17 June 2002

INCLUDING COR 1 TO 12

DOCUMENT C-M(2002)49

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO)

Note by the Secretary General

Reference: C-M(2002)23 and its Action Sheet

1. This document is the result of a Fundamental Review by the NATO Security Committee (NSC) and it was approved by Council under the silence procedure on 26th March 2002 (reference refers).

2. This present document, in conjunction with C-M(2002)50, "Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats", supersedes C-M(55)15(Final). With the exception of Enclosure "A", the "Security Agreement by the Parties to the North Atlantic Treaty" which is still valid for those nations which have not yet ratified the "Agreement between the Parties to the North Atlantic Treaty for the Security of Information", all previous versions of C-M(55)15(Final) should now be destroyed.

3. The following Directives support this present document:

AC/35-D/2000	Directive on Personnel Security
AC/35-D/2001	Directive on Physical Security
AC/35-D/2002	Directive on Security of Information
AC/35-D/2003	Directive on Industrial Security
AC/35-D/2004	Primary Directive on INFOSEC
AC/35-D/2005	INFOSEC Management Directive for CIS

(The first four directives (AC/35-D/2000-2003) were approved by Council (reference refers) and the remaining two AC/35-D/2004 and D/2005) were approved by the NATO Security Committee (NSC) and the NATO C3 Board.

4. For ease of reference, a compendium, containing the two security policy documents (C-M(2002)49 and C-M(2002)50) and the above-mentioned supporting directives, will be distributed in the near future to all current holders of C-M(55)15(Final).

(Signed) George Robertson

Original: English

RECORD OF AMENDEMENTS

Strike out corresponding number
as each amemdment is 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

TABLE OF CONTENTS

ENCLOSURE "A"
C-M(2002)0049

ENCLOSURE "A"

AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949.

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties.

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary.

Realising that a general framework for security standards and procedures is required.

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization, have agreed as follows:

ARTICLE 1

The Parties shall:

(i) protect and safeguard:

(a) classified information (see ANNEX 1), marked as such, which is originated by NATO (see ANNEX 2) or which is submitted to NATO by a member state;

(b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

(ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;

(iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;

(iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

May 2013
Amdt. n° 10

ARTICLE 2

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

ARTICLE 3

(1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.

(2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.

(3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

ARTICLE 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see ANNEX 3).

ARTICLE 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

ARTICLE 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

(b) this Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval;

(c) this Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C. 2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

ARTICLE 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own constitutional procedures. Its instrument of accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

ARTICLE 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

ARTICLE 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depository which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depository, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

In witness whereof the undersigned, duly authorized to this effect by their respective Governments, have signed this Agreement.

Done in Brussels, this ..... day of ..... xxxx in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

ANNEX 1

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

(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 an 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.

ANNEX 2

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

ANNEX 3

This Annex forms an integral part of the Agreement.

Consultation takes place with military commanders in order to respect their prerogatives.

ENCLOSURE "B"

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

1. INTRODUCTION

1.1. 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.

2. AIMS AND OBJECTIVES

2.1. 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.

2.2. 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.

3. APPLICABILITY

3.1. 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.

3.2. 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.

3.3. 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".

3.4. 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.

3.5. 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 its companion Allied Joint Publication (AJP).

4. AUTHORITY

4.1. 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.

5. BASIC PRINCIPLES

5.1. 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 security, physical security, security of information, Communication and Information System Security (CIS Security), which shall extend to all individuals having access to classified information, all media-carrying information, and to all premises containing such information;

(e) Coordinating the management of the Insider Threat with the appropriate national authorities and NATO Civil and Military Bodies;

(f) NATO Nations and NATO Civil and Military Bodies shall establish Security Awareness and Training Programmes related to all security aspects as described in paragraph 5.1 (d) above;

(g) 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;

(h) 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;

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

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

(k) 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.

5.2. 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.

5.3. Personnel Security

5.3.1. 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.

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

5.3.3. Personnel security is addressed further at Enclosure "C" of this C-M and in the supporting personnel security directive.

5.4. Physical Security

5.4.1. 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.

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

5.5. Security of Information

5.5.1. 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.

5.5.2. 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.

5.5.3. 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.

5.5.4. 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.

5.5.5. 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).

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

5.5.7. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) may require specific additional security aspects to be addressed; the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (NNEs) contains security provisions and guidance applicable in these circumstances.

