NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

5 December 2006

DOCUMENT
C-M(2002)49-COR3

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION

Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 3

1. Council has approved text[1] with respect to the following :

   (a) the updated responsibilities of the NATO Office of Security;

   (b) NATO classified contracting involving non-NATO nations;

   (c) release procedures for NATO classified information; and

   (d) partners' integration into NATO civil and military bodies.

2. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosures "B", "C", "D", "E" and "G" and destroy the old ones.

3. This amendment bears serial number 3. Holders of C-M(2002)49 are therefore requested to strike out number 3 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annexes : Enclosure "B"
Enclosure "C"
Enclosure "D"
Enclosure "E"
Enclosure "G"

Original: English

[1] C-M(2006)0112

ENCLOSURE "B" to
C-M(2002)49

ENCLOSURE "B"

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

INTRODUCTION

1. This C-M establishes the basic principles and minimum standards of security to be applied by NATO nations and NATO civil and military bodies in order to ensure that a common degree of protection is given to classified information exchanged among the parties. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics set out in this Enclosure. This Enclosure also addresses security responsibilities in NATO.

AIMS AND OBJECTIVES

2. NATO nations and NATO civil and military bodies shall ensure that the basic principles and minimum standards of security set forth in this C-M are applied to safeguard classified information from loss of confidentiality, integrity and availability.

3. NATO nations and NATO civil and military bodies shall establish security programmes that meet these basic principles and minimum standards to ensure a common degree of protection for classified information.

APPLICABILITY

4. These basic principles and minimum standards shall be applied to:

(a) classified information originated by NATO, originated by a member nation and submitted to NATO or submitted by a member nation to another member nation in support of a NATO programme, project or contract;

(b) classified information received by NATO from non-NATO sources; and

(c) classified information entrusted to individuals and organisations outside a government (or a NATO civil or military body), e.g., consultants, industry, universities, which shall protect it according to the same standards applied by the government or NATO civil or military body.

5. Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information – C-M(64)39. The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding ATOMAL Information – the current version of C-M(68)41 – shall be applied to control access to, to handle and protect such information.

6. Access to, and protection of, US-SIOP information are subject to the provisions of C-M(71)27(Revised), "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO".

7. The sensitive nature of cryptographic information, measures, and products requires the application of stringent security precautions, often beyond those set forth in this C-M. Therefore, access to, and protection of, cryptographic information, measures and products that are nationally- or NAMILCOM-approved, shall be in accordance with Enclosure “F”, supporting directives and procedures established by the appropriate authority.

8. The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this C-M. Therefore, access to and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 101 (NATO Signals Intelligence : Policy and Directive).

AUTHORITY

9. The North Atlantic Council (NAC) has approved this document which implements the Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (reproduced at Enclosure “A”), and thereby establishes NATO Security Policy.

BASIC PRINCIPLES

10. The following basic principles shall apply :

(a) NATO nations and NATO civil and military bodies shall ensure that the agreed minimum standards set forth in this C-M are applied to ensure a common degree of protection for classified information exchanged among the parties;

(b) classified information shall be disseminated solely on the basis of the principle of need-to-know to individuals who have been briefed on the relevant security procedures; in addition, only security cleared individuals shall have access to information classified CONFIDENTIAL and above;

(c) security risk management shall be mandatory within NATO civil and military bodies. Its application within NATO nations shall be optional;

(d) classified information shall be safeguarded by a balanced set of security measures, including personnel, physical, security of information and INFOSEC, which shall extend to all individuals having access to classified information, all media-carrying information, and to all premises containing such information;

(e) all suspected breaches of security shall be reported immediately to the appropriate security authority. Reports shall be evaluated by appropriate officials to assess the resulting damage to NATO and to take appropriate action. Enclosure “E” provides details;

(f) originators release classified information to NATO and to NATO nations in support of a NATO programme, project or contract on the understanding that it will be managed and protected in accordance with the NATO Information Management Policy (NIMP) and NATO Security Policy;

(g) classified information shall be subject to originator control;

(h) the release of classified information shall be in accordance with the requirements of Enclosure “E” to this C-M, and supporting directives; and

(i) subject to the consent of the originator and in accordance with Enclosure “E” to this C-M, NATO classified information shall only be released to non-NATO nations and organisations that have either signed a Security Agreement with NATO or that have provided a Security Assurance to NATO, either directly or through the NATO nation or NATO civil or military body sponsoring the release. In all cases, a degree of protection, no less stringent than that specified in this C-M, shall be required for any NATO classified information released.

11. The foundations of sound national security are :

(a) a security organisation responsible for :

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

(ii) the centralisation of such information so that it can be applied to any situation relating to the employment of individuals in government departments and agencies and by contractors; and

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

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

(i) identify classified information that needs to be protected; and

(ii) establish and apply common degrees of protection as set forth in this C-M.

Personnel Security

12. Personnel security procedures shall be designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorised to have initial and continued access to classified information without constituting an unacceptable risk to security. All individuals, civilian and military, who require access to, or whose duties or functions may afford access to information classified CONFIDENTIAL or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know.

13. A security clearance is not required for access to RESTRICTED information; individuals shall be briefed about their responsibilities for the protection of RESTRICTED information.

14. Personnel security is addressed further at Enclosure “C” of this C-M and in the supporting personnel security directive.

Physical Security

15. Physical security is the application of physical protective measures to sites, buildings or facilities that contain information requiring protection against loss or compromise. Physical security programmes, consisting of active and passive security measures, shall be established to provide levels of physical security consistent with the threat, security classification and quantity of the information to be protected.

16. Physical security is addressed further at Enclosure “D” of this C-M and in the supporting physical security directive.

