freight

25. Consignments of such size, weight or configuration that they cannot be hand-carried, transmitted by diplomatic pouch service, or military courier service.

Commercial Carrier

26. Any company authorized by law or regulation to provide the required transportation service and authorized by the NSA/DSA to transport (and safeguard) classified consignments under specific guidelines.

Cargo Handling Company
(may include a freight forwarder or a transportation agent)

27. A commercial company responsible for loading and unloading classified cargo from an aircraft and providing constant protection for the classified cargo while it is on trolleys, open cargo pits or cargo transfer areas.

Security Escorts

28. Armed or unarmed national police, military or government personnel. Their function is to facilitate the secure movement of material but they do not have direct responsibility in matters for the protection of the material itself.

Security Guards

29. Civilian (government or participating contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security duties only or may combine security guard duties with other duties.

Courier

30. A person officially assigned for the transportation of hand-carried material. The term can also be extended to designate any person assigned by a consignor for the transportation of hand-carried material between a consignor and a consignee.

Consignor

31. The contractor, facility or other organization responsible for organizing the international despatch of material, hand-carried or in large consignments, to the consignee.

Consignee

32. The intended recipient/organization receiving the material from the consignor. It does not include carriers or agents.

Container

33. An NSA/DSA - approved large receptacle of solid construction with a locking system, capable of being carried on an aircraft, by a road vehicle or trailer or rail flat truck or in a ship's hold or on deck.

GLOSSARY SECTION VI

International Visits

34. Visits made by individuals subject to one NSA/DSA or belonging to NATO, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO-approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO commands and agencies fall within the security jurisdiction of NATO.

SECTION II

GENERAL RESPONSIBILITIES

MEMBER NATIONS

35. 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; the NSAs/DSAs are listed at Annexes XII and XIII;

(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 the information adequately;

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

(iii) grant a NATO Personnel Security Clearance (NPSC) to all personnel whose duties require access to NATO classified information;

(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 command or agency, an NFSC 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 command or agency, a NPSC for the persons for whom it has security responsibilites to enable them to fulfil on a NATO classified contract which may include international visits;

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

(h) take action with regard to the specific arrangements to be carried out in matters of transportation in accordance with Section V, and in matters of international visits in accordance with Section VI;

(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 unauthorized persons. Each member nation shall comply with the investigative requirements in Section IX of Enclosure "C" and promptly inform the other member nations concerned via NOS of the details of any such occurrences;

(j) ensure that for any facility in which NATO classified information is to be used, a person or persons shall be appointed 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 approved for access and have a need-to-know.

THE NATO SECURITY COMMITTEE

36. The NATO Security Committee shall :

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

(b) consider matters of industrial security referred to it by the Council, a member nation, the Secretary General, the NATO Military Committee (NAMiCom), Major NATO Commands and heads of NATO military and civil agencies.

THE NATO OFFICE OF SECURITY (NOS)

37. 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 procedures in those organizations 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 procedures in connection with the activities of NPLOs;

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

(d) make annual 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;

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

38. By its Terms of Reference (TOR), the NOS is concerned only with NATO classified contracts connected with NPLOs unless other special arrangements have been made.

NATO PROJECT MANAGEMENT AGENCIES/OFFICES

39. Each of the NPLO's 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 this document, including its Supplement, 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 this Enclosure and supervise their enforcement;

(b) in conjunction with the NSAs/DSAs concerned and the NOS, co-ordinate the implementation of NATO security policies and procedures, 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 Section VI in respect of the special arrangements for International Visits;

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

NATO COMMANDS

40. Each NATO command will take action in accordance with the provisions of Section VI in respect of those of its personnel to whom the special arrangements described in that Section apply.

SECTION III

NATO CLASSIFIED CONTRACTS

GENERAL

41. NATO classified contracts result from NATO projects, worked out and managed by any NATO body; as such, they include NPLOs and NATO infrastructure projects.

42. The prime contract(s) in a NATO-related project will be let by the contracting officer designated by the NATO Project Management Office/Agency responsible for the project. A diagram showing security policy and liaison links in respect of NPLO projects is at Annex I.

43. Sub-contracts will be let by the contract manager of a facility already engaged in a NATO contract or sub-contract.

44. The security requirements and procedures in connection with NATO classified infrastructure work are set out in a separate document.

45. All NATO classified contracts will comprise a SAL which includes a Security Classification Checklist as defined in Section I. NATO classified contracts for major projects will also contain the PSI as an annex; in this case, the Security Classification Checklist will be named "Project Security Classification Guide" and will be part of the PSI.

46. The NATO Project Management Agency/Office shall develop a PSI and a Project Security Classification Guide for the project, within a specified time period previously agreed by the NSAs/DSAs. The PSI and the Project Security Classification Guide will describe the methods by which programme information and material will be handled, classified, marked, processed, transmitted and safeguarded. The PSI will include the procedure for releasing classified and, if applicable, other programme information requiring control to third parties. Both documents will be approved by the NSAs/DSAs of the participants and will be applicable to all participant and contractor personnel participating in the programme.

47. Each NATO Management Agency/Office will develop and maintain an up-to-date :

    (a) "Facilities List" consisting of contractors and sub-contractors holding NATO classified contracts connected with the NATO project/programme;

    (b) list of all government departments or agencies known to the NATO Management Agency/Office to be involved in the project/programme;

    (c) list of any NATO command or agency involved when applicable.

48. An updated "Facilities List" will be issued annually and disseminated to all NSAs/DSAs and NATO Commands/Agencies involved in the project/programme.

49. The format of the "Facilities List" is shown at Annex X.

SECURITY CLASSIFICATION OF CONTRACTS

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

    (a) the allocation of security classifications is the responsibility of the originator of the classified information;

    (b) security classifications should be applied only to those aspects of a contract that must be effectively protected and such classifications should be strictly related to the degree of protection required;

    (c) a compilation of information from more than one source will require co-ordination of the sources in the determination of the appropriate NATO security classifications;

    (d) provision should be made for downgrading and declassification as soon as this is possible;

    (e) any change of classification level has previously to be submitted to the authorization of the originating authority.

51. The responsibility for applying a security classification to a project dealing with a product wherein all components are clearly defined and classified rests with the NATO Project Management Agency/Office of the contract, acting in collaboration with the NSAs/DSAs of the participating member nations.

52. The initial assessment for the protection of information contained in a project/programme not previously identified for classification rests with the contractor having system design responsibility. Contractors will notify their government programme managers to take appropriate classification actions.

53. The Project Security Classification Guide will be developed by the NATO Project Management Agency/Office in close cooperation with the industry; in order to assist the management agency/office, a "Security Classification Board" may be established. Such boards will be comprised of representatives of the NSAs/DSAs of the participating nations in the appropriate NATO programme. The Project Security Classification Guide will be subject to regular review and revision. In the absence of clearly-defined security guidance, a security classification proposal will be forwarded by the originator who has system design responsibility to the appropriate NSA/DSA who will notify the appropriate NATO Project Management Agency/Office regarding interim classification allocated. The NATO Management Agency/Office will review the proposed security classification guide and eventually update the Project Security Classification Guide and notify all NSAs/DSAs on a regular basis.

54. The classifications for possible sub-contracts will be based on the Project Security Classification Guide of the appropriate PSI.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

55. Release of NATO classified information must be with the consent of the originator and in accordance with Enclosure "C", as follows :

    (a) responsibility for the release of NATO classified information connected with a contract or sub-contract rests primarily with the project manager of the NATO Project Management Agency/Office;

    (b) in the case of NPLO contracts or sub-contracts, it should be noted that, when considering the release of NATO classified information, even within NATO, reference should be made to the terms of the charter of the particular NPLO before NATO classified informa-

mation is released. That charter, or the security instructions for the project may prohibit the release of NATO classified information to non-participating NATO member nations except with the agreement of all the participating member nations.

NEGOTIATION OF NATO CLASSIFIED CONTRACTS

Prime Contracts

56. Before negotiating a NATO classified prime contract, a NATO Management Agency/Office or member nation contracting officer will contact the NSA/DSA of a potential contractor for a confirmation that the potential contractor holds an appropriate NFSC at least equal to the classification level of the information that will be required during the negotiation of the contract. The NSA/DSA will provide the contracting officer with the NATO Facility Security Clearance certificate/notification. If the contracting officer is aware that the potential contractor has no NFSC, he will forward a request to the NSA/DSA that such a clearance be initiated. The format for such a request is at Annex II, entitled "Facility Security Clearance Information Sheet" (FIS). The contracting officer will also include the highest NATO security classification of the information required, its nature and volume in the remarks section of the FIS.

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

58. The contracting officer negotiating the contract shall ensure that :

    (a) representatives involved in the negotiations will only receive access to NATO classified information concerned with the purpose of the contract;

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

Sub-Contracts

59. After a prime contract has been let, it may be necessary for a prime contractor to negotiate sub-contracts with sub-contractors, at the first level. These sub-contractors, in turn, may also negotiate sub-contracts with other sub-contractors at the second level etc.

60. Contractors and sub-contractors who intend to negotiate a sub-contract shall:

    (a) be aware that there are certain sub-contracts for which permission to negotiate and to place a sub-contract must be sought from the NATO Project Management Agency/ Office;

    (b) seek such permission prior to the release of the request for the NFSC. If deemed necessary both actions may be taken simultaneously. Close co-operation between the Contract Manager and the Security Officer is required.

61. When the contractor and sub-contractor are of the same NATO member nation, permission to negotiate will not be required from the contracting officer of the NATO Project Management Agency/Office concerned, unless otherwise prohibited in the contract document. It will, however, be informed by the contractor that a sub-contract is negotiated, and be given all contractual details relevant to the security of NATO information involved. It will be the

responsibility of the contractor to ensure through the NSA/DSA that all sub-contractors meet and comply with the appropriate security requirements.

62. At whatever level it is proposed to negotiate a sub-contract, the following will apply :

(a) before entering into negotiations, the Security Officer of the contractor will take the actions outlined in paragraph 56 above, with respect to the potential sub-contractor, to its own NSA/DSA. A copy of the request will be forwarded to the relevant NATO Project Management Agency/Office (or Project Manager);

(b) when the potential sub-contractor is subordinated to another NSA/DSA, the NSA/DSA of the contractor will issue the request to the former;

(c) the NSA/DSA of the potential sub-contractor will return the completed form, together with the required information to the contractor, following the same channels; a copy of the NFSC notification (FIS) should be forwarded by the NSA/DSA for information to the NATO Project Management Agency/Office concerned, which will maintain an index of the security-cleared facilities of the appropriate NATO programme;

(d) on receipt of the NFSC notification, the contractor may open negotiations with the potential sub-contractor; all classified information issued by the contractor will transit to its own 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 issued to the latter;

(e) the contractor will enforce the measures set forth in paragraphs 57 and 58 above.

63. Sub-contracts classified NATO RESTRICTED will be treated in accordance with the security policy established by the nations.

SECURITY PROVISIONS IN RELATION TO NATO CLASSIFIED CONTRACTS

64. The prime contractor and sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSA/DSA for safeguarding all NATO classified information entrusted to, generated or manufactured by the contractor.

65. The security provisions in relation to a classified contract will be stated in the SAL or the PSI, with respect to the scope of the programme.

66. By these provisions, the contractor or sub-contractor will specifically be required to :

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

(b) maintain, preferably through the official responsible for security measures, a continuing relationship with the NSA/DSA charged with ensuring that all NATO classified information involved in the contract or sub-contract is properly safeguarded;

(c) abstain from copying by any means, without the authorization of the NSA/DSA, any NATO classified information entrusted to him by the government;

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

(e) maintain at the place of work a current record of those employees who have been cleared for access to NATO classified information. This record should show the date and level of clearance and the date of end of validity of the clearance;

(f) deny access to NATO classified information to any person other than those specifically authorized to have such access by the NSA/DSA;

(g) 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;

(h) comply with any request from the NSA/DSA that persons entrusted with NATO classified information sign a statement undertaking to safeguard that information and acknowledging their understanding both of their obligations under national legislation affecting the safeguarding of classified information, and of their comparable obligations under the laws of the other NATO nations in which they have access to classified information;

(i) report to the NSA/DSA, any breaches or suspected breaches of security, suspected sabotage, or subversive activity, 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 or 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 appropriate security obligations no less stringent than those applied to his own contract or sub-contract;

(k) undertake not to utilize, other than for the specific purpose of the contract, or sub-contract, without the prior written permission of the contracting officer or contract manager, or his authorized representative, any NATO classified information with which he is provided, including all reproductions thereof in connection with the contract or sub-contract. The sub-contractor will return all NATO 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 authorized with the approval of the contracting officer or contract manager. Such NATO classified information will be returned at such time as the contracting officer or contract manager or his authorized representative may designate;

(l) comply with any procedure that is, or may be, established regarding the release of NATO information related to the contract or sub-contract.

LETTING OF CONTRACTS

67. In the case of the prime contract, the contracting officer will notify the decision to the NSA/DSA of the prime contractor, and issue the SAL or PSI as applicable (see paragraph 65).

68. In the case of a sub-contract, the contract manager will notify the decision to his parent NSA/DSA, to the prime contractor and to the NATO Project Management Agency/Office in due time and will also inform them about the security-related aspects set forth in paragraph 65. The NSA/DSA will make the necessary arrangements for the protection of all classified information released to the sub-contractor.

69. When the potential sub-contractor is from another NATO nation, the NSA/DSA of the contractor will pass the information mentioned in paragraph 65 to the NSA/DSA of the potential sub-contractor, which will be responsible for taking the actions outlined in paragraph 64. Where, however, NSAs/DSAs do not wish to receive this information automatically, they may mutually agree to obtain it on a "specific request" basis only.

70. Prior to the decision to let a contract, in the light of the requirements of the SAL or the PSI attached to the contract, the NSA/DSA will :

(a) issue to the contracting officer or contract manager, the requisite NFSC certificate/notification in accordance with Section IV;

(b) issue the requisite NPSC certificate/notification for the facility's personnel who will require access to the classified aspects of the NATO contract in accordance with Section IV;

(c) ensure that the personnel mentioned in sub-paragraph (b) above are briefed on NATO security regulations. The contract will become effective only after completion of these measures.

Consortia

71. (a) In most cases, the staff of a contracting consortium have the status of prime contractor in respect of dealings with a contracting NATO Project Management Agency/Office. The management agency/office shall hold NFSCs for each constituent part of any consortium prior to undertaking any negotiations with it;

(b) when a consortium is constituted to act as a sub-contracting party, its staff has the status of sub-contractor. The contractor will require an NFSC for each of the constituents prior to undertaking any negotiations;

(c) the SAL will be so worded as to ensure that the security measures incorporated in it are equally binding on all constituent elements of any contracting consortium.