5.6. CIS Security

5.6.1. CIS Security is the application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

5.6.2. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation a balanced set of security measures (physical, personnel, information, CIS) shall be implemented to create a secure environment in which to operate a communication, information or other electronic system.

5.6.3. CIS Security is addressed further at Enclosure "F" of this C-M and in supporting Management and Technical and Implementation directives on CIS Security.

5.7. Industrial Security

5.7.1. 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.

5.7.2. 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.

5.7.3. 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.

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

6. PROTECTION OF INFORMATION ON KEY POINTS

6.1. 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.

7. SECURITY RESPONSIBILITIES

7.1. National Security Authority (NSA)

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

7.1.2. 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 24 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.

7.2. Designated Security Authority (DSA)

7.2.1. 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.

7.3. Security Committee (SC)

7.3.1. The SC 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 C3 Board shall be present at the meetings of the SC. Representatives of NATO civil and military bodies may also be present when matters of interest to them are addressed.

7.3.2. The SC 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 SC in the areas of personnel security, physical security, security of information, industrial security and CIS Security (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 C3 Board or the heads of NATO civil and military bodies and preparing appropriate recommendations thereon.

7.4. NATO Office of Security (NOS)

7.4.1. 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 SC.

7.4.2. 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 SC, 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 HQ 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 3.2 above.

7.5. NATO Military Committee and NATO Military Bodies

7.5.1. 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 7.4.2 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

7.5.2. 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 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.6. NATO Civil Bodies

7.6.1. 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 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.7. CIS Security

7.7.1. Principal organisations with responsibilities for CIS Security (for example, the C3B, NCSAs and NDAs) are described in Enclosure "F".

8. SECURITY CO-ORDINATION

8.1. 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 Security Committee (SC) for consideration.

8.2. 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 SC, 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.

13. The term “BOHEMIA” is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA will be protected in strict accordance with MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP) which covers doctrinal and procedural issues.

Dissemination Limitation Markings

14. 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

15. 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.

16. 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.

17. 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

18. 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.

19. 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.

20. 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.

21. 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.

22. 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).

23. 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.

24. 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

25. 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

26. 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.

27. 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.

28. 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.

29. 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.

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

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

32. 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

33. 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).

34. 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.

35. 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

36. 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[2] 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

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.

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;

(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[3] 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;

3 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.

(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;

(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

37. 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 36 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.

38. 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.

39. With the exceptions applying to NR information stated in paragraphs 37(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.

40. 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

41. 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.

42. 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.

43. 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.

44. 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

45. 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 "F"

Communication and Information System Security

1. INTRODUCTION

1.1. This Enclosure sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources[1] in communication, information and other electronic systems storing, processing or transmitting NATO classified information.

1.2. This Enclosure supports the NATO Information Management Policy and complements the Policy on Management of Non-Classified NATO Information which addresses the basic principles and standards to be applied within NATO civil and military bodies and NATO member nations for the protection of non-classified NATO information.

1.3. Communication and Information System Security (CIS Security) is one of the elements of Information Assurance (Figure 1) and is defined as the application of security measures for the protection of communication, information and other electronic systems[2], and the information that is stored, processed or transmitted[3] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

1.4. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation[4] for classified information handled in these CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be implemented to create a secure environment in which to operate a CIS. Where classified information is handled by industry in contracts, additional specific industrial security measures shall be applied in accordance with Enclosure G of this C-M and the supporting industrial security directive.

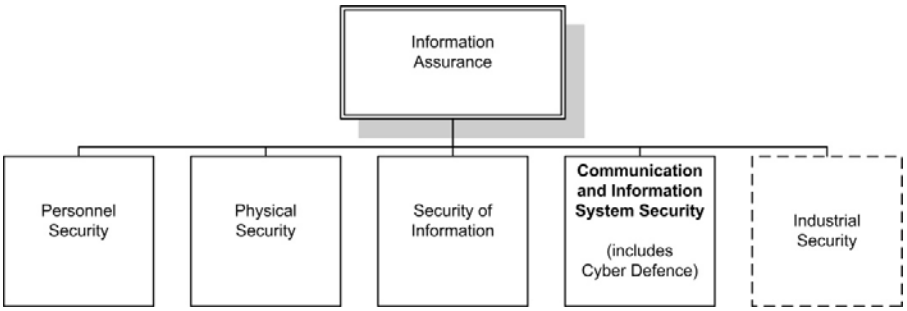

Figure 1 - Relationship between Information Assurance and CIS Security

1 Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the CIS are achieved; to include, for example, cryptographic products and mechanisms, COMSEC materials, directory services, and environmental facilities and controls.