Security of Information

17. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of information. Classified information shall be protected throughout its life cycle to a level commensurate with its level of classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary.

18. Security classifications shall be applied to information to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorised disclosure. NATO security classifications shall be applied in accordance with Enclosure “E” to this C-M. It is the prerogative of the originator of the information to determine or modify the security classification.

19. NATO security classifications and their significance are :

(a) COSMIC TOP SECRET (CTS) – unauthorised disclosure would result in exceptionally grave damage to NATO;

(b) NATO SECRET (NS) – unauthorised disclosure would result in grave damage to NATO;

(c) NATO CONFIDENTIAL (NC) – unauthorised disclosure would be damaging to NATO; and

(d) NATO RESTRICTED (NR) – unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

20. When classifying information, the originator shall take account of the damage if the information is subjected to unauthorised disclosure, and shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.

21. NATO UNCLASSIFIED information – policy and procedures for the management and protection of non-classified information marked NATO UNCLASSIFIED are contained in the NATO Information Management Policy (NIMP).

22. Security of Information is addressed further at Enclosure “E” of this C-M and in the supporting security of information directive.

INFOSEC

23. INFOSEC is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. In order to achieve the security objectives of confidentiality, integrity and availability for classified information stored, processed or transmitted in communication, information and other electronic systems, a balanced set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented to create a secure environment in which to operate a communication, information or other electronic system.

24. INFOSEC is addressed further at Enclosure “F” of this C-M and in supporting INFOSEC Management and INFOSEC Technical and Implementation directives.

Industrial Security

25. Industrial security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information handled by industry in contracts. NATO classified information disseminated to industry**,** generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance with NATO Security Policy and supporting directives.

26. Before a facility or its employees, managers or owners can have access to classified information or be invited to bid, negotiate or perform on a classified contract or work on a classified study involving access to information classified CONFIDENTIAL or above, the facility shall be granted a facility security clearance issued by the National Security Authority (NSA) (or, if appropriate, the Designated Security Authority (DSA)) of its nation of origin, that is to say, the nation in which the facility is located and incorporated to do business.

27. Facilities shall be required to protect classified information in accordance with the basic principles and minimum standards contained in this C-M. NSAs shall ensure that they have the means to make their industrial security requirements binding upon industry and that they have the right to inspect and approve the measures taken in industry for the protection of classified information.

28. Industrial security is addressed further at Enclosure “G” of this C-M and in the supporting industrial security directive.

PROTECTION OF INFORMATION ON KEY POINTS

29. The publication of information about civilian installations (defence supplies, energy supply, etc.) of military significance in times of tension or war may assist bombing, sabotage or terrorist attack by allowing potential enemies to compile a key points list, and to identify points vulnerable to sabotage or terrorism within individual key points. Policy should be designed to hamper the compilation by potential enemies of a Key Points List, to allow the invocation of security exemptions from publication of relevant data, and to encourage awareness of the risks among installation owners and operators.

SECURITY RESPONSIBILITIES

National Security Authority (NSA)

30. Each member nation shall establish a National Security Authority (NSA) responsible for the security of NATO classified information.

31. The 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) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organisations 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 organisations holding CTS or ATOMAL information, security inspections shall be made at least every 18 months, unless, during that period, they are carried out by the NOS;

(c) ensuring that a security determination of eligibility has been made in respect of all nationals who are required to have access to information classified NC and above, in accordance with NATO Security Policy;

(d) ensuring that such national emergency security plans as are necessary to prevent NATO classified information from falling into unauthorised or hostile hands have been prepared; and

(e) authorising the establishment (or dis-establishment) of national Cosmic Central Registries. The establishment (or dis-establishment) of Cosmic Central Registries shall be notified to the NOS.

Designated Security Authority (DSA)

32. Each member nation may designate one or more DSAs responsible to the NSA. In this case the DSA of a NATO nation is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some nations, the functions of a DSA may be carried out by the NSA.

NATO Security Committee (NSC)

33. The NSC is established by the NAC and is composed of representatives from each member nation's National Security Authorities (NSAs) supported, where required, by additional member nation security staff. Representatives of the International Military Staff, Strategic Commands and NATO C3 Board shall be present at the meetings of the NSC. Representatives of NATO civil and military bodies may also be present when matters of interest to them are addressed.

34. The NSC is responsible directly to the NAC for :

(a) reviewing NATO Security Policy (as set forth in C-M(2002)49 and C-M(2002)50) and making recommendations for change / endorsement to the NAC;

(b) examining questions concerning NATO Security Policy;

(c) reviewing and approving the supporting directives and guidance documents published by the NSC in the areas of personnel security, physical security, security of information, industrial security and INFOSEC (Note. a nation may request that a supporting directive also be approved by the NAC); and

(d) considering security matters referred to it by the NAC, a member nation, the Secretary General, the Military Committee, the NATO C3 Board or the heads of NATO civil and military bodies and preparing appropriate recommendations thereon.

NATO Office of Security (NOS)

35. The NOS is established within the NATO International Staff. It is composed of personnel experienced in security matters in both military and civil spheres. The Office maintains close liaison with the NSA of each member nation, and with NATO civil and military bodies. The Office may also, as required, request member nations and NATO civil and military bodies 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 NSC.