SECTION IV

NATO INDUSTRIAL SECURITY CLEARANCES

GENERAL

72. The clearance procedures described in subsequent paragraphs, whether of individuals or firms, apply only to contracts or sub-contracts requiring access to information classified NATO CONFIDENTIAL or above. The procedures for authorizing access to individuals and to facilities requiring access only to NATO RESTRICTED information will be according to regulations laid down by the relevant NSA's. Such authorization will be communicated as required and by whatever means considered appropriate by the issuing NSA/DSA or NATO command or agency.

NATO FACILITY SECURITY CLEARANCES (NFSCs)

Issue of NATO Facility Security Clearances

73. The NSA/DSA of each member nation will be responsible for ensuring that any facility registered or incorporated in that nation which will require access to information classified NATO CONFIDENTIAL or above has taken adequate measures to afford the necessary security protection to such information (Annex III) and involved NATO Project Management Agencies/ Offices will be informed accordingly. For NATO classified contracts at NATO RESTRICTED level, national rules will apply.

74. This will involve making an assessment :

- of the physical security access authorizations and procedural arrangements provided for the protection of NATO classified information to ensure that they comply with the requirements of Sections IV, V and X of Enclosure "C"; and

- of the personnel security status of owners, directors, principal officials and executive personnel of the facility, and of such other persons or employees who may by virtue of their association, position or employment, be required to have access to NATO classified information, to ensure that such status corresponds with the obligations imposed by the following paragraphs dealing with personnel security.

75. Should a facility require access to information classified NATO CONFIDENTIAL or above as a result of its wish to bid for, or enter into pre-contractual negotiations related to a NATO classified contract or sub-contract, the security measures required will be as deemed appropriate by the NSA/DSA of the facility and will be related to the NATO security classification of the information, its volume and nature and the number of persons who will require to have access to it in the course of preparing bids or negotiations.

76. In granting an NFSC, NSAs/DSAs will ensure that they have the means to be advised of any changes which may occur which have a bearing upon the validity 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 directors, a change in its physical location, an alteration to the premises it occupies or a variation in security procedures.

77. Should it be necessary to consider granting an NFSC to a facility, the management of it being subject to different factors involving several nations, the NSA/DSA will need to evaluate the extent to which any foreign interest represents a threat to the security of NATO classified information that may be entrusted to that facility.

78. The responsible NSA/DSA will issue the NFSC, when requested, in the format shown at Annex II.

79. When mutually agreed, NSAs/DSAs may inform each other by lists of all relevant information about their facility's security status, provided that such lists are regularly updated; however, should a facility not be found on the list, a request should be sent to the relevant NSA/DSA.

80. The NSA/DSA of a member nation will specify the physical security measures to be taken for the protection of NATO classified information in each facility in that member nation.

81. Consultants who perform their work on the premises of a contracting facility engaged upon a NATO classified contract and who have no need to remove classified information from the premises, will be expected to observe the same security requirements as employees of the facility concerned. Those who are obliged to work away from such premises, or to have physical custody of NATO classified information, will, in addition, be required to give the same security protection to such information as is given at the facility.

Changes to or Revocation of NATO Facility Security Clearances

82. Should an NSA/DSA which has issued an NFSC by means of a FIS form, change or withdraw that clearance, it will at once notify the NSA/DSA or NATO Project Management Agency/ Office which issued the notification.

83. The fact that an NFSC is revoked or withheld from a facility must not be disclosed to the facility by any other NSA/DSA, except with prior permission from the parent NSA/DSA.

SECURITY CLEARANCES OF PERSONNEL (NPSC)

General

84. Each person who requires access to NATO information classified NATO CONFIDENTIAL or above in connection with NATO industrial activities will be appropriately security cleared by his parent NSA/DSA and briefed on NATO security procedures in accordance with Enclosure "B" and Section V of Enclosure "C".

85. The classification of the information to which a person will have access will normally decide the extent of the clearance procedure which must be carried out to establish his bona fides, and will likewise decide what level of security clearance he requires. This basic principle applies also with regard to clearance of a person who is to be employed in the negotiation or fulfillment of a classified contract.

Application for NATO Personnel Security Clearances (NPSC)

86. Applications for the security clearance of employees of industrial facilities will be made to the NSA/DSA of the facility.

87. In submitting personal particulars, the facility will specify :

    (a) the security classification of the NATO contract or sub-contract; and

    (b) the level of NATO classified information to which the employee will have access.

Issue of Security Clearances

88. An individual's parent NSA/DSA is responsible for issuing his security clearance. When an individual who is not a national of the nation of origin of the facility requires access to classified information, the facility's parent NSA/DSA will consult the individual's parent NSA/DSA.

89. If a facility wishes to employ a national of a non-NATO nation for access to NATO classified information, it is the responsibility of the NSA/DSA of the nation of origin of this facility to issue the security clearance if it feels able to take this responsibility.

90. The NPSC is transmitted either in accordance with the procedures set forth in Section VI with respect to international visits, or by means of a NATO Security Clearance certificate, the format of which is shown at Annex III of Enclosure "C", as requested by any NSA/DSA or NATO Project Management Agency/Office.

Procedures to be followed when a security clearance is denied

91. Should the NSA/DSA of the parent nation of any person who is required to have access to the classified aspects of a contract be unable to issue a security clearance for that person, it will immediately inform the NSA/DSA of the nation of origin of the facility, who will, in turn, inform the facility itself, and not involve the employee in any classified work.

92. The question of whether or not the employee concerned is to be informed if his security clearance is withheld will be decided by his parent NSA/DSA.

Procedures to be followed when a security clearance is revoked

93. Should an employee who has received a security clearance subsequently come to adverse security notice in his parent nation in such a manner as to make it desirable to withdraw his security clearance, his parent NSA/DSA will inform the NSA/DSA of the nation of origin of the facility, which will ask the facility to withdraw the employee from classified work.

94. Should an employee already cleared for employment on classified work come to adverse security notice in the nation of origin of the facility in such a manner as to make it desirable to withdraw his security clearance, the facility's parent NSA/DSA is responsible for taking action by withdrawing the employee from classified work in accordance with its national security laws and regulations; other NSAs/DSAs and the individual's parent NSA/DSA will be notified of the action taken.

95. Clearances required for individuals working in international contexts which have been withdrawn will be cancelled immediately by the authorities which have issued them.

Interim Security Clearances

96. The basic principle to be followed is that the issue of interim security clearances in advance of full security clearance to persons to be employed on NATO classified contracts and who will require access to NATO classified information should, whenever possible, be avoided.

97. In exceptional cases, where the attainment of major military objectives would otherwise be impaired, or when other compelling reasons are present, interim personnel security clearances may be issued in connection with contracts classified NATO SECRET or NATO CONFIDENTIAL. The interim personnel security clearances may not, however, be issued in connection with contracts classified COSMIC TOP SECRET.

98. Interim personnel security clearances may only be issued to nationals of NATO member nations.

99. Interim personnel security clearances will be issued by the parent NSA/DSA of the person concerned, only when the following conditions have been fulfilled :

(a) national laws and regulations permit;

(b) after reference to relevant national records and, if appropriate, to the NSA/DSA of the country in which the person is residing, the parent NSA/DSA attests that nothing has been found to the detriment of the person in question from a security viewpoint; and

(c) the appropriate investigation is ongoing in order to issue a full personnel security clearance.

100. The period of validity of an interim personnel security clearance will be determined and notified by the issuing NSA/DSA but may never be longer than the necessary timeframe nationally required for the issuance of the full personnel security clearance.

SECTION V

INTERNATIONAL TRANSMISSION OF NATO CLASSIFIED MATERIAL[1]

INTRODUCTION

101. The following security procedures for the international transmission of NATO classified material represent minimum criteria and do not apply where more restrictive security measures have been established by member nations. Moreover, the classification of NATO SECRET is the highest classification of material that can be the subject of international transportation according to these rules.

GENERAL

Responsibilities

102. The consignor and the consignee of a consignment of NATO classified material are responsible for jointly organizing and for submitting written transportation arrangements to their respective NSA/DSA for approval. They will mutually acknowledge, all full particulars regarding the transportation the latter should find necessary to require.

103. The responsible NSAs/DSAs will issue to the consignor and the consignee all official authorizations which must be in the possession of the security personnel.

104. The NSA/DSA of the consignor shall notify the NSA/DSA of the nation to be transitted of appropriate details of the transportation, including any cancellation thereof, with sufficient advance notice to enable the necessary security measures to be taken.

105. One single transportation plan may cover several consignments of similar material, provided the itinerary, the method of transmission and packaging remains the same, and the material transmitted is classified no higher than NATO SECRET and is related to the same NATO contract.

Customs

106. Customs authorities will be advised by the appropriate national authorities of impending consignments and should be urged to give maximum credence to the shipping documents in paragraph 108 and to the authorization carried by the security guard/courier. Consignments should not be opened unless there is a cogent reason for so doing. If a consignment is opened it is to be repacked and the customs authorities should be requested to reseal it and

(1) The general policy with regard to international transmission of NATO classified material up to and including NATO SECRET level is set out in Enclosure "C", paragraph 142. The provisions set out in this Section apply only to the industrial domain and only serve to complement this policy and make it more explicit, identifying the "other means" referred to in Enclosure "C".

endorse the shipping documents confirming that it was opened by these authorities. To facilitate customs clearance, advantage should be taken of TIR, TIF (1) or other similar arrangements.

107. Nothing in the previous paragraph or elsewhere in this Section should be construed to take effect as an abrogation by any nation of any of its rights of examination of any consignment.

Shipping Documents

108. All documents concerned with the transportation of material which accompany (but are not packed with) the material, including customs manifests, TIR carnets, bills of lading, receipts, etc. will provide the consignor with a normal 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 command or agency receiving the consignment.

109. These documents will be prepared by the consignor concerned. Documents will indicate that they sponsor a consignment of NATO classified material. Care will be exercised not to reveal any classified information in these documents. Quantities may be indicated. The consignee shall acknowledge receipt of the consignment by signature on the shipping documents. Such a signature will not imply any contractual acceptance of the consignment.

Packaging

110. The security officer of the consignor facility or agency is responsible for the supervision of packaging. Special cases requiring additional guidance should be discussed with the appropriate NSA/DSA. In no circumstances should the fact that the material is classified be apparent to any casual observer.

Security Measures Applicable to all Forms of Transport

111. The following principles will be enforced when examining proposals for the international transmission of consignments of NATO CONFIDENTIAL and NATO SECRET material:

(a) security must be assured at all stages during the transportation and under all circumstances. The possibility of delays, accidents or breakdowns must be taken into consideration. Provision must be made for reporting delays to the consignor and the consignee;

(b) the degree of protection accorded to a consignment will relate to the most highly classified part of it;

(c) an NFSC will be obtained for companies providing transportation services: in such cases, personnel handling the consignment will be cleared in compliance with the provisions of paragraph 84;

(d) containers shall bear no visible indication of their contents;

(e) journeys will be completed as quickly as circumstances permit;

(f) care will be exercised to arrange routes only through NATO nations and other states only when authorized by the NSA/DSA concerned;

(g) advance notification of each consignment will be made by the consignor and confirmed by the consignee through their respective NSA/DSA at least three working days in advance of the shipment. The shipment will not occur until the terms of the notification are accepted.

---

(1) TIR : Transport International Routier : International Transportation by Road;
TIF : Transport International Ferroviaire : International Transportation by Rail.

112. In the case of consignments of NATO RESTRICTED material, journeys should be completed as quickly as practicable and precautions taken to ensure that the material does not fall into the hands of unauthorized persons en route.

HAND CARRIAGE OF NATO CLASSIFIED MATERIAL

Transmission

113. When transmission through the channels stated in paragraph 142 of Enclosure "C" will result in an unacceptable delay that will adversely affect the performance of the project, programme or contract, and when it has been verified that the information is not available at the intended destination, personal carriage may be permitted provided that all the following provisions are complied with.

114. Participating governments may decide that material of a lower maximum classification level requires hand-carriage under these special arrangements.

Security Arrangements

115. Transmission of NATO classified material by persons other than couriers will comply with the provisions of paragraph 145 of Enclosure "C".

116. Moreover, the following conditions will be fulfilled:

(a) the procedure will be used on a case-by-case basis, subject to the approval by the NSAs/DSAs of the nations concerned;

(b) the material must have been authorized by the originating government for release in conjunction with the project, programme or contract; and

(c) the courier must be a permanent employee of the despatching or receiving company. Shipping agencies or independent couriers will not be used.

117. In exceptional circumstances, a nation may, with the previous agreement of the other NSA/DSA, consider issuing a courier certificate to a national of another NATO member nation with the appropriate NPSC, who is assigned to the organization and to whom NATO classified material relating to a common programme/contract will be entrusted.

118. Packaging instructions given at Enclosure "C", paragraph 134 will be applied.

119. The bearer will 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 shown at Annex IV.

120. The classified material will be given to the bearer in the appropriate sealed cover, against receipt; two copies of the receipt will be enclosed in the inner cover; one of them will be immediately returned to the consignor after having been dated and signed by the security officer of the consignee. The consignee will notify its NSA/DSA of any new classified material in his facility.

121. NATO RESTRICTED material will be transmitted by such means as are authorized by both the NSAs/DSAs concerned.

Procedure

122. When hand carriage of NATO classified material is permitted, the following procedures will apply:

(a) The courier will carry a courier certificate recognized by all NATO nations, authorizing him to carry the package as identified (see Annex V), stamped and signed by the NSA/DSA and by the consignor's security officer;

(b) A copy of the "Notes for the Courier" (see Appendix to Annex V) will be attached to the certificate; and

(c) The courier certificate will be returned to the issuing NSA/DSA through the consignor's security officer immediately after completion of the journey.

123. 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".

124. The courier will 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.

Customs

125. The courier will comply with official requests to open classified consignments by the customs authorities or other public officials. When inspection is unavoidable, it should be requested to be effected in an area away from persons who do not have a need-to-know and in the presence of the courier, who will ensure that only sufficient parts of the contents of the classified consignments are shown, to enable the officials to determine that it does not contain any items other than those declared.

126. In cases where the classified consignment is opened at the request of customs authorities, the courier will notify his company security officer, who in turn will notify his NSA/DSA.

127. Under no circumstances will the classified consignment be handed over to customs or other public officials for their custody.