2 Hereafter referred to within this Enclosure as CIS.

3 Hereafter referred to within this Enclosure as handled.

4 Hereafter referred to within this Enclosure as Security Objectives

1.5. The "Primary Directive on CIS Security", which is published by the SC and the C3B in support of this policy, addresses the CIS Security activities in the CIS life-cycle, and the CIS Security responsibilities of committees, and NATO civil and military bodies. The "Primary Directive on CIS Security" is supported by directives addressing CIS Security management (including security risk management, security accreditation, security-related documentation, and security review / inspection) and CIS Security technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographic security, transmission security, and emission security).

2. SECURITY OBJECTIVES

2.1. To achieve adequate security protection of NATO classified information handled in CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be identified and implemented to create a secure environment in which a CIS operates, and to meet the following security objectives:

(a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;

(b) to ensure the integrity of NATO classified information, and supporting system services and resources;

(c) to ensure the availability of NATO classified information, and supporting system services and resources;

(d) to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information; and

(e) to ensure appropriate non-repudiation for individuals and entities having processed the information.

2.2. NATO classified information and supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all systems and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a security risk assessment has established that NATO classified information and/or supporting system services and resources are subject to increased risks from specific threats and vulnerabilities.

2.3. Independent of the security classification of the NATO information being handled, NATO security authorities shall assess the risks and the level of damage done to NATO if the measures to achieve the non-confidentiality security objectives fail. The minimum set of measures for non-confidentiality services shall be determined in accordance with directives supporting this policy.

3. SECURITY ACCREDITATION

3.1. The extent to which the security objectives are to be met, and the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and supporting system services and resources shall be determined during the process of establishing the security requirement. The security accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained.

3.2. All CIS handling NATO classified information shall be subject to a security accreditation process, addressing the Security Objectives.

4. PERSONNEL SECURITY

4.1. Individuals authorised access to NATO classified information in any form shall be security cleared, where appropriate, taking account of their aggregate responsibility for achieving the Security Objectives of the information and the supporting system services and resources. This includes individuals who are authorised access to supporting system services and resources, or who are responsible for their protection, even if they are not authorised access to the information handled by the system.

5. PHYSICAL SECURITY

5.1. 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 the Security Objectives is met.

6. SECURITY of INFORMATION

6.1. All classified computer storage media shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information.

6.2. NATO classified information recorded on re-usable computer storage media, shall only be erased in accordance with procedures approved by the appropriate security authority.

6.3. Approved security measures (confidentiality and non-confidentiality), implemented in accordance with directives supporting this policy, may be used to protect NATO classified information in computer storage media in such a manner as to reduce the physical security requirements commensurate with a lower classification level.

7. INDUSTRIAL SECURITY

7.1. A contractor facility used for contracts in which NATO classified information is handled on CIS shall be established to meet the aggregate requirement for the Security Objectives.

7.2. A consistent set of CIS security measures shall be described in contracts, Security Aspect Letters (SAL) and/or Project Security Instructions (PSI) and/or Service Level Agreements (SLA), as applicable, and be implemented by contractors to meet the NATO CIS security objectives and to protect NATO classified information and supporting services.

8. SECURITY MEASURES

8.1. For all CIS handling NATO classified information, a consistent set of security measures shall be applied to meet the Security Objectives to protect information and supporting system services and resources. The security measures shall include, where appropriate, the following:

(a) a means to provide sufficient information to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of classified information and supporting system services and resources, commensurate with the damage that would be caused;

(b) a means to reliably identify and authenticate persons, devices and services authorised access. Information and material which controls access to a CIS shall be controlled and protected under arrangements commensurate with the information to which it may give access. On NATO CIS strong authentication mechanisms for persons shall be implemented;

(c) a means to control disclosure of, and access to, NATO classified information and supporting system services and resources, based upon the need-to-know principle;

(d) a means to verify the integrity and origin of NATO classified information, and supporting system services and resources;

(e) a means to maintain the integrity of NATO classified information and supporting system services and resources;

(f) a means to maintain the availability of NATO classified information and supporting system services and resources;

(g) a means to control the connection of CIS handling NATO classified information;

(h) a determination of the confidence to be placed in the protection mechanisms of CIS Security;

(i) a means to assess and verify the proper functioning of the protection mechanisms of CIS Security over the life-cycle of the CIS;

(j) a means to investigate user and CIS activity;

(k) a means to provide non-repudiation assurances that the sender of information is provided with proof of delivery and the recipient is provided proof of the sender's identity; and

(l) a means to protect stored NATO classified information where the physical security measures do not meet the minimum standards.