36. The NOS is responsible for :

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

(b) identifying means whereby NATO security might be improved;

(c) the overall co-ordination of security for NATO among member nations and NATO civil and military bodies;

(d) ensuring the implementation of NATO security decisions, including the provision of such advice as may be requested by member nations and NATO civil and military bodies either in their application of the basic principles and the standards of security described in this Enclosure, or in the implementation of the specific security requirements;

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

(f) carrying out periodic surveys of security systems for the protection of NATO classified information in member nations, NATO civil bodies, and SHAPE and SACT;

(g) carrying out periodic surveys of security systems for the protection of released NATO classified information in non-NATO nations and international organisations with whom NATO has signed a Security Agreement;

(h) co-ordinating, with NSAs and NATO civil and military bodies, the investigation into cases of lost, compromised or possibly compromised NATO classified information;

(i) informing NSAs of any adverse information which comes to light concerning their nationals;

(j) devising security measures for the protection of the NATO Headquarters, Brussels and ensuring their correct implementation; and

(k) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the NAC 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 and supporting Administrative Arrangements referenced at paragraph 5 above.

NATO Military Committee and NATO Military Bodies

37. 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 including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO classified information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure “F”. In accordance with previously agreed policy and in compliance with its Terms of Reference in paragraph 35 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

38. The Heads of NATO military bodies established under the aegis of the NAMILCOM are responsible for all security matters within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 18 months, unless, during that period, an inspection has been carried out by the NOS.

NATO Civil Bodies

39. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 18 months, unless, during that period, an inspection has been carried out by the NOS.

INFOSEC

40. Principal organisations with responsibilities for INFOSEC (for example, the NC3B, NCSAs and NDAs) are described in Enclosure "F".

SECURITY CO-ORDINATION

41. Any NATO security problem necessitating co-ordination between NSAs of member nations, and NATO civil and military bodies, shall be referred to the NATO Office of Security (NOS). In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences arising in the course of such co-ordination shall be submitted by the NOS to the NATO Security Committee (NSC) for consideration.

42. Any proposals by member nations and NATO civil and military bodies involving modification of NATO security procedures shall be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. If the NATO security problems giving rise to such proposals cannot be resolved except by modification of NATO Security Policy, the proposals shall be referred to the NSC, and if necessary, by it to the NAC.

ENCLOSURE "C" to
C-M(2002)49

ENCLOSURE "C"

PERSONNEL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for personnel security. Amplifying details are found in the supporting directive on personnel security.

2. There shall be an agreed standard of confidence about the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, NATO classified information. All individuals, civilian and military, whose duties require access to information classified NC and above shall be sufficiently investigated to give a satisfactory level of confidence as to their eligibility for access to such information.

3. Individuals authorised to have access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC), granted by their NSA or other competent authority, valid for the duration of the authorised access, and have a need-to-know. The extent of security clearance procedures shall be determined by the classification of the NATO information to which the individual is to have access. Security clearance procedures shall be in accordance with NATO security policy and supporting directives.

4. Individuals who require access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC) , shall have been briefed on NATO security procedures, shall have acknowledged their responsibilities, and shall have a need-to-know. Individuals who require access to only information classified NR shall have been briefed on their security responsibilities, and shall have a need-to-know. Unless specifically required by national security rules and regulations, a security clearance is not required for access to information classified NR.

5. The granting of a PSC should not be considered as a final step in the personnel security process; there is a requirement to ensure an individual's continuing eligibility for access to NATO classified information. This should be achieved through continuous evaluation by security authorities and managers; and through security education and awareness programmes which remind individuals of their security responsibilities and of the need to report, to their managers or security staffs, information which may affect their security status.

APPLICATION OF THE "NEED TO KNOW" PRINCIPLE

6. Individuals in NATO nations and in NATO civil and military bodies shall only have access to NATO classified information for which they have a need-to-know. No individual is entitled solely by virtue of rank or appointment or PSC to have access to NATO classified information.

PERSONNEL SECURITY CLEARANCES (PSCs)

Responsibilities

7. The PSC responsibilities of NSAs, or other competent national authorities, NATO nations and the Heads of a NATO civil or military body are set out in the supporting personnel security directive.

8. Individuals shall be made aware of their responsibilities to comply with security regulations, and act in the interests of security.

Personnel Security Directive

9. The supporting personnel security directive sets out the following :

(a) the requirements for identifying positions requiring an appropriate PSC;

(b) the criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC;

(c) the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET clearances;

(d) the requirements for the provision of PSCs for employees of NATO civil and military bodies;

(e) the requirements for revalidation of PSCs;

(f) the procedures for addressing adverse information about an individual holding a PSC; and

(g) the requirements for maintaining records of PSCs granted to individuals.

SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS

10. All individuals employed in positions where they have access to NR information, or hold a clearance for access to NC or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand

their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO nation or NATO civil or military body authorising access to NATO classified information.

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

AUTHORISING ACCESS TO NATO CLASSIFIED INFORMATION

ACCESS BY NATO NATIONALS

12. An individual shall only be authorised access to NATO classified information after he has been granted the appropriate personnel security clearance, a determination of his need-to-know has been made, and he has been briefed on NATO security procedures and has acknowledged his security obligations.

Exceptional Circumstances

13. However, circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 12 above cannot be met. Details in respect to provisional appointments, one-time access, emergency access, and attendance at conferences and meetings are set out in the supporting personnel security directive.

ACCESS BY NON-NATO NATIONALS

14. Non-NATO nationals serving as integrated members of the Armed Forces of NATO member nations may be authorised access up to and including information classified CTS. In the case of such nationals it shall be incumbent upon the NSA to satisfy itself that the conditions for access stipulated in paragraphs 12 or 13 above are fulfilled.