128. Specific attention is drawn to the fact that the courier documents are only provided in order to have the journey carried out under secure conditions. It will not be used as an instrument to avoid legal obligations on the exportation, importation and transit of material subject to export/import laws and regulations. As such, the security procedures described will be completed in addition to all the administrative procedures needed for export of material.

TRANSMISSION OF CLASSIFIED MATERIAL AS FREIGHT

129. Priority must be given to the following transmission methods :

(a) diplomatic pouch service;

(b) military transportation; and

(c) security cleared courier, accompanied by a security escort when appropriate.

However, when, in the opinion of the NSAs/DSAs concerned, these services are unavailable or impractical to use, commercial carriers may be used.

130. The following procedures outline the minimum security requirements which will be met by the participating NSAs/DSAs when it is necessary to transmit consignments of NATO classified material as freight.

131. Prior to any international transportation the NSAs/DSAs of the consignor and of the consignee must agree on a transportation plan as described in Annex VI.

132. 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 transferred to the receiving NSA/DSA, or to the consignee, or to that NSA's/DSA's designated government representative. The official transfer may take place in either the despatching or receiving nation, as mutually agreed by the NSAs/DSAs. The security officer of the consignor/consignee may be appointed by the NSAs/DSAs as designated government representatative within the scope of national security regulations.

133. 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, who will be involved in ensuring the security of the shipment (see Annex VI).

134. As described in Appendix to Annex VI, the security officer of the consignor will provide a "Notice of Classified Consignment" to the security officer of the consignee and to the NSA/DSA of each nation involved. Copies of the Notice will be sent to other government or industrial entities, as appropriate.

Commercial Carriers

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

(a) hold an appropriate NFSC issued by the applicable NSA/DSA, if deemed necessary, and according to national security regulations;

(b) be authorized under laws or regulations of the nation where it operates to provide international transportation services;

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

Transportation by Road

136. The following minimum standards will be applied when consignments of NATO classified material are transmitted by road :

(a) material classified NATO CONFIDENTIAL and NATO SECRET will 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 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 unauthorized persons from gaining access;

(b) in cases where stops must be made, arrangements should 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;

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

(d) when the consignment is classified NATO SECRET, the driver or co-driver and the security guard must be security cleared to the classification level of the consignment; where no separate security guard is provided, both the driver and co-driver are to be so cleared, one of whom is to be the designated security guard. When the consignment is of material classified NATO CONFIDENTIAL or NATO RESTRICTED, the security guard's

duties may be undertaken by the driver or co-driver, in accordance with national regulations;

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

Transportation by Rail

137. Transportation by rail will be utilized for consignments of NATO CONFIDENTIAL and NATO SECRET material only in the following conditions :

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

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

138. With respect to the volume of the consignment, priority will be given to closed and sealable rail cars or containers, giving maximum security.

Transportation by Sea

139. The following minimum standards will be applied when consignments of NATO classified material are sent by sea :

(a) consignments of all classifications must only be carried in ships sailing under the flag of a NATO nation. The masters of such ships shall be nationals of a NATO nation;

(b) consignments of NATO CONFIDENTIAL and NATO SECRET material should be stowed in locked stowage space approved by the NSA/DSA agency; 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 disguised. In all cases, the consignment must be under security control;

(c) maritime countries presenting special security risks will be assessed by the NSA/DSA concerned in the light of the political environment, at the moment they receive the transportation proposals drawn up by the consignor and the consignee. Unless the ship is in extremis, it shall not enter the coastal waters of any of these countries, nor shall it call at any non-NATO port unless prior approval of the consignor's NSA/DSA has been obtained;

(d) in all cases, loading and unloading shall be carried out under security control;

(e) 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, however, this is unavoidable, sufficient security guards must be provided to keep the consignment under adequate supervision;

(f) where the consignment is of material classified NATO RESTRICTED or NATO CONFIDENTIAL, the security guard's duties may be carried out by the ship's master or specially designated crew member(s).

Transportation by Aircraft

140. Preference shall be given to the utilization of military aircraft of a NATO nation and the captain should be security cleared.

141. If utilization of a military aircraft of a NATO nation is not practicable, a commercial air carrier may be used, provided it is registered in a NATO nation and the captain is a NATO national, with the exception that Scandinavian Airlines System aircraft may be used, provided the captain is a NATO national.

142. When using flights between NATO member nations, the security guard's duties may be carried out by the captain of the aircraft or a designated crew member.

143. Consignments of material classified NATO SECRET by aircraft carrying freight may be authorized in exceptional circumstances. Where the presence of specially assigned security guards is not possible, these duties will be undertaken by the captain of the aircraft.

144. The following minimum standards will be observed:

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

(b) similarly, 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) during intermediate routine stops of short duration, the consignment shall remain in the aircraft but the aircraft itself shall be kept under security control;

(d) in the event of the aircraft being delayed at an intermediate stop, or having to make an emergency landing, it is the responsibility of the security guard, or the person fulfilling the duties of the security guard, to 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 will be assessed by the NSAs/DSAs concerned in the light of the political environment, at the moment they receive the transportation plan drawn up by the security officer of the consignor;

(f) no flight shall be permitted either over the designated countries or near enough to such countries as to make emergency landing or accidental over-flying possible;

(g) direct flights should be used wherever possible;

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

145. When the conditions outlined in paragraphs 146 and 147 are met, the requirements for a commercial air carrier to hold an NFSC do not apply.

146. The following conditions will be met for the transmission of classified material up to and including the level of NATO SECRET:

(a) the commercial air carrier will be responsible for the consignment while it is in the hold of the airplane, and will be cognizant of the security requirements, particularly the emergency procedures specified by the NSAs/DSAs;

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

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

(d) the NSAs/DSAs will provide to a requesting NSA/DSA written assurance that the commercial air carrier will comply with appropriate security measures designed to provide adequate protection to the classified consignment;

(e) consignments will be transmitted point-to-point, i.e. that the service provided by the commercial air carrier cannot be sub-contracted and intermediate stops are not permitted;

(f) flights over countries presenting special security risks will not be allowed without the written permission of the NSAs/DSAs;

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

(h) the NSA/DSA of the consignor is responsible for protecting any classified consignment transmitted under these procedures until such time as custody of the consignment is transferred to an individual approved by the NSA/DSA of the consignee as identified in an approved transportation arrangement;

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

147. Documents classified no higher than NATO CONFIDENTIAL may be transmitted using the procedures described in paragraph 146. NATO SECRET documents may only be transmitted by the methods listed at paragraph 129 or at paragraphs 140 to 143 inclusive.

SECURITY GUARDS

148. Persons 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. They must be nationals of NATO nations and be security cleared.

149. 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.

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

151. 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 should contact and other measures to be taken in the event of an emergency. Security guards should also be given a copy of "Notes for the Courier" (Appendix to Annex V) and be required to sign a receipt for it.

152. The NSAs/DSAs will issue in advance to the consignor (and, where applicable, the consignee) sufficient authorizations (Annex VII) so that they may be completed and issued to the security guards.

153. Both authorizations and "Notes for the Courier" will 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

154. If the classified material contains explosives, propellants or other dangerous substances, the transportation across international borders is subject not only to the security and customs requirements, but also to mandatory international and national safety regulations.

SECTION VI

INTERNATIONAL VISIT PROCEDURES

GENERAL

155. The arrangements described in this Section relate to international visits as defined in Section I. They accordingly apply to military and civilian representatives of NATO member nations, NATO contractors and sub-contractors, and personnel from NATO commands and agencies who need to visit on approved NATO-related activities :

(a) a government department or establishment of another NATO member nation;

(b) the facility of a contractor or sub-contractor of another NATO member nation;

(c) a NATO command or agency.

Visits (a) and (b) are approved by the NSA/DSA of the member nation in which the visit(s) will occur. This approval is assumed unless expressly denied by the NSA/DSA of that NATO member nation.

156. The approval by the NSA/DSA is subject to the following conditions :

(a) the visit has an official purpose related to NATO activities;

(b) the visitor(s) holds an appropriate NATO Personnel Security Clearance, and has a need-to-know for the information related to the NATO Project/Programme or activity;

(c) the facility to be visited has the appropriate NATO Facility Security Clearance.

157. Government departments, establishments, contractors, sub-contractors, NATO commands and agencies receiving visitors should ensure that :

(a) visitors meet the requirements of paragraph 156 above;

(b) visitors are given access only to NATO classified information related to the purpose of the visit;

(c) records are kept of all visitors, including their name, the organization they represent, the date(s) of the visit(s) and the name(s) of the person(s) visited. Such records are to be retained in accordance with national requirements.

158. Each NSA/DSA shall arrange for the government departments, establishments, contractors and sub-contractors which intend to send personnel on international visits, to submit to the host NSA/DSA, through the agreed official channels, an international visit request in accordance with the procedures stated in this section. The international visit request shall include an assurance/certification of NATO Personnel Security Clearance in respect of the visitors.

159. The NATO international visit procedures will normally be those defined in this Section. However, in the case of a specific project/program, when all NSAs/DSAs involved, in coordination with the responsible NATO Project Management Agency/Office, determine that these

general procedures would not be the best suitable for their specific requirements, they are authorised to establish other procedures, provided that these comply with the principles set out in this Section, and allow such authorities to obtain the same information and the same essential guarantees of security.

REQUIREMENTS AND PROCEDURES FOR VISITS

160. The procedures for NATO international visits are based on the use of the "Request for Visit" (RFV), as shown at Annex VIII, which is a standardised format for all kinds of visits.

161. The following types of visits will be taken into consideration :

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

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

(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.

162. Intended one-time and recurring visits will be initiated by means of a "RFV" sent by the visiting establishment or facility to the host facility or establishment through the NSAs/DSAs concerned.

163. A "RFV" will include such basic security information as is necessary to enable the NSA/DSA of the host NATO member nation to decide on the application. This will include :

(a) the identity of the visitors and the level of their NATO Personnel Security Clearance;

(b) the type of visit;

(c) the subject to be discussed and the anticipated level of classification of the matters to be discussed. The extent to which subject matters and level of classification will require to be detailed will vary with the type of visit, whether one-time or recurring;

(d) the government agency or industrial facility to be visited.

The way in which the RFV must be completed is provided at Annex VIII.

164. Annex IX sets forth the minimum number of working days prior to the date of a one-time visit, or the date of the first recurring visit, required by the receiving NSA/DSA, to process a RFV.

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

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

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

The leadtimes allowed are set out at Annex IX. 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.

166. Before receiving the visitor(s), the host facility will 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.

167. Requests for recurring visits will be valid for one year from the start date requested in the RFV. Recurring visits will be re-submitted for re-issuance annually. Superseded lists will be retained in accordance with national requirements.

168. 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.

SPECIAL ARRANGEMENTS FOR EMERGENCY VISITS

169. Unforeseen circumstances may occur which do not permit the use of standard visit request procedures. 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. To qualify as an emergency visit, one of the following conditions must 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 Project Management Agency/Office; or

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

170. Emergency visit requests will be critically reviewed, fully justified and documented by the Security Officer of the requesting government departments, establishments, contractors or sub-contractors. When the Security Officer is satisfied that the conditions cited in paragraph 167 have been met, he will contact a knowledgeable person at the government department, establishment, contractors or sub-contractors 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 departments, establishments, contractors or sub- sub-contractors to be visited (host facility) shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the government requesting the visit (requesting facility) and explain the reason for the emergency.

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

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

(b) the subject of the message will be :

EMERGENCY VISIT - Name of programme, 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, telephone and facsimile numbers of the person contacted pursuant to sub-paragraph (a) above, 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 any adverse 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.

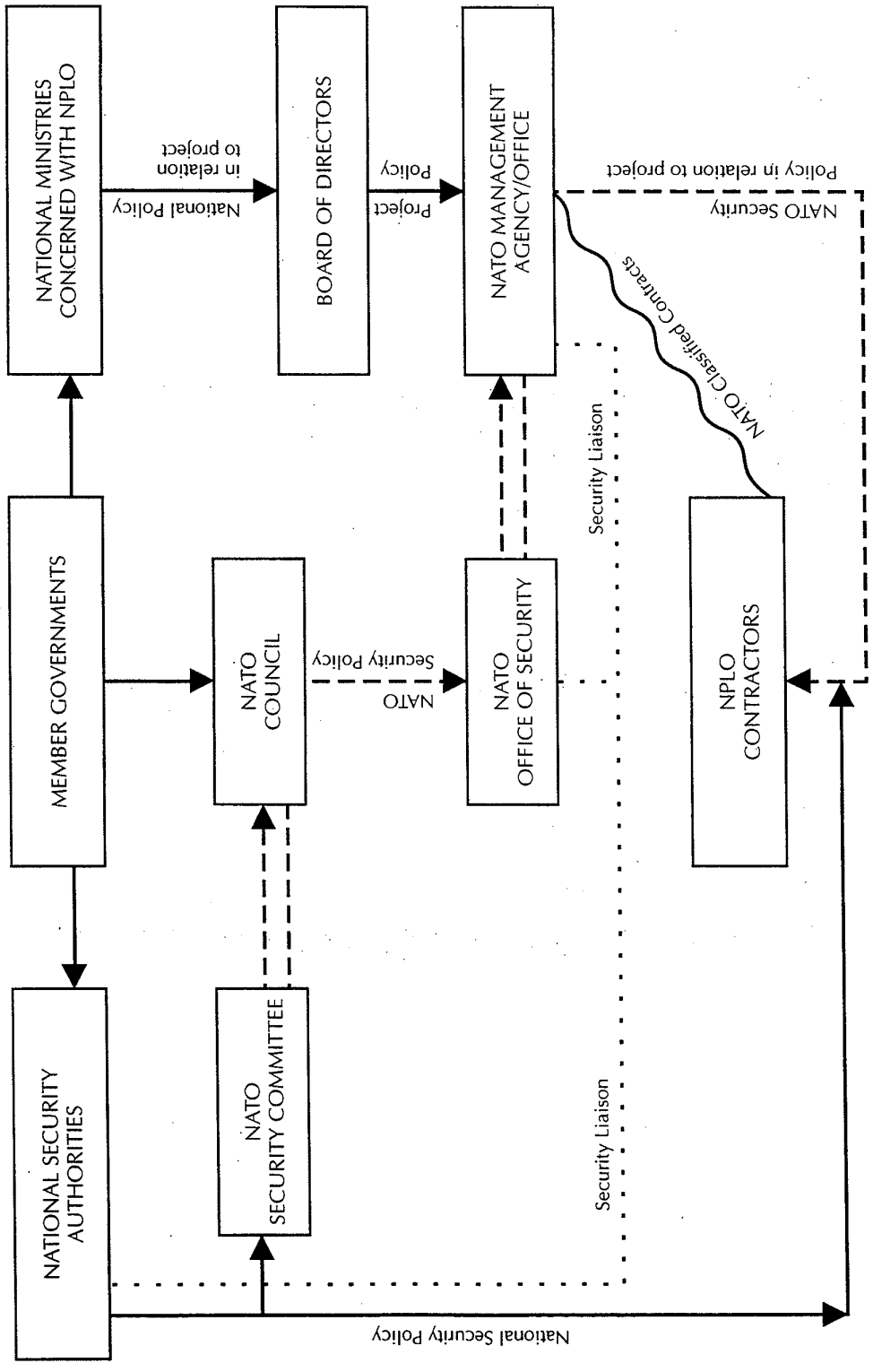
172. Emergency visit procedures shall not be used in lieu of standard visit request procedures. Therefore, each NATO member nation will establish guidelines to ensure compliance with these procedures. When it becomes apparent that the procedures are being abused by personnel of another NATO member nation,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

PERSONNEL ON LOAN WITHIN A NATO PROJECT/PROGRAMME

173. When a individual, who has been cleared for access to NATO classified information, is required to be loaned from one facility to another involved in the same NPLO programme but in a different country, the individual's parent facility will request its NSA/DSA to provide a NATO Personnel Security Clearance certificate for him to the NSA/DSA of the facility to which he is to be loaned. The person on loan will be assigned using the international visit process as described above, and in accordance with national regulations.