8.2. Security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand, and recover from, the impacts of incidents affecting the Security Objectives of NATO classified information and supporting system services and resources, including the reporting of security incidents.

8.3. The security measures shall be managed and implemented in accordance with directives supporting this policy.

9. SECURITY RISK MANAGEMENT

9.1. CIS handling NATO classified information, in NATO civil and military bodies, shall be subject to security risk management, including security risk assessment, in accordance with the requirements of directives supporting this policy.

9.2. Security risk management of NATO CIS shall ensure continuous assessment of system vulnerabilities and security compliance and shall move towards dynamic risk management to be able to face effectively the challenges posed by today's complex operational scenarios and multifaceted threat environments.

10. ELECTROMAGNETIC TRANSMISSION [5] of NATO CLASSIFIED INFORMATION

10.1. When NATO classified information is transmitted electromagnetically, special measures shall be implemented to achieve the Security Objectives of such transmissions. NATO authorities shall determine the requirements for protecting transmissions from detection, interception or exploitation.

11. CRYPTOGRAPHIC SECURITY

11.1. When cryptographic products or mechanisms are required to provide confidentiality and non-confidentiality protection, whether during information transmission, processing or storage (data at rest), such products or mechanisms shall be specifically approved for the purpose and specific cryptographic requirements for physical, procedural and technical measures shall be implemented to achieve the required Security Objectives.

11.2. Data at rest shall be protected to a level adequate to the required Security Objectives, and, where cryptographic products and mechanisms are used, the requirements for cryptographic security shall be in accordance with the relevant NATO Technical and Implementation Directives.

11.3. During transmission, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.4. During transmission, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

11.5. During transmission, the non-confidentiality requirements shall be assured in accordance with the communications system's operational requirement. The evaluation requirements and approval authority, for non-confidentiality mechanisms based on cryptography, shall be identified and agreed in conjunction with the specification of such mechanisms in the operational requirement, as agreed in technical directives.

[5] The term "electromagnetic transmission" covers transmission having both an electrical and magnetic character or properties, and includes, inter alia, visible light, radio waves, microwave, and infrared radiation.

11.6. Under exceptional operational circumstances, information classified NC and NS may be transmitted in clear text provided each occasion is properly reported to the higher authorities. The exceptional circumstances are as follows:

(a) during impending or actual crisis, conflict, or war situations; and

(b) when speed of delivery is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

11.7. Under exceptional operational circumstances, when speed is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations, information classified NR may be transmitted in clear text.

11.8. During transmission between NATO and non-NATO nations / International Organisations (NNN/IO) CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.9. During transmission within NNN/IO CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.10. Where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO and an IO may reach agreement on the mutual acceptance of each others' evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or IO information of the equivalent classification level. The conditions for such acceptance are set out in paragraph 11.12 below.

11.11. In exceptional circumstances, in order to support specific operational requirements, and where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO may agree the NNN's evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or NNN information of the equivalent classification level. The conditions for such agreement are set out in paragraph 11.12 below.

11.12. The following conditions are applicable in respect to the scenarios described at paragraphs 11.10 and 11.11 above:

(a) the NNN/IO shall have a Security Agreement with NATO and be certified by the NATO Office of Security (NOS) that they can appropriately protect released NATO classified information;

(b) each NNN/IO shall be treated on a case-by-case basis; and the basis of any acceptance / agreement shall be set out in the security arrangements supporting the Security Agreement between NATO and the NNN/IO;

(c) the terms of any such acceptance / agreement shall be approved by the NAMILCOM on the basis of an objective assessment carried out by the NOS, working in conjunction with the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN), the C3B Information Assurance and Cyber Defence Capability Panel and the NATO HQ C3 Staff, of the capability of the NNN/IO to perform cryptographic evaluations that meet requirements equivalent to those used within NATO for the cryptographic protection of NS information; and

(d) the NOS, in conjunction with SECAN and the NATO HQ C3 Staff, shall satisfy themselves, through verification and periodic re-verification, that the NNN/IO has in place appropriate structures, rules and procedures for the evaluation, selection, approval and control of cryptographic products and mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice.