15. Individuals who are nationals[1] of non-NATO nations may be granted access to NATO classified information on a case-by-case basis, provided that :

1 Nationals of non-NATO nations includes "nationals of a Kingdom", "citizens of a State", and "landed immigrants in Canada". "Landed immigrants in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

(a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;

(b) the individual is granted a NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives; noting that a NATO PSC is not required for access to NR information;

(c) the prior written consent of the NATO nation or NATO civil or military body that originated the information is obtained; and

(d) the non-NATO individual in question shall have clearly understood and undertaken, by means of personally undersigning an acknowledgement of responsibilities, that NATO information that he might have access to in the context of a specified NATO programme, project, contract, operation, or related task, shall strictly and solely be used for the purposes of the entrusted task and shall not be shared with or transmitted to third persons, bodies, organisations or governments.

16. As an exception to the requirement for originator control in sub-paragraph 15(c) above, NSAs of NATO nations may approve access to NATO classified information by nationals of certain non-NATO nations who are employed by the Government of the NATO nation, or by a contractor that is located and incorporated in the NATO nation, provided that, in addition to those criteria set out in sub-paragraphs 15(a), 15(b) and 15(d) above, the criteria set out in the equivalent section of the supporting personnel security directive are applied.

ENCLOSURE "D"

PHYSICAL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for physical security measures for the protection of NATO classified information. Amplifying details are found in the supporting directive on physical security.

2. NATO nations and NATO civil and military bodies shall establish physical security programmes that meet these minimum standards. Such programmes, which consist of active and passive security measures, shall provide a common degree of protection consistent with the security classification of the NATO information to be protected.

SECURITY REQUIREMENTS

3. All premises, buildings, offices, rooms, and other areas in which NATO classified information and material is stored and/or handled shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as:

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

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

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

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

(e) how the information will be stored.

4. Physical security measures shall be designed to:

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

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

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

(d) detect and act upon all security breaches as soon as possible.

PHYSICAL SECURITY MEASURES

5. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and INFOSEC measures, details of which will be found respectively in Enclosures "C", "E" and "F". Sensible management of security risks will involve establishing the most efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these areas. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

6. Physical security programmes shall be based on the principle of "defence in depth", and although physical security measures are site-specific, the following general principles shall apply. It is first necessary to identify the locations that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors. The outermost physical security measures shall define the protected area and deter unauthorised access. The next level of measures shall detect unauthorised or attempted access and alert the guard force. The innermost level of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

7. Regular maintenance of security systems is necessary to ensure that equipments operate at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important if there is a change in use of the site or elements of the security system. This can be achieved by exercising incident response plans.

Security Areas

8. Areas in which information classified NC and above is handled and stored shall be organised and structured so as to correspond to one of the following:

(a) **NATO Class I Security Area**: an area in which information classified NC and above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information. Such an area requires:

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

(ii) an entry control system which admits only those individuals appropriately cleared and specifically authorised 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) **NATO Class II Security Area**: an area in which information classified NC and above is handled and stored in such a way that it can be protected from access by unauthorised individuals by controls established internally. Such an area requires:

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

(ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

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

Administrative Zones

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

Access to NATO Class II Security Areas by Individuals from Non-NATO Nations / International Organisations

11. Individuals from non-NATO nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted unescorted access to a NATO Class II Security Area. Such individuals may also be assigned office space within a NATO Class II Security Area in order to fulfil their assignment and official duties. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis, and shall be in accordance with the criteria set out in the supporting Directive on Physical Security.

Specific Measures

12. The following measures are identified to indicate examples of physical security measures that can be implemented :

(a) perimeter fence - a perimeter fence will form a useful physical barrier and will identify the boundary of an area requiring security protection. The effectiveness of any security perimeter will depend, to a large extent, on the level of security at the points of access;

(b) intruder detection system (IDS) – IDS may be used on perimeters to enhance the level of security offered by the fence, or may be used in rooms and buildings in place of, or to assist, guards;

(c) control of access – control of access may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical;

(d) guards – the employment of appropriately cleared, trained and supervised guards can provide a valuable deterrent to individuals who might plan covert intrusion;

(e) closed circuit television (CCTV) - CCTV is a valuable aid to security guards in verifying incidents and IDS alarms on large sites or perimeters; and

(f) security lighting - security lighting can offer a high degree of deterrence to a potential intruder, in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system.

Entry and Exit Searches

13. NATO establishments shall undertake random entry and exit searches which are designed to act as a deterrent to the unauthorised introduction of material into, or the unauthorised removal of NATO classified information from a site or building.

Access Control

14. A pass or personal recognition system governing the regular staff shall control entry into Class I or II security areas. Visitors shall be permitted escorted or unescorted access to a NATO establishment based upon checks on the individual and their access requirements.

MINIMUM STANDARDS FOR THE STORAGE OF NATO CLASSIFIED INFORMATION

15. NATO classified information shall be stored only under conditions designed to deter and detect unauthorised access to the information.

16. **COSMIC TOP SECRET (CTS)**. CTS information shall be stored within a class I or II security area under one of the following conditions :

(a) in an IDS-equipped vault, or in a nationally-approved security container in an area which is subject to continuous protection or periodic inspection; or

(b) an IDS-protected open storage area constructed in accordance with the supporting physical security directive.

17. **NATO SECRET (NS).** NS information shall be stored within a class I or II security area under one of the following conditions :

(a) in the same manner as prescribed for CTS information; or

(b) in a nationally-approved security container or vault; or

(c) an open storage area, which is IDS-protected, or subject to continuous protection or periodic inspection.

18. **NATO CONFIDENTIAL (NC).** NC information shall be stored in the same manner as prescribed for CTS or NS information except that supplemental controls, as described in the supporting physical security directive, are not required.

19. **NATO RESTRICTED (NR).** NR information shall be stored in a locked container.

20. Amplifying details for the storage of NATO classified information are set out in the supporting directive on physical security.

PROTECTION AGAINST TECHNICAL ATTACKS

Eavesdropping

21. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be coordinated with technical specialists and decided by the appropriate security authority.