ANNEX I

DIAGRAM SHOWING SECURITY POLICY AND LIAISON LINKS IN RESPECT OF NATO PRODUCTION AND LOGISTICS ORGANIZATION PROJECTS



ANNEX II

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 provide on ..... (ddmmyy)
[x] provide the correct and complete information, if applicable

1. Full facility name :	/	corrections/additions :
.....	/	.....
2. Full facility address :	/	
.....	/	.....
3. Mailing address (if different from 2)	/	
.....	/	.....
4. Zip 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 :

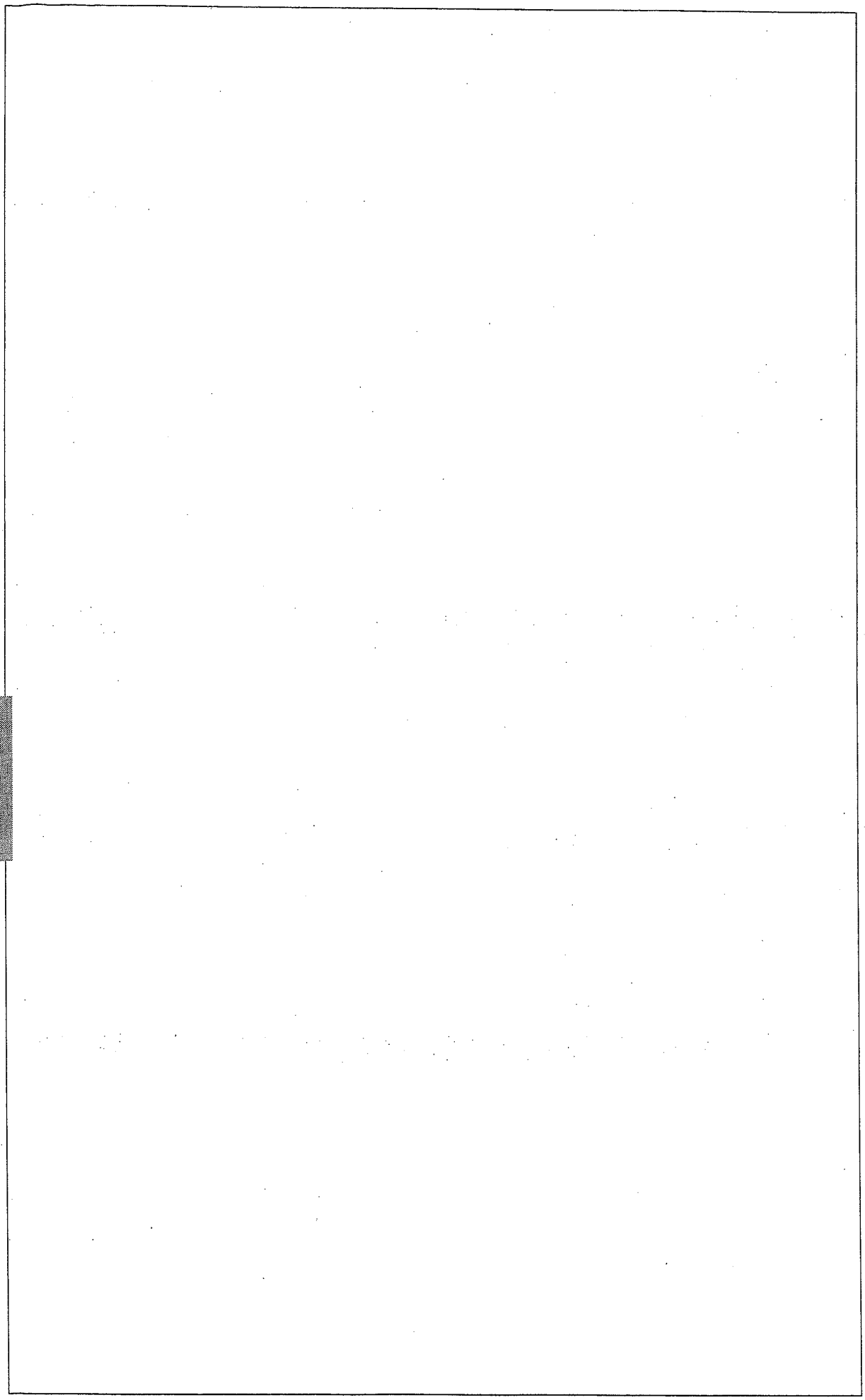
[ ] holds a FSC up to and including the level of : [ ] NS [ ] NC
[ ] does not hold a FSC.
[ ] does not hold a FSC but, on the above mentioned request, the FSC is in progress. You will be informed when the FSC has been established.
Expected date : ../.. (mmyy). (if known)

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 or 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 : .....

0216-97 - October 97



ANNEX III

NATO FACILITY SECURITY CLEARANCE CERTIFICAT (NFSC)

1. This is to certify that on ....., the National
(date)
Security Authority of .....

granted to the .....
(name of facility)
located at .....
(address of facility)

a NATO ..... security clearance in accordance with the
(classification)

provisions of paragraphs 73 & 74 of Enclosure "D" to
C-M(55)15(Final), 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

ANNEX IV

(LETTERHEAD)

SECURITY ACKNOWLEDGEMENT

DECLARATION

(name, forename)

of (**name of company**)

(position in company)

The Security Officer of the (**name of company/organization**) 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/organization, against receipt, to the designated consignee.

(place and date) **(signature of courier)**

Witnessed by: (**company Security Officer's signature**)

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

ANNEX V

(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 organization**)

is authorized 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 consignment 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-authorized persons or those having special permission.

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

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

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

ITINERARY

From: (**originating country**) .....

To: (**country of destination**).....

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

Authorized 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)

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

APPENDIX to ANNNEX V

(LETTERHEAD)

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

NOTES 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 obligations.

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;

   (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;

(*) may also be used by security guards.

(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 inquire 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 DSA's 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 :

.....

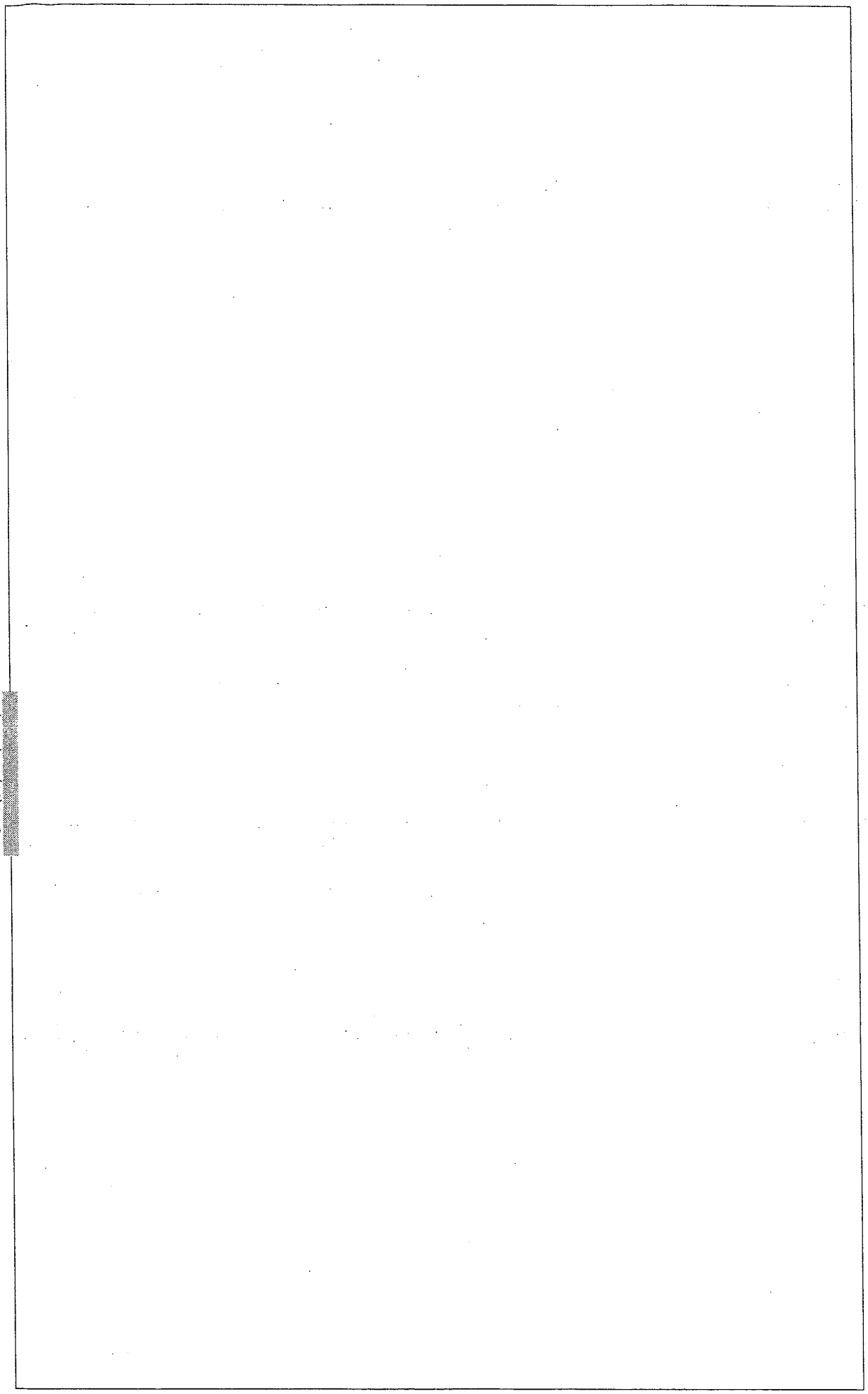
.....

.....

.....

.....

.....



ANNEX VI

(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 AUTHORIZED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organization, the authorized 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 repesentatives.

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.

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

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

(b) Describe specific security arrangements necessary to ensure the protection of the classi-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 coordination with customs and port security agencies may be required so that the Project/Programme movements will be recognized. 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 materials specified in Section V, 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 dispatcher of any known or suspected compromise of classified consignment or any other exigencies which may place the movement in jeopardy.

11. DETAILS OF CLASSIFIED MOVEMENTS

This section should contain 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 authorization 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 (Appendix 1); 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.

APPENDIX to ANNEX VI

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 authorized representatives, as applicable).

3. Description of Consignment :

   (a) contract or Tender Number;

   (b) export licence or other applicable export authorization 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);

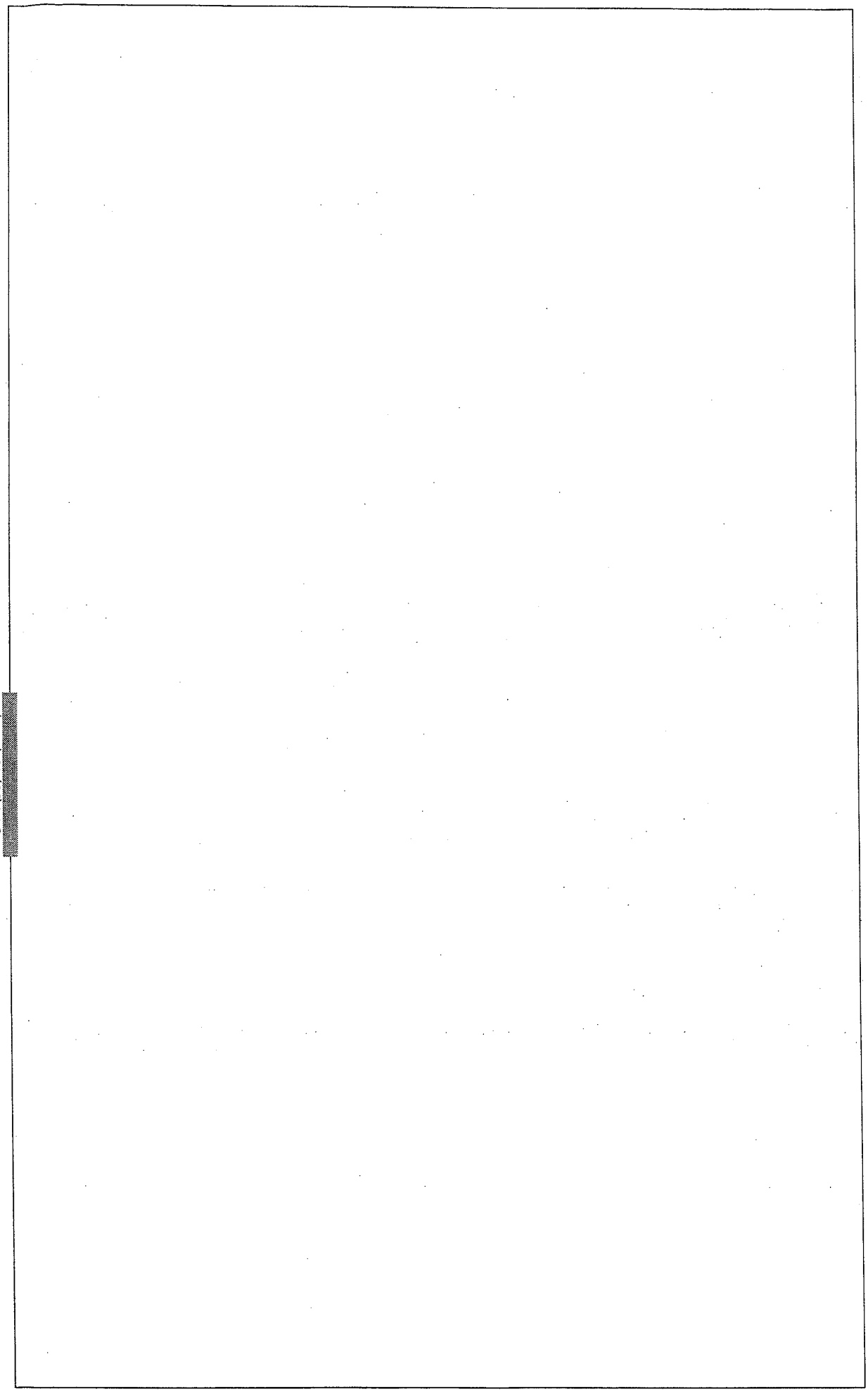
(d) method of transport for each portion of the shipment: (include names and addresses of all carriers and flight, rail or ship numbers, as applicable);

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

(Note: Shipper must reverify 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 authorized courier.