11.13. Where acceptance / agreement is reached in accordance with the conditions set out in paragraph 11.12 above, the confidentiality of information classified NS may be protected by either cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM) or cryptographic products or mechanisms approved by the NCSA (or equivalent authority) of the NNN/IO for the protection of the equivalent classification level.

11.14. During transmission between NATO and NNN/IO CIS and within NNN/IO CIS, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms evaluated and approved by an appropriate authority. The appropriate authority may be the NAMILCOM, the NCSA of a NATO member nation or the equivalent authority of the NNN/IO, provided that the NNN/IO has appropriate structures, rules and procedures in place for the evaluation, selection, approval and control of such products or mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice. The structures, rules and procedures shall be agreed between the NAMILCOM and the NNN/IO.

11.15. The sensitive nature of the cryptomaterial used to protect NATO classified information necessitates the application of special security precautions beyond those required for the protection of other NATO classified information.

11.16. The protection which shall be afforded to cryptomaterial shall be commensurate with the damage that may be caused should that protection fail. There shall be positive means to assess and verify the protection and proper functioning of the cryptographic products and mechanisms, and the protection and control of cryptographic information (e.g. implementation details and associated documentation).

11.17. In recognition of the particular sensitivity of cryptographic information, special regulations and bodies shall exist within NATO and within each member nation to govern the receipt, control and dissemination of NATO cryptographic information to specially certified persons.

11.18. Special procedures shall also be followed which regulate the sharing of technical information, and which regulate the selection, production and procurement of cryptographic products and mechanisms.

12. EMISSION SECURITY

12.1. Security measures shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

13. SPECIFIC CIS SECURITY RESPONSIBILITIES

13.1. NATO Military Committee (NAMILCOM)

13.1.1. The NAMILCOM's responsibilities on CIS Security include the security approval and release of cryptographic equipment and participating in the evaluation and selection of cryptographic products and mechanisms for standard NATO use. The four nationally manned agencies of the Military Committee (SECAN, DACAN, EUSEC and EUDAC) provide advice and support on CIS Security to the NAMILCOM, to the SC, to the C3B and, as appropriate, to their sub-structures, to member nations and to other NATO organisations.

13.2. C3 Board (C3B)

13.2.1. As the senior Consultation, Command and Control (C3) policy committee within the Alliance, the C3B supports the NAMILCOM and the NATO political authorities in their validation process for C3 capabilities and projects by reviewing operational C3 requirements. The C3B is responsible for the provision of secure and interoperable NATO-wide C3 systems. Staff support to the C3B is provided by the NATO HQ C3 Staff (NHQC3S).

13.3. NATO Cyber Defence Management Board (CDMB)

13.3.1 The CDMB is the cyber defence coordination body providing strategic planning and direction for the implementation of the Cyber Defence Policy and facilitating cooperation with Allies. The CDMB reports to and receive political guidance from the NAC through the Defence Policy and Planning Committee in reinforced format (DPPC(R)). The CDMB is supervised by Allies through the C3B on C3 policy and implementation aspects of cyber defence. CDMB consults on specific subject matters through the appropriate NATO committees.

13.4. National CIS Security Authority (NCSA)

13.4.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NCSA, which may be established as an agency in the national security infrastructure. The NCSA is responsible for :

(a) controlling cryptographic technical information related to the protection of NATO information within their nation;

(b) ensuring that cryptographic systems, products and mechanisms for protecting NATO information are appropriately selected, operated and maintained;

(c) ensuring that CIS security products for protecting NATO information are appropriately selected, operated and maintained within their nation;

(d) communicating on NATO communications security and technical matters on CIS Security, both civil and military, with appropriate NATO and national bodies; and

(e) identifying a National TEMPEST Authority, as appropriate.

13.4.2. NCSAs work in co-ordination with their NSA(s).

13.5. **National Distribution Authority (NDA)**

13.5.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NDA, which may be established as an agency in the national security infrastructure, which is responsible for the management of NATO cryptomaterial within their nation and shall ensure that appropriate procedures are enforced and channels established for the comprehensive accounting, secure handling, storage, distribution and destruction of all cryptomaterial.