Technically Secure Areas

22. Areas to be protected against audio eavesdropping shall be designated as technically secure areas and entry to them shall be specially controlled. Rooms shall be locked and /or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas shall be subject to regular physical and/or technical inspections in accordance with the requirements of the appropriate security authority, and shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

PHYSICAL SECURITY FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

23. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for confidentiality, integrity and availability is met. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II security areas or the national equivalent. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

APPROVED EQUIPMENT

24. NSAs shall maintain lists of equipment which they or other NATO nations have approved for the protection of NATO classified information under various specified circumstances and conditions. NATO civil and military bodies shall ensure that any equipment purchased complies with the regulations of a NATO member nation(s).

OTHER PHYSICAL SECURITY MEASURES

25. Detailed requirements are set out in the supporting physical security directive, addressing, for example, rooms and locks, keys and combinations, and containers and locks.

ENCLOSURE "E" to
C-M(2002)49

ENCLOSURE "E"

SECURITY OF INFORMATION

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO classified information. Amplifying details are found in the supporting security of information directive.

2. NATO classified information requires protection throughout its life-cycle. It shall be managed to ensure that it is appropriately classified, clearly identified as classified information, and remains classified only for as long as this is necessary. Security of information measures shall be complemented by personnel, physical and INFOSEC safeguards to ensure a balanced set of measures for the protection of NATO classified information.

CLASSIFICATION and MARKINGS

General

3. The originator is responsible for determining the security classification and initial dissemination of information. The classification level of NATO information shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, originators shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.

4. The classification assigned determines the physical security given to the information in storage and transmission, its circulation, destruction and the personnel security clearance required for access. Therefore both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency.

5. NATO nations and NATO civil and military bodies shall introduce measures to ensure that information created by, or provided to NATO is assigned the correct security classification, and protected in accordance with the requirements of the supporting security of information directive.

6. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to

ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

7. The overall security classification of a document shall be at least as high as that of its most highly classified component. Component parts of documents classified NC and above shall, where possible, be classified (including by paragraph) by the originator to facilitate decisions on further dissemination of appropriate sections. Covering documents shall be marked with the security classification of the information contained therein when they are separated from the information they accompany.

8. When information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts. Original security classification caveats must be retained when information is used to prepare composite documents.

Qualifying Markings

9. The terms COSMIC and NATO are qualifying markings which, when applied to classified information, signify that the information shall be protected in accordance with NATO Security Policy.

Special Category Designators

10. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement and supporting Administrative Arrangements referenced in Enclosure "B", paragraph 5.

11. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with the reference cited in Enclosure "B", paragraph 6.

12. The term "CRYPTO" is a marking and a special category designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying NATO security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security instructions.

Dissemination Limitation Markings

13. As an additional marking to further limit the dissemination of NATO classified information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

Objectives of Accountability

14. The primary objective of accountability is to provide sufficient information to be able to investigate a deliberate or accidental compromise of accountable information and assess the damage arising from the compromise. The requirement for accountability serves to impose a discipline on the handling of, and control of access to, accountable information.

15. Subordinate objectives are :

(a) to keep track of access to accountable information – who has, or potentially has, had access to accountable information; and who has attempted to access accountable information;

(b) to know the location of accountable information; and

(c) to keep track of the movement of accountable information within the NATO and national domains.

16. CTS and NS and ATOMAL information shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting security of information directive. Where required by National rules and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

17. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single registry system, in which case strict compartmentalisation of CTS information shall be maintained at all times, or by establishing separate registries and control points.

18. Each NATO member nation and NATO civil or military body shall establish a Central Registry(s) for CTS, which acts as the main receiving and despatching authority for the nation or body within which it has been established. The Central Registry(s) may also act as a registry(s) for other accountable information.

19. Registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information and for keeping records of all accountable documents held on that registry's or control point's charge; they may be established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by National security rules and regulations.

20. With regard to NATO accountable information, registries and control points shall be able at all times to establish its location. Infrequent and temporary access to such information does not necessarily require the establishment of a registry or control point, provided procedures are in place to ensure that the information remains under the control of the Registry System.

21. The dissemination of information classified CTS shall be through COSMIC registry channels. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable, in accordance with the requirements of the supporting security of information directive. Regardless of the type of registry organisation, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

22. The supporting security of information directive sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for CTS and NS information, the procedures for reproductions, translations and extracts, the requirements for the dissemination of transmission of information, and the requirements for the disposal and destruction of information.

23. The NAMILCOM has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system do not require accountability in the Registry System.

CONTINGENCY PLANNING

24. NATO nations and NATO civil and military bodies shall prepare contingency plans for the protection or destruction, during emergency situations, of NATO classified information to prevent unauthorised access and disclosure and loss of availability. These plans shall give highest priority to the most sensitive, and mission- or time-critical information.

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

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

26. All breaches of security shall be reported immediately to the appropriate security authority. Each reported breach of security shall be investigated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the breach.

27. 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 minimising action taken shall be forwarded to the NOS.

28. When a compromise of NATO classified information has to be reported to the NOS, the report shall be forwarded through the NSA or the Head of the NATO civil or military body concerned. 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.

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

30. The supporting security of information directive sets out the detailed actions, records and reporting requirements for breaches and compromises of security.

31. Separate provisions relating to the compromise of cryptographic material have been issued by the NAMILCOM to communications security authorities of member nations and NATO civil and military bodies.