ANNEX VII

AUTHORIZATION FOR SECURITY GUARDS

Valid until .....

This is to certify that Mr. .....

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

.....

.....

holder of Passport No. ..... is authorized 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 Organization.

ITINERARY

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

Stamp of Firm/Establishment

Signature of Authorizing Official

Stamp of Government Agency

Signature of Authorizing Official

* Delete as applicable

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

ANNEX VIII

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

GENERAL INSTRUCTIONS

(a) The Request for Visit (RFV) (Appendix 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 for 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.

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

(3) In case of a manual application, Appendix 1 can be used. When two or more agencies or facilities have to be visited in the framework of the same subject, Appendix 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 alternate 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 organization (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, Appendix 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.

APPENDIX 1 to ANNEX VIII

One-time
Recurring

REQUEST FOR VISIT

Annex(es)
[ ] Yes : .....
[ ] No

ADMINISTRATIVE DATA

1. REQUESTOR :
   TO :
   DATE : . . ./. . ./. . .
   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	( )	

REQUEST FOR VISIT (continuation)

9. PARTICULARS FOR VISITORS

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

NAME :
DATE OF BIRTH : . . ./. . ./. . .
SECURITY CLEARANCE : ID/PP NUMBER : PLACE OF BIRTH :
POSITION : NATIONALITY :
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 :

SIGNATURE : (optional)

12. REQUESTING NATIONAL SECURITY AUTHORITY

NAME :
ADDRESS : STAMP

TELEPHONE :

SIGNATURE : (optional)

13. REMARKS

APPENDIX 2 to ANNEX VIII

REQUEST FOR VISIT

Reference : RFV - format, Item 3.

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

1. NAME :
   ADDRESS :

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

2. NAME :
   ADDRESS :

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

3. NAME :
   ADDRESS :

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

4. NAME :
   ADDRESS :

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

5. NAME :
   ADDRESS :

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

APPENDIX 3 to ANNEX VIII

REQUEST FOR VISIT

Reference : RFV - format, Item 9.

PARTICULARS OF VISITORS

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

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

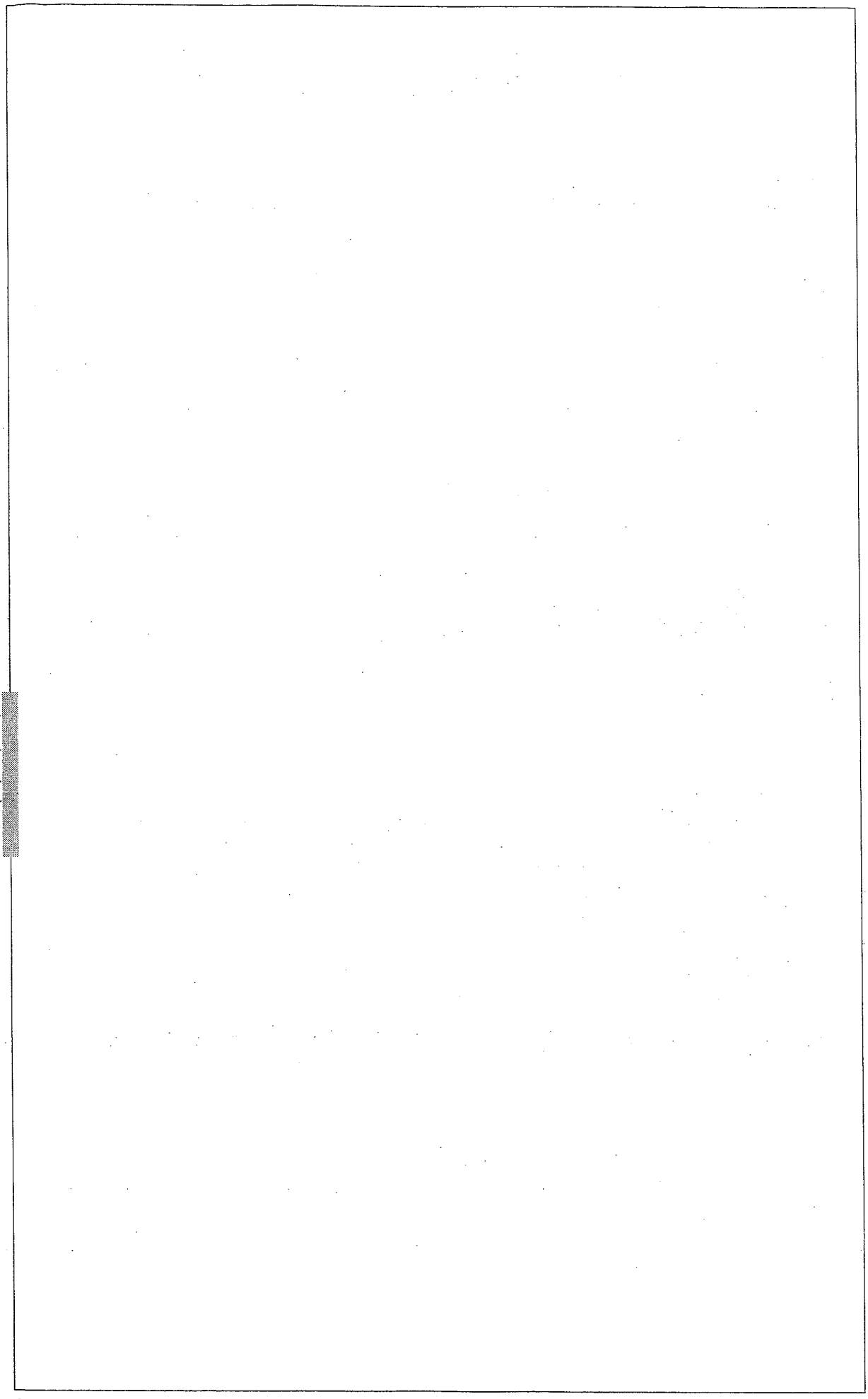
3. NAME :
   DATE OF BIRTH : . . ./. . ./. . . PLACE OF BIRTH :
   SECURITY CLEARANCE : ID/PP NUMBER : NATIONALITY :
   POSITION :
   COMPANY/AGENCY :

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

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

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

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



ANNEX IX

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
Belgium	BE	10	5
Canada	CA	20	-
Denmark	DE	15	-
France	FR	25	5
Germany	GE	20	7
Greece	GR	20	10
Italy	IT	20	7
Luxembourg	LU	10	5
Netherlands	NL	14	-
Norway	NO	21	-
Portugal	PO	-	-
Spain	SP	-	-
Turkey	TU	-	-
United Kingdom	UK	15	7
United States	US	21	-

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

NATO Management Agency / Office	NUMBER OF WORKING DAYS	
	Request	Changes
Central European Pipe Line Management Agency (CEPMA)	3	
NATO HAWK Management Office (NHMO)	7	
NATO EF2000 and Tornado Development, Production & Logistics Management Agency (NETMA)	3	
NATO Maintenance and Supply Agency (NAMSA)	3	
NATO Consultation, Command and 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 and Logistics Management Agency (NAHEMA)	3	

ANNEX X

FACILITIES LIST

From: (Letterhead of Management Office/Agency)

To: (Relevant NSA/DSA or NATO Command or Agency)

List of government departments, establishments, contractors and sub-contractors in (insert country) employed on NATO project (insert name) classified NATO .....

Serial Number	Facilities	Address Telephone/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. 0772-633333 Telex. 56789	YES (NATO SECRET)
2	.....	.....	.....

The Security Officer :

(Name) (Signature)

ANNEX XI

NATO AGENCIES, PROGRAMMES, PROJECTS AND PARTICIPATING NATIONS

NATO Agencies	Programmes and Projects
The Security Officer Central Europe Pipeline Management Agency (CEPMA) 11 bis rue Général Pershing, BP 552 78005 Versailles-Cedex, France Telephone : (33-1) 39 24 + extn. Telex : CEOA VERSAILLES (Transmission via NATO Military System only) Fax : (33-1) 47 38 57 90	Central Europe Pipeline System Programme (CEPS)
The Security Officer NATO HAWK Management Office (NHMO) 26 rue Galliéni 92500 Rueil-Malmaison, France Telephone : (33-1) 47 08 75 00 Telex : 203 378 Fax : (33-1) 47 52 10 99	HAWK Programme
The Security Officer NATO Helicopter for the 1990's Design and Development, Production and Logistics Management Agency (NAHEMA) Complexe Quatuor Route de Galice 13090 Aix-en-Provence, France Telephone : (33) 42 95 92 00 Fax : (33) 42 64 30 50	NATO Helicopter Programme
The Security Officer NATO Maintenance and Supply Agency (NAMSA) 8302 Capellen, Luxembourg Telephone : (352) 30 85 85 + extn. Telex : (402) 23 59 (Attention Security Office) Fax : (352) 30 87 21	Supply and Maintenance Management, Procurement and Technical Assistance Programme

NATO Agencies	Programmes and Projects
The Security Officer NATO Consultation Command and Control Agency (NC3A) Rue de Genève 8 1140 Brussels, Belgium Telephone : (32-2) 728 83 44 Telex : 25 931 Fax : (32-2) 728 87 70	NATO C3 Networks
The Security Officer NATO Airborne Early Warning and Control Programme Management Agency (NAPMA) Akerstraat 7 6445 CL Brunssum, The Netherlands Telephone : (31-45) 26 27 09 (from 1.10.95 : (31-455) 26 27 09 Fax : (31-45) 25 43 73 (from 1.10.95 : (31-455) 25 43 73	NATO Airborne Early Warning and Control System Programme
The Security Officer NATO EF 2000 and Tornado Development Production + Logistics Management Agency (NETMA) Inselkammerstrasse 12 & 14 82008 Unterhaching, Germany Telephone : (089) 66680-0 Telex : 529.361 Fax : (089) 66680555 & 66680556	European Fighter Aircraft Programme (EF2000)
The Security Officer NATO Air Command and Control System Agency (NACMA) 8 rue de Genève 1140 Brussels, Belgium Telephone : (32-2) 707 85 23 Fax : (32-2) 707 87 77	

Participating Nations	Programmes
Belgium, Canada, France, Germany, Luxembourg, Netherlands, United Kingdom, United States	CEPS
France, Italy	HAWK-TSQ-73
France, Germany, Italy, Netherlands	NAHEMA
Germany, Italy, United Kingdom	MRCA
Belgium, Canada, Denmark, France, Germany, Greece, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, United States	NAMSO

Belgium, Canada, Denmark, Germany, Greece, Italy, Luxembourg, Netherlands, Norway, Portugal, Turkey, United Kingdom, United States	NC3
Belgium, Canada, Denmark, Germany, Greece, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, United States	NAPMO
Germany, Italy, Spain, United Kingdom	EF2000
Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, United States	ACCS

ANNEX XII

NATIONAL AGENCIES AND MAJOR NATO COMMANDS CONCERNED WITH INTERNATIONAL VISIT CONTROL PROCEDURES

BELGIUM

Ministère de la défense nationale
Service Général du Renseignement et de la Sécurité
Section de Sécurité Industrielle (SGR/SI)
Quartier Reine Elisabeth
Rue d'Evere 1
B 1140 Brussels, Belgium
Telephone : (32-2) 701 46 28 or 69 34
Telex : 21 808
Fax : (32-2) 243 00 94

CANADA

Security Branch
Department of Supply and Services
10B3, Place du Portage, Phase III
11 Laurier Street
Hull, Quebec
K1A OS5
Telephone : (1-613) 953 36 23
Telex 053 37 03

DENMARK

Danish Defence Intelligence Service
Industrial Security Branch
Kastellet 30
DK 2100 Copenhagen OE
Telephone : (45) 33 32 55 66
Telex : 22 662 DENMARK

FRANCE

NSA (Policy and national regulations)
Secrétariat Général de la Défense Nationale
51 Boulevard de Latour-Maubourg
75700 Paris, France
Telephone : (33-1) 44 18 82 98
Telex : SEGEDEFNAT 20 00 19
Fax : (33-1) 44 18 83 48

FRANCE (continued)

DSA (implementation, except visits)
Délégation Générale pour l'Armement
Cabinet du Délégué/Bureau de sécurité
(DGA/CAB/BS)
14 rue Saint-Dominique
0457 Paris Armées, France
Telephone : (33-1) 45 52 47 54
Telex : 27 00 03 DEFNAT PARIS
Telegraphic address : DELEGARM PARIS
Fax : (33-1) 45 52 61 62

DSA (international visits)
Délégation Générale pour l'Armement
Délégation aux Relations Internationales
(DGA/DRI)
Sous-Direction du Contrôle du commerce des matériels de défense/Bureau des visites
14 rue Saint-Dominique
0457 Paris Armées, France
Telephone : (33-1) 40 25 41 63
Telex : 27 00 03 DELEGARM PARIS
Telegraphic address : DELEGARM PARIS
Fax : (33-1) 40 25 41 86

GERMANY

Bundesministerium für Wirtschaft
Referat ZS1
D-53107 Bonn, Germany
Telephone : (49)228 615-0 (switchboard)
615 2069(direct line)
Fax : (49) 228 615 4007