13.5.2. NDAs work in co-ordination with their NSA(s).

13.6. **Security Accreditation Authority(s)**

13.6.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify a security accreditation authority(s) which is responsible for the security accreditation of the following :

(a) national CIS handling NATO classified information; and

(b) NATO CIS operating within national bodies / organisations, as appropriate for non-NATO Nations.

13.6.2. Where a NATO civil or military body is established within a NATO nation, the NATO CIS shall be subject to security accreditation by a NATO SAA. In this case, the security accreditation may be co-ordinated with the appropriate national security accreditation authority.

13.7. **NATO Security Accreditation Authority (SAA)**

13.7.1. There are three NATO SAAs which are responsible for the security accreditation of NATO CIS handling NATO classified information. The SAA shall be the Director, NATO Office of Security and the Strategic Commanders, or their delegated / nominated representative(s), dependent upon the CIS to be accredited.

13.7.2. The NATO CIS Security Accreditation Board, composed of the NATO SAAs as identified in the paragraph above, shall have security accreditation oversight for all NATO CIS handling NATO classified information to ensure a corporate and consistent approach to security of NATO CIS. The NSAB Terms of Reference shall be subject to approval by the Security Committee.

13.8. **Security Authority for NNN**

13.8.1. The NNN shall appoint a security authority to be responsible for the security provisions of the present Enclosure and the oversight of the NNN Authorities with specific CIS Security responsibilities for national CIS handling NATO classified information (including NCSA, NDA and SAAs).

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

ENCLOSURE "G"

CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

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

(a) the security requirements for tendering, negotiation and letting of contracts involving NATO classified information;

(b) contracts involving NATO classified information with contractors in non-NATO nations

(c) the industrial security clearances for contracts involving NATO classified information (Facility Security Clearances (FSCs) and Personnel Security Clearances (PSC));

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

(e) the handling of NATO classified information in Communication and Information Systems (CIS);

(f) International Visit Control Procedures (IVCP); and

(g) the international transmission and transportation of NATO classified material;

2. This Enclosure is supported by the Directive on Classified Project and Industrial Security which sets out the detailed requirements and procedures.

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). An FSC shall be required for all Contractors involved in contracts that require the Contractor's facility to manage, generate or have access to classified information NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

4. The NPA/NPO or other contracting authority which initiates the contract shall ensure that Contractor's facilities hold an appropriate FSC for the specific phase of the contract. The contracting authority shall verify that Contractor's personnel accessing classified information NC or above at the premises of the contracting authority hold the appropriate PSC.

5. After the 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 these sub-contracts require access to information classified NC and above, the facility and personnel security requirements identified in the "Industrial Security Clearances For NATO Contracts" section of this Enclosure and in the Directive on Classified Project and Industrial Security shall apply. If a potential Sub-contractor is under the jurisdiction[1] of a non-NATO nation *prior* permission to negotiate a sub-contract shall be obtained from the NPA/NPO or other contracting authority respectively. 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 be requested to consider and give permission prior to contract discussion with contractors from those nations.

6. Upon letting the contract, the NPA/NPO or other contracting authority shall notify the NSA/DSA of the 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.

SECURITY REQUIREMENTS FOR CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

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 protecting all NATO classified information generated by or entrusted to the Contractor, or embodied in articles manufactured by the Contractor.

(a) Contracts for major programme/projects involving NATO classified information shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other contracts involving NATO classified information 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 supplements the NATO security policies and requirements, establishes specific security procedures associated with the NATO programme/project concerned and assigns responsibilities for the implementation of security measures concerning classified information.

(b) For contracts involving only NR information specific regulations have been established in the Directive on Classified Project and Industrial Security, in particular in its Appendix 4 "Contract Security Clause for Tenders and Contracts involving NATO RESTRICTED Information".

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

---

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

CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION *WITH CONTRACTORS* IN NON-NATO NATIONS

9. The letting of contracts involving NATO classified information with Contractors in non-NATO nations constitutes release of information and has to be in accordance with Enclosure "E" to C-M(2002)49, the Directive on Security of Information and the Directive on Classified Project and Industrial Security. The release shall always be with the consent of the relevant originator(s).