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND INTERNATIONAL ORGANISATIONS

Introduction

32. Classified information entrusted to or generated by NATO in order to enable it to perform its missions is disseminated and protected in accordance with NATO Security Policy, directives and procedures. This section sets out the policy for the release of NATO classified information to non-NATO nations and international organisations including such nations (hereinafter referred to as non-NATO recipients). This section also covers information contained in documents issued by the NAC, or by any other NATO committee or NATO civil or military body (hereinafter referred to as NATO bodies).

33. The release of NATO classified information to non-NATO recipients shall take place in the context of NATO cooperative activities approved by the NAC. Any request for the release of NATO classified information to non-NATO recipients outside such cooperative activities shall be examined and approved on a case-by-case basis.

34. ATOMAL information of any classification may not be released to any nation/organisation which is not a party to the current versions of C-M(64)39 and C-M(68)41.

Principles for Authorising the Release of NATO Classified Information to Non-NATO Nations and International Organisations

35. Authorisation to release shall always be subject to the consent of the originator(s). Additionally, the following shall apply :

(a) for NATO classified information to be released under NAC-approved NATO cooperative activities, where the non-NATO participants to that activity have been endorsed by the NAC on a case-by-case basis :

(i) release decisions can either concern clearly identified information or a general category of information;

(ii) the subject matter shall be included in the general work plan or the OPLAN for the activity or in the practical measures established for cooperation;

(iii) the release of NATO classified information shall be necessary to initiate cooperation on a specific subject, and to continue cooperation within the approved activity;

(iv) a Security Agreement, signed by the Secretary General on behalf of NATO and by a representative duly mandated[1] by the non-NATO recipient, shall have been concluded. In the absence of a Security Agreement and in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient, signed by a representative duly mandated[1] by the non-NATO recipient that any information received will be protected in accordance with its national laws and regulations and to a degree no less stringent than NATO minimum standards, shall have been provided to the NATO Office of Security;

(v) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities;

(vi) the Security Assurance provided by the non-NATO recipient shall also identify the NATO security classifications and the equivalent security classifications of the non-NATO recipient. The Security Assurance shall be forwarded to the relevant committee responsible for the approval of the release. Copies of the written Security Assurances shall be provided to the NATO Office of Security who shall maintain a database of Security Assurances;

1 A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

(vii) only information classified up to and including NC may be released through Security Assurances. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC, NS information may be released; and

(viii) where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release; and

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

(i) release decisions shall be taken on a case-by-case basis and can only concern clearly identified information;

(ii) a bilateral Security Agreement / Arrangement shall exist between the NATO member nation sponsoring the release and the non-NATO recipient;

(iii) the Sponsor shall be responsible for providing a written Security Assurance, signed by a representative duly mandated[2] by the non-NATO recipient, to NATO from the non-NATO recipient. The Security Assurance provided by the non-NATO recipient shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information. The NATO security classifications shall be identified with their equivalents to the national classifications cited in the bilateral Security Agreement / Arrangement;

(iv) the Sponsor shall forward this written Security Assurance to the relevant committee, together with the release request. Copies of written Security Assurances shall also be provided to the NATO Office of Security;

2 A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

(v) the request shall demonstrate the advantage which would accrue to NATO. Justifications for release shall be specific, avoiding general statements;

(vi) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities; and

(vii) only information classified up to and including NC may be released through Security Assurances in this case. Where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release.

Release Authority

36. 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, taking into account the principles for authorising the release identified in paragraph 35 above, to :

(a) the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it. For NR, the appropriate subject-matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to that committee;

(b) the NAMILCOM for information classified up to and including NS which has been originated by the NAMILCOM and/or bodies subordinate to it. For NR, the NAMILCOM may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to the NAMILCOM;

(c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET), under the following conditions :

(i) the information is limited to NATO classified information necessary for the effective participation of non-NATO Troop Contributing Nations (NNTCN) in operations and exercises, as approved on a case-by-case by the NAC;

(ii) the information to be released is only that NATO classified information originating from within Allied Command Operations (ACO) and is directly related to specific operations and exercises where the participation of non-NATO nations to that activity has also been endorsed by the NAC on a case-by-case basis; and

(iii) the ACO Security Authority (SHAPE J2) shall implement an authoritative and auditable process for the release of classified information;

(d) the Mission Commander for an operation involving non-NATO Troop Contributing Nations, as endorsed by the NAC, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR), under the following conditions :

(i) the information shall be related specifically to the Mission;

(ii) the information shall be limited to tactical information related to an ongoing operation and deemed necessary for the successful conduct of the ongoing operation;

(iii) the Mission Security Authority shall implement an authoritative and auditable process for the release of classified information; and

(iv) the NOS, in close co-ordination with SHAPE J2, reserves the right to conduct inspections of the security arrangements in place; and

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

37. Authority for release shall only be delegated to an appropriate subject-matter committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the appropriate subject-matter committee shall assume the responsibility of the originator. Authority for release may be delegated to the lowest committee level best suited to evaluate the importance of the classified information.

38. With the exceptions applying to NR information stated in paragraphs 36(a) and (b) above, delegated release authorities cannot further delegate their powers, although they can entrust subordinate bodies with the implementation of the release decision.

39. NATO civil and military bodies shall keep control records of information classified CONFIDENTIAL and above which they have released to non-NATO recipients. These records shall be subject to inspection by the appropriate NATO security authority (for example, NOS, SHAPE J2).

Administrative Arrangements for the Implementation of a Security Agreement

40. The completion of the administrative arrangements shall be confirmed by a security survey carried out by the NOS of the relevant agencies of the non-NATO recipient. The security survey shall establish the ability of the non-NATO recipient to comply with the provisions of the Security Agreement and with the minimum standards.