GREECE

Hellenic National Defence General Staff
B' Branch Security Section
(HNDGS- B' BRSEC)
Athens, Greece
Telephone : (30-1) 646 86 96
Fax: (30-1) 642 69 40

ITALY

Presidenza del Consiglio dei Ministry
Autorita Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti 216
00168 Roma, Italy
Telephone : (39-6) 627 47 14
Telex : 62 38 76 AQUILA I
Fax : (39-6) 614 33 97

LUXEMBOURG

Autorité nationale de sécurité OTAN
Ministère d'Etat
Bâtiment Vauban
Plateau du St. Esprit
L 1475 Luxembourg
Telephone :(352)478 22 10 (switchboard)
Telex : 3481 a SERET LU
Fax : (352) 478 22 43

NETHERLANDS

Netherlands Industrial Visit Control Office (NIVCO)
P.O. Box 20010
2500 EA The Hague, The Netherlands
Telephone : (31-70) 32 00 331/32 00 619
Telex : 32 166 SYTH N.L.
Fax : (31-70) 34 56 163/31 78 533

NORWAY

Headquarters Defence Command Norway
(HQ DEFCOMNOR)
Security Staff
Oslo Mil/Huseby
N 0016 Oslo 1, Norway
Telephone : (47) 22 49 80 80
Telex : 21 453 (during working hours)
Fax : (47) 22 49 80 44

PORTUGAL

Autoridade Nacional de Segurança
Ministerio da Defesa Nacional
Avenida Ilha da Madeira 1
1499 Lisboa Codex, Portugal
Telephone : (351-1)301 58 12
301 55 10
301 00 01
(ext.4377,4378,4257)
Fax : (351-1) 302 03 50

SPAIN

Director General del CESID
Avenida Padre Huidobro
(Carretera Nacional Radial VI, Km 8500)
Madrid 28023, Spain
Telephone : (34-1) 463 93 49
Telex : 41 361 ALIMA

TURKEY

(TCCD Turkish NATO Central Council Department, Ministry of Foreign Affairs Cukurambar - Balgat, Ankara, Turkey)
Kuzey Atlantik Andlasmasi Merkez
Kurulu Baskanligi, Disisleri Bakanligi
Cukurambar - Balgat, Ankara, Turkey
Telephone : (90-312) 287 17 90
Telex : 42 203 SFA - TR
(Please transmit to MGNA-II)

UNITED KINGDOM

(A) **Contractors Employees only**
International Visit Control Office
D MOD Sy 5C/IVCO
Room 2/3
Ministry of Defence
Whitehall
London SW1
Tel.: (44-171) 218 0130 (switchb.)

(B) **MOD Service & Civilian Personnel**
MOD Sy 1DR
Room 0302
Ministry of Defence
Main Building
Whitehall
London SW1
Tel.: (44-171) 218 9000 (switchb.)
218 7691 or 2703
(direct lines)

UNITED STATES

(A) (1) By electronic connection to the Foreign Visits System (FVS)
Policy Automation Directorate
Office of the Secretary of Defense (Policy)
Telephone : (1-703) 695 8935

(2) Hard copy to the appropriate organizations :

Army : Department of the Army
Office of the Deputy Chief of Staff for

UNITED STATES (continued)

Intelligence
Washington, DC 20310-1001
Telephone : (1-703) 695 8935

Navy : Department of the Navy
Navy International Programs
Office
1111 Jefferson Davis Highway
Arlington, VA 22202-1111
Telephone : (1-703) 603 0150

Air Force : Department of the Air Force
Attn. : SAF/IADV
Washington, DC 20330-1010
Telephone : (1-703) 695 6057

(B) All other DoD organizations :

DIA : Defense Intelligence Agency
Attn. : C-AS-1
Washington, DC 20301-6111
Telephone : (1-703) 694 3254

SACEUR

Supreme Headquarters Allied Powers Europe
(SHAPE)
Attention : Intelligence Division Plans Branch,
CI & Security Section
B 7010 SHAPE, Belgium
Telephone : (32-65) 44 71 11 (switchboard)
44 + extn.
Telex : 57 460

SACLANT

Supreme Allied Commander Atlantic
Attention : Security Officer
Norfolk
Virginia 23511, USA
Telephone : (1-804) 444 6042
444 6043
Telex : 82 36 16

ANNEX XIII

NATIONAL AGENCIES CONCERNED WITH INTERNATIONAL TRANSPORTATION OF NATO CLASSIFIED MATERIAL

BELGIUM

Ministère de la défense nationale
Service Général du Renseignement et de la Sécurité
Section de Sécurité Industrielle (SGR/SI)
Quartier Reine Elisabeth
Rue d'Evere 1
B 1140 Brussels, Belgium
Telephone : (32-2) 701 46 28 or 69 34
Telex : 21 808
Fax : (32-2) 243 00 94
FRANCE (continued)

CANADA

Security Branch
Department of Supply and Services
10B3, Place du Portage, Phase III
11 Laurier Street
Hull, Quebec
K1A OS5
Telephone : (1-613) 953 36 23
Telex 053 37 03

DENMARK

Danish Defence Intelligence Service
Industrial Security Branch
Kastellet 30
DK 2100 Copenhagen OE
Telephone : (45) 33 32 55 66
Telex : 22 662 DENMARK

FRANCE

NSA (Policy and national regulations)
Secrétariat Général de la Défense Nationale
51 Boulevard de Latour-Maubourg
75700 Paris, France
Telephone : (33-1) 44 18 82 98
Telex : SEGEDEFNAT 20 00 19
Fax : (33-1) 44 18 83 48

FRANCE (continued)

DSA (implementation, except visits)
Délégation Générale pour l'Armement
Cabinet du Délégué/Bureau de sécurité
(DGA/CAB/BS)
14 rue Saint-Dominique
0457 Paris Armées, France
Telephone : (33-1) 45 52 47 54
Telex : 27 00 03 DEFNAT PARIS
Telegraphic address : DELEGARM PARIS
Fax : (33-1) 45 52 61 62

DSA (international visits)
Délégation Générale pour l'Armement
Délégation aux Relations Internationales
(DGA/DRI)
Sous-Direction du Contrôle du commerce des matériels de défense/Bureau des visites
14 rue Saint-Dominique
0457 Paris Armées, France
Telephone : (33-1) 40 25 41 63
Telex : 27 00 03 DELEGARM PARIS
Telegraphic address : DELEGARM PARIS
Fax : (33-1) 40 25 41 86

GERMANY

Bundesministerium für Wirtschaft
Referat ZS2
D-53107 Bonn, Germany
Telephone : (49-228)615 0 (switchboard)
615 2523(direct line)
Telex : 88 67 74
Fax : (49-228) 615 2676

GREECE

Hellenic National Defence General Staff
B' Branch Security Section
(HNDGS- B' BRSEC)
Athens, Greece
Telephone : (30-1) 646 86 96
Fax: (30-1) 642 69 40

ENCLOSURE "D" to C-M (55) 15 (Final)

0216-97 - October 97

ITALY

Presidenza del Consiglio dei Ministry
Autorita Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti 216
00168 Roma, Italy
Telephone : (39-6) 627 47 14
Telex : 62 38 76 AQUILA I
Fax : (39-6) 614 33 97

LUXEMBOURG

Autorité nationale de sécurité OTAN
Ministäre d'Etat
Bâtiment Vauban
Plateau du St. Esprit
L 1475 Luxembourg
Telephone :(352)478 22 10 (switchboard)
Telex : 3481 a SERET LU
Fax : (352) 478 22 43

NETHERLANDS

Ministry of Interior
The National Security Service (BVD)
P.O. Box 20010
2500 EA The Hague, The Netherlands
Telephone : (31-70) 32 04 400
Telex : 32 166 SYTH NL
Fax : (31-70) 32 00 733

NORWAY

Headquarters Defence Command Norway
(HQ DEFCOMNOR)
Security Staff
Oslo Mil/Huseby
N 0016 Oslo 1, Norway
Telephone : (47) 22 49 80 80
Telex : 21 453 (during working hours)
Fax : (47) 22 49 80 44

PORTUGAL

Autoridade Nacional de Seguranáa
Ministerio da Defesa Nacional
Avenida Ilha da Madeira 1
1499 Lisboa Codex, Portugal
Telephone : (351-1)301 58 12
301 55 10
301 00 01
(ext.4377,4378,4257)
Fax : (351-1) 302 03 50

SPAIN

Director General del CESID
Avenida Padre Huidobro
(Carretera Nacional Radial VI, Km 8500)
Madrid 28023, Spain
Telephone : (34-1) 463 93 49
Telex : 41 361 ALIMA

TURKEY

(TCCD Turkish NATO Central Council Department, Ministry of Foreign Affairs Cukurambar - Balgat, Ankara, Turkey)
Kuzey Atlantik Andlasmasi Merkez
Kurulu Baskanligi, Disisleri Bakanligi
Cukurambar - Balgat, Ankara, Turkey
Telephone : (90-312) 287 17 90
Telex : 42 203 SFA - TR
(Please transmit to MGNA-II)

UNITED KINGDOM

D MOD Sy5b
Room 2/2
Ministry of Defence
Metropole Building
Northumberland Avenue
London WC2N 5BL
Tel.: (44-71) 218 9000 (switchb.)
218 4263 and 0125
(direct dialling)

UNITED STATES

DIS HQ
Attn. : Deputy Director
(Industrial Security)
1340 Braddock Place
Alexandria, VA 22314-1651
Telephone : (1-703) 325 6034/5494
Fax : (1-703) 325 1329/6033

TABLE OF CONTENTS ENCLOSURE "E"

SECURITY PROTECTION OF NATO COMMANDS AND AGENCIES

0216-97 - October 97

ENCLOSURE

SECURITY PROTECTION OF NATO COMMANDS AND AGENCIES

SECTION I

COUNTER-SABOTAGE MEASURES FOR NATO COMMANDS AND AGENCIES

INTRODUCTION

1. Paragraph 2(b) of Enclosure "B" states as a second principal objective of protective security the safeguarding of important installations from sabotage. Host nations are responsible for assessing all threats to NATO installations and for the latter's external protection.

2. Although NATO installations are not likely in normal peacetime conditions to be at risk from sabotage in the classic sense, they are nevertheless exposed to the same risks of damage to property, incapacity of personnel and loss of essential supplies and services as could result from sabotage attacks. These risks arise generally from a climate of increased violence and particularly from terrorists whose groupings, objectives and targets are so unpredictable as to make the success of conventional countermeasures by the host nation uncertain. NATO commands and agencies cannot, therefore, rely entirely on the protection afforded by the host nation but, with the latter, must plan for their own internal protection and preserve their ability to continue to function at the minimum level essential in various circumstances. Section II covers the terrorist threat and counter-terrorist measures for NATO commands and agencies and AC/35-D/1007(2nd revise) gives further general guidance.

RESPONSIBILITIES

Host Nations

3. Host nations are responsible for providing external protection to NATO commands and agencies. Whether this protection is rendered by national counter-intelligence services, law enforcing agencies or national defence forces is a host nation decision. When requested, host nations will specify to the head of a NATO command or agency those authorities with whom overall protective security plans should be co-ordinated and at what level. Host nations are also responsible whenever circumstances in their judgement so require for keeping the heads of NATO commands and agencies informed of the assessment of the threats from hostile intelligence services, subversive organizations, terrorist groups and the like.

NATO Commands and Agencies

4. The head of a NATO command or agency will determine in consultation, as necessary, with NATO and national authorities, those important installations under his jurisdiction, the whole or part of which are vital to the continuance of a function itself essential to the fulfilment of the primary NATO mission, bearing in mind the overall NATO objectives. The head of a NATO command or agency is responsible for planning internal security measures. Further, he will co-ordinate with the specified host nation authorities in the mutual interests of assuring that the internal and external plans are complementary.

0216-97 - October 97

ENCLOSURE "E" to C-M (55) 15 (Final)

5. Any intelligence or general information acquired by a NATO command or agency concerning threats to itself or to the host nation shall be transmitted promptly to the appropriate security authority of the host nation.

SCOPE OF SECURITY PROTECTION

6. Important installations require security protection to counter the assessed threats of damage or disruption. There will be other NATO installations where a lesser degree of protection will be necessary with the limited object of preserving fixed installations from damage whilst accepting that they will not be operational during emergencies.

7. Many of the protective measures needed to counter the assessed threats of damage or disruption will also be needed for the protection of NATO classified information. There will, however, be cases where security protection of installations is necessary even when no classified information is involved.

8. In the final analysis, the investments in money and manpower required for the adequate protection of an installation must be judiciously weighed against the operational and real estate value of the installation.

RISKS

9. The risks to NATO commands and agencies arising from the threats may be of three types:
   (a) physical damage;
   (b) denial of essential supplies and services;
   (c) incapacity of personnel due to injury, kidnapping or hostage-taking.

INTERNAL SECURITY PLANNING

Design of NATO Installations

10. The design of NATO installations must take into account security considerations and must include such material protection and emergency standby equipment as is considered necessary for:
   (a) essential operational functions to continue;
   (b) the preservation of valuable assets; and
   (c) the general safety of all personnel.

The Internal Security Plan

11. The security plan must first provide for the minimum and basic security protection required by an installation in normal peacetime conditions for safeguarding both its NATO classified information and its ability to function. To this basic security protection the security plan must add such additional protection as is deemed necessary in periods of crisis, periods of tension possibly leading to war, and in war. It follows that security planning through all stages must take account of all arrangements for peacetime and wartime conditions which may already have been made by NATO Authorities and the civil and military authorities of host nations.

12. Having decided what needs to be protected to what extent and under which conditions, the internal security plan should be drawn up in close consultation with the appropriate host nation authorities to provide defence in depth. Many internal protective measures will depend on the strengths or weaknesses of the complementary external measures taken by the host nation. Better protection is given by a number of co-ordinated and complementary measures than by placing complete reliance on any one type of defence.

13. The internal security plan must include, inter alia:

    (a) identification of the authority responsible for ordering various stages of the plan to be put into effect and of the officials responsible for implementing the specific measures listed in the plan;

    (b) designation of responsibilities for exercising command and control and for transferring them in the event of violent attack or occupation of NATO premises;

    (c) contingency arrangements for support and back-up forces;

    (d) a description of actions by NATO security forces on and off NATO premises permitted under the laws of the host nation;

    (e) alternative means of communication for security forces;

    (f) arrangements for evacuation of personnel; and

    (g) manning of alternate premises.

TRAINING

14. Having drawn up the internal security plan, NATO commands and agencies will train their staffs in their functions in differing circumstances by formal instruction and by exercises arranged, as appropriate, with the authorities of the host nation. Exercises should include alerting staff outside normal working hours. To ensure that the security plan can be implemented effectively when required, it is clearly essential that training should take place well in advance of an anticipated emergency.