10. Contracts involving NATO classified information with Contractors in non-NATO nations require the existence of a bilateral Security Agreement/Arrangement between NATO or a contracting/sponsoring NATO nation and the non-NATO nation where the Contractor is under the jurisdiction of a NSA/DSA or other competent authority with the authority to commit the Contractor to provide the required protection. If the contract is governed by a bilateral Security Agreement/Arrangement between a contracting/sponsoring NATO nation and a non-NATO nation, the NATO nation shall provide a written security assurance to NATO confirming that the NATO classified information provided is governed under the scope of that Security Agreement/Arrangement. A copy of the assurance shall be provided to the NOS and the relevant NPO/NPA.

11. The undertaking of placing a contract to a Contractor of a non-NATO nation shall follow the procedures as established in the Directive on Classified Project and Industrial Security.

12. 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.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

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

Facility Security Clearances (FSC)

14. The NSA/DSA of each NATO nation is responsible for ensuring that any facility under its jurisdiction which will require access to information classified NC and above has adopted the protective security measures necessary to qualify for an FSC. In granting an FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted.

15. The assessment to be made prior to issuing an FSC shall be in accordance with the requirements and criteria set out in the supporting Directive on Classified Project and Industrial Security in addition to any applicable national laws and regulations.

16. A bidder, not holding an appropriate FSC as required by the potential contract/subcontract shall not be automatically excluded from the competition. The contracting authority should make all efforts in restricting the classification level of the information required to be provided to bidders to the lowest possible level still permitting an informed and qualified response to the invitation to tender. However, the tender document shall advise on the requirement for an appropriate FSC prior to the award of the contract/subcontract.

17. Scenarios identifying FSC requirements are provided in the supporting Directive on Classified Project and Industrial Security.

18. An FSC or PSC is not required for contracts or access to information classified NR. A nation which, under its National security laws and regulations, requires an FSC for a contract or sub-contract classified NR shall not discriminate against a Contractor from a nation not requiring an 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

19. The facility’s employees who require access to NATO classified information NC and above shall hold an appropriate PSC. The issuing of PSCs shall be in accordance with Enclosure “C” to C-M(2002)49, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

20. 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 the level of NATO classified information to which the employee will have access.

21. If a facility wishes to employ a citizen 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 which has jurisdiction over the hiring facility, 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”, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

22. The release of NATO classified information in contracting can constitute either release to non-NATO Nations and International Organisations or release to non-Programme/Project participants from NATO Nations. The release shall be with the consent of the relevant NPA/NPO and/or originator, as applicable, and in accordance with other relevant enclosures to the NATO Security Policy, the Directive on Security of Information as well as the Directive on Classified Project and Industrial Security.

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

23. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO classified information. Enclosure “F” to C-M(2002)49, the “Primary Directive on CIS Security” (AC/35-D/2004), the “INFOSEC Management Directive for CIS” (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO classified information.

24. The security accreditation of CIS handling NR information may be delegated to Contractors according to national security laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate, the security authority as established in the Directive on Classified Projects and Industrial Security with a statement of compliance certifying that the CIS handling NR information has been accredited in compliance with the policy on Security within NATO and its supporting directives on CIS Security.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

25. IVCP apply to international visits by representatives of NATO Nations, NATO Civil and Military Bodies, Contractors and Sub-Contractors involving NATO classified information. They also apply to representatives of a Non NATO Nation including Contractors/Sub-Contractors of such Nation if the Nation has adopted the IVCP.

26. Visits involving access to NATO information classified NC and above or unescorted access to security areas shall be approved by the NSA/DSA. Visits involving access to NU[2] or NR information may be arranged directly between the sending and receiving facility without formal requirements.

27. Detailed arrangements for the conduct of International Visits are laid down in the Directive on Classified Project and Industrial Security.

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 Directive on Classified Project and Industrial Security, and in accordance with National security laws and regulations.

2 NU is not a NATO security classification

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

29. 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 required, for companies providing transportation. In such cases, personnel handling the consignment shall be issued an PSC 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 having jurisdiction over the consignor and in accordance with the supporting Directive on Security of Information.

30. 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.

31. The security standards for the international transportation of NATO classified material can be found in the supporting Directive on Security of Information. However, the detailed requirements for the hand carriage of NATO classified material, carriage of classified material by commercial courier companies, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting Directive on Classified Project and Industrial Security.