41. The NOS shall produce a report of the survey and transmit a copy to the Security Authority of the non-NATO recipient. The original report shall be filed in the NOS and made available, upon request, to NATO member nations. The NATO Security Committee shall be provided with a written summary of the results of the NOS survey. The conclusion drawn from the survey as to the ability of the non-NATO recipient to protect NATO classified information shall be communicated by the NOS to the relevant NATO bodies and to NATO member nations.

42. The NOS shall carry out periodic security surveys, at least once every two years, of the relevant agencies of the non-NATO recipients to ensure that the non-NATO recipient continues to be compliant with the provisions of the Security Agreement and with the minimum standards.

43. Where a Security Assurance has been provided to NATO in respect to the protection of released classified information, an annual re-validation of that Security Assurance shall be provided, as appropriate, in accordance with the assessed continued need to receive information. The NOS shall also assess whether or not it would be more appropriate to negotiate a Security Agreement in lieu of the Security Assurance. The NOS shall keep the record of validated Security Assurances, which shall also comprise the grounds for such re-validation. The NATO member nations, on request, shall be provided with a copy of this record.

Supporting Directive on the Security of Information

44. The supporting security of information directive contains, inter alia, the :

(a) procedures for the release of NATO classified information to non-NATO recipients;

(b) specific release procedures for NATO Production and Logistics Organisations (NPLOs), international organisations and Combined Joint Task Forces (CJTFs);

(c) minimum standards required for the handling and protection of NATO classified information released to non-NATO recipients. The minimum standards apply to any non-NATO recipient, regardless of whether a Security Agreement has been concluded with NATO or a Security Assurance provided to NATO;

(d) detailed administrative arrangements to be implemented by all non-NATO recipients; and

(e) samples of the Security Assurance, the Personnel Security Clearance Certificate and the Certificate of Security Clearance.

ENCLOSURE "G" to
C-M(2002)49

ENCLOSURE "G"

INDUSTRIAL SECURITY

INTRODUCTION

1. This Enclosure deals with security aspects of industrial operations that are unique to the negotiation and letting of NATO classified contracts and their performance by industry, including the release of NATO classified information during pre-contract negotiations. This Enclosure sets out the security policy for :

(a) the negotiation and the letting of NATO classified contracts;

(b) the security requirements for NATO classified contracts;

(c) the release of NATO classified information in contracting;

(d) Facility Security Clearances (FSCs) for NATO contracts;

(e) the international transportation of NATO classified material;

(f) international visits;

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

(h) NATO classified contracts involving non-NATO nations.

2. This Enclosure is supported by an industrial security directive which sets out the detailed requirements and procedures. The directive includes the requirements for the negotiation and letting of NATO classified contracts, the security requirements for NATO classified contracts, National authorities for granting FSCs and PSCs, the authorities for international transport, the authorities for international visits, a list of the various entities that typically are involved in NATO classified contracts, and their responsibilities, and a list of NATO Programmes/Projects, Participating Nations and NATO Agencies.

NEGOTIATION AND LETTING OF NATO CLASSIFIED CONTRACTS

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme / Project Agency / Office (NPA/NPO). A FSC shall be required for all

contractors involved in contracts classified NC and above. For contracts classified NR, a FSC is not required unless specifically required by National security rules and regulations.

4. The NPA/NPO who negotiates the contract shall ensure that, for contracts classified NC and above, contractor representatives involved in the negotiations hold appropriate Personal Security Clearance (PSC), and only receive access to NATO classified information needed for the negotiation of the contract.

5. After a prime contract has been let, a prime contractor may negotiate sub-contracts with other contractors, i.e., sub-contractors. These sub-contractors may also negotiate sub-contracts with other sub-contractors. If a potential sub-contractor is located and incorporated in a non-NATO nation permission to negotiate a sub-contract shall be obtained from the NPA/NPO (c.f. Enclosure "E", paragraphs 29-33). If the NPA/NPO has placed restrictions on the award of contracts to NATO-nations that are not participants in a programme/project, the NPA/NPO shall give permission prior to contract discussion with contractors from those nations.

6. Upon letting the prime contract, the NPA/NPO shall notify the NSA/DSA of the prime contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime contractor, with the contract (see paragraphs 8 and 9, below).

SECURITY REQUIREMENTS FOR NATO CLASSIFIED CONTRACTS

7. The prime contractor and sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for safeguarding all NATO classified information generated by or entrusted to the contractor, or embodied in articles manufactured by the contractor.

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

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

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

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

11. The release of NATO classified information shall be with the consent of the originator and in accordance with other applicable enclosures to the NATO Security Policy and the supporting industrial security directive.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

12. The policy described in subsequent paragraphs for facilities and individuals apply to contracts or sub-contracts.

Facility Security Clearances (FSC)

13. The NSA/DSA of each NATO nation is responsible for ensuring that any facility located and incorporated in that nation which will require access to information classified NC and above in order to enter into pre-contractual negotiations or bid on a NATO classified contract, has adopted the protective security measures necessary to qualify for a FSC. Moreover, the facility's employees who require access to NATO classified information shall have been properly cleared and briefed before furnishing a Facility Security Clearance Certificate (FSCC). The clearances shall be based upon the classification level of the information, its volume and nature, and the number of individuals who will require access to it in the course of preparing bids or negotiations.

14. A contractor may participate in pre-contractual negotiations, bid on, or perform on a NATO classified contract provided the NSA/DSA of the nation in which the contractor is located and incorporated to do business has given the contractor facility the requisite level of FSC.

15. The assessment to be made prior to issuing a FSC shall be in accordance with the requirements and criteria set out in the supporting industrial security directive.

16. Lack of a FSC, or PSCs for facility employees, shall not prevent the contractor bidding for a contract or sub-contract classified NR. A nation which, under its National security rules and regulations, requires a FSC for a contract or sub-contract classified NR shall not discriminate against a contractor from a nation not requiring a FSC, but shall ensure that the contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

17. The issuing of PSCs shall be in accordance with Enclosure "C", Personnel Security, to NATO Security Policy, and the supporting personnel and industrial security directives.

18. Applications for the security clearance for employees of contractor facilities shall be made to the NSA/DSA which is responsible for the facility. In submitting the request for verification or initiation of a PSC, the facility shall include :

(a) the identity and security classification of the NATO contract or sub-contract; and

(b) the level of NATO classified information to which the employee will have access.

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

INTERNATIONAL TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

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

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

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

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

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

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

21. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorized access to classified material.

22. The security standards for the international transportation of NATO classified material can be found in the supporting security of information directive. The detailed requirements for the hand carriage of NATO classified material, the transportation of classified material by commercial carriers as freight, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting industrial security directive.

INTERNATIONAL VISITS

General

23. The arrangements described in this section relate to international visits by military and civilian representatives of NATO nations, NATO civil and military bodies, and NATO contractors and sub-contractors who need to visit the following locations 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; or

(c) a NATO civil or military body.

24. Visits referred to in paragraph 23 (a) and (b) above shall be approved by the NSA/DSA of the member nation in which the visit(s) will occur, taking into consideration the following :

(a) the visit has an official purpose related to a NATO programme or project; and

(b) all visitors hold an appropriate PSC and have a need-to-know for the information related to the NATO Project or Programme or activity.

25. Government departments and establishments, contractors and sub-contractors, and NATO civil and military bodies receiving visitors shall ensure that :

(a) visits meet the requirements of paragraph 24 above;

(b) visitors are given access only to NATO classified information related to the purpose of the visit; and

(c) records are kept of all visitors, including their name, the organisation 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.

26. Government departments and establishments and contractors and sub-contractors which intend to send personnel on international visits, shall submit to the NSA/DSA of the facility to be visited, through their NSA/DSA or the agreed official channels, an international visit request in accordance with the procedures set out in the industrial security directive. The international visit request shall provide an assurance that each visitor holds a valid personnel security clearance, as appropriate.

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

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

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

NATO CLASSIFIED CONTRACTS INVOLVING NON-NATO NATIONS

29. The policy described in subsequent paragraphs applies to the following scenarios involving NATO classified contracts / sub-contracts :

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

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

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

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

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

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

(a) a NATO nation; or

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

(c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 32 below).

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

(a) a NATO nation; or

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

(c) in a non-NATO nation with whom the contracting NATO nation has a bilateral Security Agreement / Arrangement (see paragraph 32 below); or

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

32. In the case of a bilateral Security Agreement / Arrangement (see paragraphs 30(c) and 31(c) above), in accordance with the requirements of Enclosure "E" to this C-M, the NATO nation shall provide a written assurance to NATO based upon a separate exchange of letters of understanding agreed between the NATO nation and the non-NATO nation requiring the latter to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement. This understanding shall identify the NATO security classifications as equivalents to the national classifications on which the bilateral Security Agreement / Arrangement is based; and identify that NATO classified information shall not be transferred to a third party without the prior approval of the originator of the information.

33. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of the NSA/DSA in a NATO nation.

Negotiation and Letting of NATO Classified Contracts

34. This subject is addressed by paragraphs 3 to 6 of this Enclosure. All aspects of that section are applicable to the negotiation and letting of NATO classified contracts / sub-contracts involving non-NATO nations, with the following clarifications :

(a) for contracts / sub-contracts classified NR, a FSC is not required unless specifically required under the security rules and regulations of the NATO parent nation or of the non-NATO parent nation of the contractor / sub-contractor performing the contract; and

(b) contractor representatives from non-NATO nations shall hold an appropriate PSC, and shall only receive access to NATO classified information authorised for release and needed for the negotiation of the contract / sub-contract.

Security Requirements for NATO Classified Contracts

35. This subject is addressed by paragraphs 7 to 10 of this Enclosure. All aspects of that section are applicable to the security requirements for NATO classified contracts / sub-contracts involving non-NATO nations.

Release of NATO Classified Information in Contracting

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

Industrial Security Clearances for NATO Contracts

37. This subject is addressed by paragraphs 12 to 19 of this Enclosure. All aspects of that section are applicable to industrial security clearances for NATO classified contracts / sub-contracts involving non-NATO nations, with the following clarifications :

(a) the appropriate security authority from the non-NATO nation is responsible for providing the appropriate FSCs; and

(b) the appropriate security authority from the non-NATO nation is responsible for issuing the appropriate PSCs .

International Transportation of NATO Classified Material

38. This subject is addressed by paragraphs 20 to 22 of this Enclosure. All aspects of that section are applicable to the international transportation of NATO classified material, noting that routes may originate from non-NATO nations and thus be authorised by the appropriate security authority of the non-NATO nation.

International Visits

39. This subject is addressed by paragraphs 23 to 27 of this Enclosure. All aspects of that section are applicable to international visits by individuals of non-NATO nations in support of NATO classified contracts involving non-NATO nations. The individuals may be from the following :

(a) a government department or establishment of a non-NATO nation; or

(b) the facility of a contractor or sub-contractor of a non-NATO nation.

Personnel on Loan Within a NATO Project / Programme

40. This subject is addressed by paragraph 28 of this Enclosure. All aspects of that section are applicable to personnel on loan within a NATO project / programme, with the following clarifications :

(a) where an individual is to be loaned to a facility in a non-NATO nation, the individual's parent facility shall request its security authority to provide the appropriate PSC to the appropriate security authority of the non-NATO nation; and

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