INSPECTIONS

15. The validity of the internal security plan will be examined during NATO security inspections.

SECTION II

COUNTER-TERRORIST MEASURES FOR NATO COMMANDS AND AGENCIES

16. This Section lays down the policy for counter-terrorist measures for NATO commands and agencies and installations under their jurisdiction. Throughout this Section it is axiomatic that all measures implemented in pursuance of this policy must be in accordance with the legislation of the host nation concerned.

THE THREAT

17. The potential threat of terrorist activity against NATO commands and agencies and personnel assigned to NATO is from existing terrorist organizations, (which for the purposes of this paper includes groups and individuals) who might select NATO personnel or property as a target to publicise or advance their aims, and who operate both inside and outside NATO member nations. The threat of violence against NATO commands and agencies includes:

(a) bomb attacks, including car bombs, carrier bag type bombs, postal bombs and blast incendiary devices;

(b) assassination, abduction, holding as hostages, or intimidation of NATO staff members or their families;

(c) demonstrations which may be organized with violent intent or in regard of which there are clear indications that they may lead to violence through confrontation;

(d) direct attack on and occupation of NATO premises in the same way that has occurred with embassies and missions;

(e) hoaxes, particularly false bomb warnings, with intent to harass.

18. The specific threats vary among and within the NATO member countries and may also vary among personnel from different NATO member nations serving in the same Headquarters.

DIVISION OF RESPONSIBILITIES

The Host Nations

19. (a) Host nations are responsible for the external protection of NATO commands and agencies within their national territory and for providing them with a general assessment of the terrorist threat against them and for informing them whenever a specific threat arises. Nations will ensure, unless otherwise agreed, that information concerning threats, pertaining to NATO commands and agencies and their personnel located outside their respective territories, is passed on bilateral channels from nation to nation.

(b) Host nations will notify NATO commands and agencies of the specific additional counter-terrorist measures that they should plan and implement under different levels of threat.

(c) Host nations are responsible for providing such security personnel and protective security equipment for the protection of NATO personnel under terrorist threat outside the premises of NATO commands and agencies as are required in accordance with the host nation's national protective security standards and procedures. The designation of personnel to be considered under terrorist threat as well as the security measures to be put into effect for their protection are determined by the security authorities of the host nation, taking into account as well proposals with justification from interested NATO commands and agencies (among others).

(d) In respect of each NATO command or agency, on national territory, host nations will nominate points of contact for passing information on threat assessments and for co-ordinating internal security plans.

Parent (or Sending) Nations

20. (a) Parent nations will ensure that security considerations are taken into account when selecting residences for their personnel, utilising the expertise of host government security authorities. Expenditure by parent nations for physical security improvements will be confined to residences officially funded by them.

(b) The deployment of security personnel and the provision of protective security equipment by parent nations to counter any terrorist threat against their nationals must be co-ordinated with the host nation's security authorities and the NATO command or agency concerned.

(c) Parent nations will inform the host nation's security authorities and the NATO command or agency concerned of any specific threat existing against any of their nationals on the NATO staff or in national delegations, military representations or liaison missions co-located with the NATO command or agency.

NATO Commands and Agencies

21. NATO commands and agencies are responsible for planning and implementing counter-terrorist measures for the protection of their installations to include residences provided by NATO and all personnel located within their premises. Senior NATO personnel should be identified by NATO commands and agencies to host and parent nations. To achieve adequate and cost-effective arrangements NATO commands and agencies will:

(a) nominate their own point of contact for formal liaison via NATO approved channels with the appropriate host nation's security authorities via the latter's nominated points of contact (paragraph 19(d) above):

(i) for obtaining a general assessment of the terrorist threat;

(ii) for making arrangements for receiving and exchanging information regarding specific threats;

(iii) for co-ordinating counter-terrorist measures commensurate with the assessed threat; and

(iv) for the submission of proposals as in paragraph 19(c);

(b) maintain formal liaison via NATO approved channels with the security authorities of parent nations of senior NATO or national personnel for co-ordination of counter-terrorist measures in the event of a special threat existing:

(i) against such personnel from terrorist organizations operating in their parent nation; or

(ii) against citizens of a particular country;

(c) institute an alert system as described in paragraph 22 below and define responsibilities for implementing pre-planned measures to deal with the threat;

(d) institute procedures as required in paragraph 23 below for reporting and for informing host nations, parent nations, the NOS and other NATO commands and agencies regarding terrorist threats and incidents.

SECURITY PLANNING

Standard Alert System

22. A standard alert system will be instituted for all headquarters of NATO commands and agencies. This alert system will have four separate stages above normal and will contain basic minimum measures applicable throughout all NATO commands and agencies. The details regarding the alert system and the associated communications system and the basic minimum measures for each stage as well as other required or recommended measures will be developed and issued under the auspices of the NATO Security Committee.

Reporting of Terrorist Activities

23. Reports about terrorist threats or incidents by the various military or civil authorities will systematically specify:

    (a) the nature of the threat or incident;

    (b) the authority orginating the information;

    (c) the action taken.

    To avoid duplication of reports and to ensure adequate information of interested authorities, threats or actual terrorist incidents will be reported as specified below:

    (a) when information has been received from host nation security authorities, who will specify the protection that must be afforded to the source of information:

        (i) military commands will report the specific threat, or incident, the authority originating the information ("originator") and a summary of measures implemented to the next headquarters in the chain of command, with a copy to the NOS;

        (ii) civil agencies will report as in (i) above to the NOS;

    (b) when information originates within a NATO command or agency:

        (i) military commands will report the specific threat or incident and originator together with a summary of measures implemented to the host nation's security authorities in accordance with arrangements under 21(a) above, to the next headquarters in the chain of command and to the NOS;

        (ii) civil agencies will report as in (i) above to the host nation's security authorities and to the NOS.

Budgeting for Physical Protection and Other Protective Material

24. (a) NATO commands and agencies will request funds for physical protection of their premises (including official NATO residences) from the NATO military or civil budgets as appropriate. Budget requests will be supported by a threat assessment established by the host nation security authorities and by details of the specific aspects of the threat which would be countered by implementation of the physical measures requested;

    (b) requests for NATO funds for special communications systems to be used outside NATO premises as part of counter-terrorist measures will require a justification showing full co-ordination with host nation security authorities;

    (c) armoured vehicles provided by the NATO budgets will be restricted to the Secretary General and SACEUR. For emergency situations where a specific verifiable threat exists against which an armoured vehicle is considered imperative by the host nation security authorities and cannot be provided by the host nation or parent nation, the armoured vehicle may be rented from NATO funds, under procedures laid down in advance by the appropriate finance committees, for the duration of the threat;

    (d) other personal protective material such as bullet-proof clothing and special arms may be acquired from NATO funds in reasonable quantities for the use of NATO security personnel. Justifications for budget requests for such material must include a description of how this material will be used. NATO funds will not be authorized for the acquisition of personal protective materials for use by personnel not filling established NATO posts and only in exceptional cases will funds be approved for the acquisition of such material for use other than by NATO security personnel.

Security Personnel

25. NATO commands and agencies will consider counter-terrorist aspects when establishing or reviewing guard arrangements for their headquarters. Personnel for the personal protection of senior NATO officials should be maintained separately from other security forces, and their deployment must be co-ordinated with the host nation security authorities.

Co-ordination and Monitoring of Counter-Terrorist Arrangements

26. The NOS will assist in co-ordination between NATO commands/agencies and host nations/ parent nations on counter-terrorist matters and procedures. The NOS will also furnish technical assessments/justifications to the appropriate budget committees concerning construction work and equipment/material requested for counter-terrorist purposes.

27. Counter-terrorist arrangements and activities related to NATO commands and agencies will be monitored by the NOS. In this regard, the NOS will receive a copy of the general threat assessment applicable to each headquarters or group of headquarters. Commands and agencies will forward to the NOS two copies of their counter-terrorist plans. Special activities will be notified to the NOS through the reporting system described in paragraph 23 above.

28. Counter-terrorist arrangements will be subject to examination during the security inspection programme for NATO commands and agenies. The findings of these inspections will be included in the inspection reports.

ANNEX

NATO SECURITY ALERT STATES

INTRODUCTION

1. Information and warnings of terrorist activity against installations and personnel of NATO commands and agencies will normally be received from National Security Authorities through the security agencies of the host nations concerned. Information may also come from the local police forces and may be received directly by a NATO command or agency in the form of a threat or a warning from a terrorist organization and finally as an attack on a NATO installation or NATO personnel.

AIM

2. The aim of this instruction is to outline a common counter-terrorist alert system for NATO commands and agencies and the appropriate measures to be implemented corresponding to each alert state.

SECURITY ALERT STATES

3. The normal security arrangements for the protection of NATO sites, units and bases (including official residences, clubs, messes and domestic areas i.e. non-classified areas) are to be established in accordance with local standing orders. The introduction of the minimum measures outlined in the Alert States (Appendix) will reflect a higher state of security protection required to counter an increase of terrorist threat. Additional measures for each standard Alert State may be specified by host nations.

SECURITY ALERT STATES DEFINITIONS

4. The four security Alert States above normal are defined as follows:

(a) **Alert State ALPHA.**
This applies when there is a general threat of possible terrorist activity against NATO installations and personnel, the nature and extent of which are unpredictable and when the circumstances do not justify the full implementation of the measures of Alert State BRAVO. It may be necessary, however, to implement certain selected measures from State BRAVO, as a result of intelligence received, or as a deterrent. The measures in this Alert State must be capable of being maintained indefinitely.

(b) **Alert State BRAVO.**
This applies when there is an increased and more predictable threat of terrorist activity. It must be possible to maintain this state for a period of weeks without causing undue hardship, without affecting operational capability and without aggravating relations with local authorities.

(c) **Alert State CHARLIE.**
This applies when an incident occurs or when intelligence is received which indicates that some form of terrorist action against NATO installations and personnel is an imminent possibility. The implementation of this measure for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel.

(d) **Alert State DELTA.**
This applies in the immediate area where a terrorist attack has taken place or when intelligence has been received that terrorist action against a specific location or person is likely. Normally this Alert State is issued as a localised warning.

DECLARATION OF ALERT STATES AND IMPLEMENTATION OF MEASURES

5. The declaration of Alert States and the implementation of measures may be decreed by the host nation, by a NATO command or agency as a result of intelligence received, or by the local commander or head of agency following receipt of intelligence through official sources or following an anonymous threat message.

6. The Alert States may be suffixed with the geographical area deemed at risk. All unofficial information received should always be referred to the host nation security authority for authentication.

Weapons and ammunitions

7. Local orders are to include specific instructions concerning the issuing of weapons and the issuing of live ammunition to guard rooms and to sentries. These orders must comply with the policy of the host nation and of the NATO command and agency concerned.

IMPLEMENTATION AT INTEGRATED UNITS

8. The detailed measures to be adopted by NATO Headquarters at certain locations, where they share facilities with national formations, will need to be co-ordinated with the latter.

CLASSIFICATION OF ALERT STATES

9. The full definitions of the Alert States are NATO UNCLASSIFIED and may be used over non-secure telephone lines and in NATO UNCLASSIFIED signal messages (e.g. "Assume STATE CHARLIE"). This is a rapid way of passing initial information which can be followed up by an amplifying message whose classification would depend on the sensitivity of its contents (e.g. source protection).

APPENDIX to ANNEX

NATO SECURITY ALERT STATES - MINIMUM MEASURES

ALERT STATE ALPHA

1. This is issued as a general warning of possible terrorist activity, the nature and extent of which are unpredictable, and when the circumstances do not justify the full implementation of the measures contained in a higher Alert State. It may be necessary, however, to implement certain selected measures from Alert State BRAVO.

MEASURE 1.
All personnel, including dependents, are to be reminded at regular intervals to be suspicious and inquisitive about strangers, particularly if they are carrying suitcases or other containers; alert for unidentified vehicles on, or in the vicinity of, NATO installations; abandoned parcels or suitcases or any other unusual activity.

MEASURE 2.
The duty security officer, or other appointed officers, should be available at all times with access to plans for the evacuation of buildings and areas in use and for sealing off any areas where an explosion or attack has occurred. Key personnel who may be needed for the implementation of security plans should be on call.

MEASURE 3.
Buildings, rooms and cupboards not in regular use should be secured.

MEASURE 4.
Increase Security spot checks of vehicles and persons entering the installations and non-classified areas under the jurisdiction of the NATO command and agency are to be made.

MEASURE 5.
Limit access points for vehicles and personnel to a minimum commensurate with a reasonable flow of traffic.

MEASURE 6.
One of the following measures from State BRAVO should be applied individually and irregularly as a deterrent :

(a) All buildings, rooms and cupboards not in regular use are to be secured and inspected regularly. (Measure 14)

(b) The interior and exterior of buildings in regular use are to be inspected regularly and frequently for suspicious activity or packages. (Measure 15).

(c) All deliveries to clubs/messes are to be checked. (Dependents to be advised to do the same for deliveries at homes.) (Measure 17).

(d) As far as resources allow, surveillance of domestic accommodation, messes, schools, clubs and other soft targets should be increased to improve deterrence, defence and confidence amongst staff and dependents. (Measure 18).

MEASURE 7.
Review all plans, orders, personnel details and logistic requirements related to the introduction of the higher alert stages.

MEASURES 8-9
Spare.

ALERT STATE BRAVO

2. This is issued when there is an increased and more predictable threat of terrorist activity although no particular target has been identified.

MEASURE 10.
Measure 1 should be repeated and personnel warned of any other form of attack to be used by terrorists.

MEASURE 11.
All officers involved in implementing anti-terrorist contingency plans are to be on call.

MEASURE 12.
Plans for the implementation of the measures contained in the next alert stages are to be checked.

MEASURE 13.
Where possible, cars and such objects as crates, dustbins, etc., are to be moved to at least 25 m from buildings and particularly those buildings of a sensitive or prestige nature. Consider the application of centralized parking.

MEASURE 14.
All buildings, rooms and cupboards not in regular use are to be secured and inspected regularly.

MEASURE 15.
The inside and outside of buildings in regular use are to be inspected regularly and frequently for suspicious packages and always at the start of work and at close of work.

MEASURE 16.
All mail is to be positively examined for letter/parcel bombs.
(Increase checks above normal).

MEASURE 17.
All deliveries to messes, clubs, etc., are to be checked.
(Dependents to be advised to do the same for deliveries to their homes).

MEASURE 18.
As far as resources allow, surveillance of domestic accommodation, schools, messes, clubs and other soft targets should be increased to improve deterrence, defence and confidence amongst staff and dependents.

MEASURE 19.
Staff and dependents are to be made aware of the general situation in order to stop rumours and prevent alarm.

MEASURE 20.
Members of local security committees are to be informed, at an early stage, of any action being taken and why.

MEASURE 21.
Visitors to the unit and a percentage of their suitcases, parcels and other containers should be subjected to random check on entry.

MEASURE 22.
Wherever possible, random patrols should be operating, briefed to check vehicles, people and buildings.

MEASURE 23.
Personal and service transport off-base should be protected, in accordance with prepared plans. Drivers should be reminded to lock parked vehicles and institute a positive system of checking before they enter the car and drive.

MEASURES 24-29.
Spare

ALERT STATE CHARLIE

3. This applies when an incident occurs, or when intelligence is received which indicates that some form of terrorist action is an imminent possibility.

MEASURE 30.
All BRAVO Alert Measures are to continue or those outstanding are to be introduced.

MEASURE 31.
All officers who are responsible for implementing anti-terrorist plans are to be available on the place of duty.

MEASURE 32.
Limit access points to the absolute minimum.

MEASURE 33.
Control of entry is to be strictly enforced and a percentage search is to be made of vehicles.

MEASURE 34.
Centralized parking of vehicles away from sensitive buildings should be enforced.

MEASURE 35.
Weapons issued to guards. (Local orders should include specific instructions on issue of ammunition.)

MEASURE 36.
Increased patrolling of the installation should be introduced.

MEASURE 37.
All designated Vulnerable Points (VPs) are to be protected and special attention is to be given to VPs which are not installed inside military establishments.

MEASURE 38.
Erect ramps and chicanes to control vehicles.

MEASURE 39.
Spare.

ALERT STATE DELTA

4. This measure applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally this alert stage is issued as a localised warning.

MEASURE 40.
All measures as listed for Alert Stages BRAVO and CHARLIE are to continue or are to be introduced.

MEASURE 41.
Guards are to be augmented, as necessary.

MEASURE 42.
All vehicles already in the installation are to be identified.

MEASURE 43.
All vehicles and their contents entering the complex or installation are to be searched.

MEASURE 44.
All access is to be controlled.

MEASURE 45.
All suitcases, briefcases, packages, etc., brought into the complex or installation are to be searched.

MEASURE 46.
Measures are to be taken to control access to all areas under the jurisdiction of the NATO command or agency concerned.

MEASURE 47.
Frequent checks are to be made of the exterior of buildings and car parking areas.

MEASURE 48.
Minimize all administrative journeys and visits.

MEASURE 49.
Consult local authorities with a view to the closing of public (and military) roads which might make sites vulnerable to terrorist attack.

MEASURE 50.
Spare.

INDEX

ENCLOSURES "A", "B", "C", "D", "E" AND THE SUPPLEMENT

Note : In this Index, the references given are to paragraphs, preceded by the letters A, B, C, D and E representing the appropriate Enclosures, with cross-references to the Index of The Supplement (S)

0216-97 - Oct. 97

C-M (55) 15 (Final)

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

TABLE OF CONTENTS THE SUPPLEMENT

0216-97 - October 97

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

SUPPLEMENTAL SECURITY PRINCIPLES AND PRACTICES

1. The security principles and practices set forth in this document are supplemental to those contained in the NATO document C-M(55)15(Final). They have received the approval of the North Atlantic Council.

SECTION I

PERSONNEL SECURITY

SECURITY CLEARANCES

2. Access to NATO classified information[1] will be granted only to those individuals whose duties require such access and who have been investigated and cleared for access in accordance with the standards prescribed in Section II. Before granting access to classified information, a responsible authority of the government will make a security determination of eligibility for each individual.

3. When persons are employed in circumstances in which they may have access to classified information (e.g. security guards, messengers, maintenance personnel, etc.) consideration must be given to their first being appropriately security cleared.

4. On initial appointment to NATO, security clearances for personnel seconded from either the armed forces or the civil services of member nations, will not be older than five years from the date on which the last investigative action made in respect of them was completed; that is to say, the interval of time between the date of the last investigative action and the date of the appointment will not exceed five years. On initial appointment to NATO of personnel who are not seconded from the armed forces or civil services of member nations, the security clearance will not be older than nine months from the date of the last investigative action. (In both cases the date of expiry appearing on the certificate will in no case be more than five years from the date of the last investigative action).

---

[1] As set forth in the footnote to paragraph 1 of Enclosure "C" to C-M(55)15(Final), the words "classified information" mean:

(a) information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

(b) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

(c) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

0216-97 - Oct. 97

5. After the issue of the initial security clearance certificate and provided that the individual has unbroken service with NATO, the certificate will be reviewed for revalidation at intervals not exceeding five years with effect from the date of the investigative action on which that certificate was based. The revalidation of a clearance at the COSMIC TOP SECRET level shall be in accordance with the normal review procedures of the NATO member nation concerned which may include an interview with the individual. The review must include a check by the parent National Security Authority of all available records about the individual which are relevant to security. These records must include information received from the NATO command or agency concerned which that command or agency has obtained from its own records and enquiries (paragraph 14(b) refers) and, where applicable, from enquiries made by other National Security Authorities (paragraph 14(e) refers).. When an applicant, who is not seconded from the armed forces or civil services, does not take up an appointment within nine months of the issue of the initial security clearance certificate or when a non-seconded staff member leaves the Organization and applies to re-join it morethan nine months after resignation, the clearance will be referred to the National Security Authority that issued it, for confirmation, after such further processing, if any, as national procedures require. When the relevant command or agency requests the individual's National Security Authority to re-examine the clearance, it will also pass details of the individual's temporary employment, if any, during the period under review.

6. The decision whether the granting of a clearance is clearly consistent with the interests of security will be a determination based upon all available information. Based upon such information a determination shall be made as to whether or not such an individual is of :

   (a) unquestioned loyalty; and

   (b) such character, habits and associations and discretion as to cast no doubt upon:

      (i) his/her trustworthiness in the handling of classified information or for employment in circumstances in which he/she may have access to classified information; or

      (ii) his/her suitability for regular unescorted access to installations containing NATO classified information.

   Section III describes the circumstances and character traits which may give rise to security risks.

7. NATO classified information shall not be disseminated or released to any person who is not a national of the member nation having custody of the information or to any person or place beyond control or jurisdiction of the member nation except in accordance with C-M(55)15(Final). A national of another member nation may be authorized access to classified information only after receipt of a written security clearance from the responsible authority of the individual's parent nation.

8. Where the needs of NATO cannot otherwise be served :

   (a) information classified up to and including NATO SECRET, relating to a specific task or project, may be released to a national of a non-NATO nation only when a NATO member nation has with satisfactory results, carried out, or caused to be carried out, a clearance procedure not less rigorous than that required for a national of a NATO nation, or has verified that he/she has been cleared in accordance with this requirement;

   (b) access to COSMIC TOP SECRET information by non-NATO nationals will be authorized only in the case of nationals of New Zealand and Australia serving in the armed forces of Canada or the United Kingdom as integrated members thereof. In the case of such nationals it will be incumbent upon the Canadian or the United Kingdom government to satisfy itself that the conditions in sub-paragraph (a) above are fulfilled.

9. Upon request, the National Security Authorities shall provide mutual assistance with regard to the security clearance procedure.

SECTION II

STANDARDS OF INVESTIGATION

10. The standards of investigation shall be in accordance with national investigative practices of the NATO member nations but in no case shall these standards be less than those prescribed in this section.

INVESTIGATIVE REQUIREMENTS

Clearance for access to COSMIC TOP SECRET

11. Clearance for access to COSMIC TOP SECRET information will be based upon a background investigation conducted by a governmental investigative agency and covering a sufficient period of the life span of the individual, normally at least the last ten years, or from the date of his eighteenth birthday, and in sufficient detail to provide assurance that the criteria in sub-paragraphs 6(a) and 6(b) above have been met.

Clearance for access to NATO SECRET and NATO CONFIDENTIAL

12. Clearance for access to NATO SECRET and NATO CONFIDENTIAL information will be based upon a national records check and an identity check as prescribed in 13(a) and 13(b) below. However, if information of the kind set out in Section III is developed during the records check, a background investigation will be conducted to the extent necessary to arrive at a reasonable determination in the case.

BACKGROUND INVESTIGATION

13. A background investigation will cover the following:

(a) **National Records Check** - A check will be made of national security and central criminal records, where these latter exist, or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability.

(b) **Birth Records and Check of Identity** - The individual's date and place of birth will be verified and his/her identity will be checked.

(c) **Citizenship Status** - In all cases the citizenship status and/or nationality, present and past, of the individual will be established.

(d) **Education** - Investigation will normally cover attendance since the eighteenth birthday at schools, universities and other educational establishments.

(e) **Employment** - Investigations will cover present and former employment, reference being made to sources such as employment records, performance or efficiency reports and employers or supervisors.

(f) **Interviews** - Interviews will be held with persons who are in a position to give a true unbiased assessment of the individual's background, activities and trustworthiness. When it is the national practice to ask for referees, these will be interviewed unless there are good reasons for not doing so. Additional enquiries will be conducted to develop all information available on an individual and to substantiate or disprove derogatory information.

(g) **Records of Local Law Enforcement Agencies** - The records of law enforcement agencies in the vicinities where the individual has resided or been employed for substantial periods of time will be checked.

(h) **Military Service** - The service of the individual in the armed forces and type of discharge will be verified.

(i) **Foreign Connections** - The vulnerability to pressure from foreign sources, e.g. due to former residence or past associations will be ascertained whenever possible.

(j) **Credit Records** - Information should be sought about the credit standing and financial reputation of the individual.

(k) **Organizations** - During the course of the investigation, as set forth above, efforts will be made to determine if the individual has or has had membership in, or affiliation with, any foreign or domestic organization, association, movement, group or similar combination of persons which is subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights, or which seeks to alter the form of government of member nations by unconstitutional means.

REVALIDATION

14. Apart from the personal interview that may precede the revalidation of a COSMIC TOP SECRET clearance (paragraph 5 refers), an updated investigation for the purpose of renewing a COSMIC TOP SECRET clearance certificate within the terms of paragraph 4 above will cover the following :

(a) the completion of a personal particulars form by the staff member concerned. (The form may be either the NATO Supplementary Personal Particulars Form or a similar national form supplied by the relevant national authorities to the requesting NATO command or agency);

(b) a check of the personal particulars form against the security and personnel records held by the requesting NATO command or agency;

(c) the despatch by the requesting NATO command or agency of the completed personal particulars form mentioned at (a) above and of the results of the check required at (b) above to the parent National Security Authority concerned;

(d) consultation by the host nation of its national records at the request of the parent National Security Authority (or direct by the NATO command or agency if so authorized by the parent and host nation for the purpose of saving time);

(e) where applicable, consultations identical with those in (d) above by any other NATO nation in which the staff member has resided if so requested by the parent National Security Authority;

(f) where character references are required by member nations who have supplied their own Personal Particulars Form, such references will be taken up in consultation with the National Security Authority of the host nation;

(g) in the event that it is thought that a more detailed investigation is required, procedures foreseen for doing so will be implemented. These procedures may include, if considered useful, interviews with at least two persons who are in a position to give a true unbiased assessment of the individual's background, activities and trustworthiness;

(h) when the clearance of an individual serving abroad has to be revalidated more than once during uninterrupted expatriation, consideration should invariably be given to undertaking the detailed investigation referred to under (g) above;

(i) additional enquiries, where necessary, by the National Security Authority of the host nation on behalf of the parent nation arising from any information which may come to light as a result of the action under (b) and (d) to (h) inclusive above;

(j) the despatch by the National Security Authority of the host nation and of any other member nation in which the subject has resided, of any information developed within the terms of (b) and (d) to (i) inclusive above to the National Security Authority of the parent nation;

(k) a review by the parent nation against the background of its own records of any information which has been sent to it within the terms of (j) above;

(l) the despatch of the parent nation's decision, with regard to the renewal of the security clearance certificate, to the requesting NATO command or agency.

15. For revalidation of NATO SECRET and NATO CONFIDENTIAL clearances, the procedures outlined at sub-paragraphs 14(a) to (e) above will, as a minimum, be carried out. The parent nation will then review against the background of its own records any information arising during the course of these records checks and despatch its decision to the requesting NATO command or agency.

SECTION III

SUITABILITY FOR SECURITY CLEARANCE

16. The following paragraphs, although not exhaustive, contain the principal criteria for assessing the trustworthiness of an individual to hold security clearance, especially at the higher levels. These paragraphs consider aspects of circumstances and character which may give rise to security risks. Although the criteria apply to the individual being cleared, a spouse's or cohabitant's ideology, character and conduct and circumstances may also be relevant and should be taken into account when considering an individual's suitability for clearance.

THE INDIVIDUAL (INCLUDING HIS/HER SPOUSE OR COHABITANT)

17. The factors to be taken into account are whether the individual :

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of persons reasonably suspected of being such or an associate of representatives of organizations or foreign nations which are inimical to the security of the member nations unless these associations were authorized in the course of official duty;

(c) advocates or seeks, or is, or has been, a member of any organization which advocates or seeks the overthrow of the government of the member nations, or a change in the form of government of the member nations by violent, subversive or other unlawful means;

(d) is, or has recently been, an active supporter of any organization described in sub-paragraph (c) above, or who is, or who has recently been closely associated with members of such organizations in such a way as to raise reasonable doubts about the subject's reliability.

THE INDIVIDUAL

18. The factors to be taken into account are whether the individual :

(a) has deliberately withheld, misrepresented or falsified information of security significance, or has deliberately lied during the course of a security interview;

(b) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; has serious financial difficulties; is addicted to the use of alcohol to excess, or to the use of drugs; is or has been involved in conduct, including promiscuous sexual conduct or any other form of sexual misconduct, which gives rise to the risk that the subject may be susceptible to blackmail or pressure; has demonstrated by act or speech, consistent unreliability, dishonesty, untrustworthiness or indiscretion; has grossly infringed security regulations;

(c) is suffering, or has suffered, from any illness or mental condition which may cause significant defects in his or her judgement or may make the individual, unintentionally, a security risk. In all such cases competent medical advice should be sought;

(d) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services whose interests are inimical to the security interests of the Alliance and/or member nations.

INDEX[1]

[1] This index relates to the Supplement only.

0216-97 - Oct. 97