GLOSSARY

Accountable Information	All information classified CTS and NS and all Special Category Information (such as ATOMAL).
Authentication	Authentication is the act of verifying the claimed identity of an entity.
Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity.
Breach of security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area where uncleared persons have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Communication and Information System Security (CIS Security)	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Competent Authority	An authority identified by the NSA of a NATO nation which is authorised to carry out personnel security clearances in order to give their nationals access to NATO classified information.
Compromise	Compromise denotes a situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The contractor, facility or other organisation receiving material from the consignor.
Consignor	The contractor, facility or other organisation responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.

February 2013
Amdt. n° 9

Contractor	An industrial, commercial or other entity that agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Cryptomaterial	Includes cryptographic algorithms and cryptographic hardware - and software-modules and products including implementation details and associated documentation and keying material (for both, symmetric and asymmetric cryptographic mechanisms).
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA.
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Dynamic risk management	The ability to perform risk management in a way that the risk of using a CIS is continuously assessed, any change in the context in which the CIS operates is reflected in the risk signature dynamically and the security countermeasures, most appropriate to the situation, are applied timely.
Escorts	Armed or unarmed national police, military, or other government personnel. Their function is to facilitate the secure movement of the material, but they do not have direct responsibility in matters of the protection of the material itself.
Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
Facility Security Clearance (FSC)	An administrative determination by a 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 perform on the NATO classified contracts.
Guards	Civilian (Government or participating contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.

Host Nation	General : the nation in which a NATO civil or military body is located. Industrial security : the nation designated by an official body of NATO to act as the governmental agency to contract for the performance of a NATO prime contract. Nations in which sub-contracts are performed are not referred to as host nations.
Information	Knowledge that can be communicated in any form.
Information Assurance	Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.
Infraction	A security infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (e.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.).
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO civil and military bodies fall within the security jurisdiction of NATO.
Life-cycle	Life cycle of information encompasses the stages of planning, collection, creation or generation of information; its organisation, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction.
Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and ”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.

February 2013
Amdt. n° 9

National Security Authority (NSA)	An authority of a NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad.
NATO	"NATO" denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.
NATO Classified Contract	Any contract issued by a NATO civil or military body or a NATO member nation in support of a NATO funded or administered programme/project that will require access to or generate NATO classified information.
NATO Classified Information	(a) information means knowledge that can be communicated in any form (b) classified information means information or material determined to require protection against unauthorised disclosure which has been so designated by a security classification (c) the word "material" includes documents and also any items 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 or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
NATO Military Committee (NAMILCOM)	The highest military authority in NATO; the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.
NATO Personnel Security Clearance	A determination that an individual is eligible to have access to NATO classified information.
NATO Production and Logistics Organisation (NPLO)	A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which North Atlantic Council grants clearly defined organisational, administrative and financial independence. It shall be comprised of a board of directors; and an executive body, composed of a General Manager and staff.
NATO Programme	A Council approved programme that is administered by a NATO management /office under NATO regulations.
NATO Project	A Council approved project that is administered by a NATO management agency/office under NATO regulations.

February 2013
Amdt. n° 9

NATO Project Management Agency	The executive body of a NPLO.
Need-to-know	See under "Principle of Need-to-know".
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.
Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients
Open Storage Area	An area, constructed in accordance with security requirements and authorized by the head of the civil or military body for open storage of classified information.
Originator	The nation or international organisation under whose authority information has been produced or introduced into NATO.
Parent Nation	The Kingdom of which an individual is a national, or the state of which an individual is a citizen.
Parent National Security Authority (NSA)	The NSA of the Kingdom of which an individual is a national, or the state of which an individual is a citizen.
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information.
Prime Contract	The initial contract led by a NATO Project Management / Agency / Office for a Programme/project.
Prime Contractor	An industrial, commercial or other entity of a 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 sub-contractors as approved.
Principle of Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.
Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the program lifecycle. For sub-contracts let within the program, the PSI constitutes the basis for the SAL.

Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Risk management	A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Security Assurance	A guarantee provided to NATO either directly or through a NATO nation or NATO civil or military body sponsoring release, that a non-NATO recipient of NATO classified information will provide the same degree of protection to it as required by NATO Security Policy.
Security Classification Check List	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified, specifying the security classification levels. In case of contracts let within a program/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Special Category Information	Information such as ATOMAL or Single Integrated Operational Plan (SIOP) to which additional handling/protection procedures are applied.
Sub-contract	A contract entered into by a prime contractor with another contractor (i.e., the sub-contractor) for the furnishing of goods or services.
Sub-contractor	A contractor to whom a prime contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources.