NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

20 November 2020

DOCUMENT
C-M(2002)49-REV1

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO)

Note by the Secretary General

Revision 1 to C-M(2002)49 dated 17 June 2002

Reference: C-M(2002)49-COR1 to COR12 (consolidated version), dated 17 June 2002

1. This document is the result of a major and comprehensive review of the NATO Security Policy and its supporting directives, as approved by the Security Committee.

2. C-M(2002)49-REV1, which replaces the document at reference, introduces both structural and content changes.

3. The structure has changed with the addition of a new Enclosure H to address specifically security in relation to non-NATO entities. This topic is developed further into the newly developed Directive for NATO on Security in Relation to Non-NATO Entities (reference AC/35-D/2006) and the revised Supporting Document for Non-NATO Entities on Security in Relation to NATO (reference AC/35-D/1038-REV3).

4. In terms of content, this revision has addressed Basic Principles, Minimum Standards and Responsibilities (Enclosure B), as well as provisions of Personnel Security, Physical Security, Security of Information and Security in Relation to Non-NATO Entities (Enclosures B, C, D, E and H). Enclosures F and G to C-M(2002)49 were not subject to this review.

(Signed) Jens Stoltenberg

1 Annex
Enclosures A,B,C,D,E,F,G,H
1 Glossary

Original: English

ANNEX 1
C-M(2002)49-REV1

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO)

INTRODUCTION

1. This C-M, entitled Security Within the North Atlantic Treaty Organization (NATO), 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 a common degree of protection for classified information. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics equivalent/conformant to those set out in this policy. In addition, this policy also addresses the security roles, functions and responsibilities within NATO.

2. This policy document consists of the Security Agreement at Enclosure "A" entitled "Agreement between the Parties to the North Atlantic Treaty for the Security of Information" together with the following additional Enclosures:

(a) Enclosure A – Agreement between the parties to NATO for the Security of Information
(b) Enclosure B – Basic Principles, Minimum Standards and Responsibilities.
(c) Enclosure C – Personnel Security.
(d) Enclosure D – Physical Security.
(e) Enclosure E – Security of NATO Classified Information.
(f) Enclosure F – Communication and Information System Security.
(g) Enclosure G – Classified Project and Industrial Security.
(h) Enclosure H – Security in relation to non-NATO entities.

3. This policy document supports the NATO Information Management Policy (C-M(2007)0118). The Policy on Management of Non-Classified NATO Information (C-M(2002)60) addresses the basic principles and standards to be applied within NATO Civil and Military bodies and NATO Nations for the protection of Non-Classified NATO information (NATO UNCLASSIFIED and Information releasable to the Public).

AIMS AND OBJECTIVES

4. 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 NATO Classified Information from loss of confidentiality, integrity and availability.

5. 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 NATO Classified Information.

APPLICABILITY

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

(a) classified information originated by NATO;

(b) classified information originated by a NATO Nation which is provided to NATO or provided to another NATO Nation in support of a NATO programme, project, or contract;

(c) classified information exchanged between NATO and non-NATO entities (NNE)[1]; and

(d) classified information entrusted to individuals and organizations outside a government (or a NATO Civil or Military body), e.g. consultants, industry, universities.

7. 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 (C-M(68)41) shall be applied to ensure appropriate access control, handling and protection of such information.

8. 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".

9. 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) its companion Allied Joint Publication (AJP) and the NATO Advisory Committee on Signals Intelligence (NACSI) Guide to SIGINT Administration and Procedures.

AUTHORITY

10. 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.[2]

[1] Non-NATO nations, and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies.

[2] Per Terms of reference for the Security Committee (C-M(2015)0002) NATO Security Policy consists of C-M(2002)49 and C-M(2002)50.

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.

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 any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

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, MINIMUM STANDARDS AND RESPONSIBILITIES

BASIC PRINCIPLES

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) Acknowledging the responsibility to share, classified information shall only be disseminated on the basis of the principle of need-to-know[1] to individuals who have been briefed on the relevant security procedures.

   (c) Only appropriately cleared individuals shall have access to information classified NATO CONFIDENTIAL and above.

   (d) The granting of a clearance shall not be considered as a final step in assessing an individual's eligibility for access to classified information but ongoing personnel security procedures, referred to as Aftercare, shall be established in order to address the management of the Insider Threat[2].

   (e) The NATO Office of Security (NOS) shall coordinate the management of the Insider Threat in conjunction with the appropriate national authorities and NATO Civil and Military bodies.

   (f) Security risk management[3] shall be mandatory within NATO Civil and Military bodies in accordance with the NATO Security Risk Management Process (AC/35-D/1035). Its application within NATO Nations is optional. Risk management shall not be used to circumvent security policy.

   (g) NATO Nations and NATO Civil and Military bodies shall establish Security Education and Awareness Programmes within their organizations addressing all security aspects as described in paragraph (l) below.

---

1 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.

2 Insider Threat is represented by personnel who have privileged access to NATO Classified Information and/or NATO assets by virtue of their role within the organization and could subsequently abuse this access to destroy, damage, remove or disclose NATO Classified Information and/or NATO assets either by intention or negligence.

3 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.

(h) All suspected Security Breaches and compromise of classified information shall be reported immediately to the appropriate security authority.

(i) 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.

(j) Classified information shall be subject to Originator Control[4].

(k) The release of NATO Classified Information shall be in accordance with the established procedures and criteria for the release, and in all cases, a degree of protection, no less stringent than that specified in this C-M and the supporting directives, shall be required for any NATO Classified Information released.

(l) Classified information shall be safeguarded by a balanced set of security measures addressing the following subjects: personnel security, physical security, security of information and security of Communication and Information Systems (CIS). When classified information is provided to contractors and released to non-NATO entities (NNE) it shall also be safeguarded by following the procedural measures set by these policies. These requirements shall extend to all individuals having access to classified information, all media carrying classified information, and to all premises containing such information.

(m) Establishments that hold NATO Classified Information shall develop mechanisms and processes to ensure application of NATO Security Policy requirements under adverse operational conditions, including disruptive incidents. Such mechanisms and processes may be reflected in either a Business Continuity Plan or Disaster Recovery Plan, depending on the nature of the incident.

PROTECTION OF INFORMATION ON KEY POINTS

2. The publication of information about critical civilian installations (e.g. defence supplies, energy supply) of military significance in times of tension or war may assist in the delivery of a kinetic attack or act of sabotage by allowing potential enemies or terrorists to compile a key points list, and to use this in order to identify points which may be vulnerable to attack. Appropriate steps shall be taken to ensure that such information is not freely available in the public domain in order to prevent its use in a hostile manner by enemies. Additionally, installations' owners and operators shall be fully aware of the risk of such activity against them and take such steps as necessary to protect this information.

SECURITY RESPONSIBILITIES

National Security Authority (NSA)

3. Each NATO Nation shall establish a National Security Authority (NSA) responsible for the security of NATO Classified Information. The NSA serves as the main point of contact for the NOS for any matter relating to security within NATO. Thereafter, the NSA may direct the NOS to the appropriate Designated Security Authority (DSA) or other competent security authority.

[4] The principle by which a nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.

4. The NSA is responsible for:

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

(b) ensuring that periodic and appropriate inspections of the security arrangements for the protection of NATO Classified Information are undertaken in all national organizations at all levels, both military and civil, to determine that NATO Classified Information is appropriately protected in accordance with current NATO security regulations. In the case of organizations 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 Personnel Security Clearance (PSC) has been granted to all nationals who are required to have access to information classified NATO CONFIDENTIAL and above, in accordance with NATO Security Policy;

(d) ensuring that security plans have been prepared in order to prevent NATO Classified Information from falling into unauthorised or hostile hands in the event of an emergency; and

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

Designated Security Authority (DSA)

5. An authority 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 function of a DSA may be carried out by the NSA.

Security Committee (SC)

6. The SC is established by the North Atlantic Council (NAC) and is composed of representatives from each NATO Nation's NSAs/DSAs and supported, where required, by additional NATO Nation security staff. Representatives of the International Military Staff (IMS), Strategic Commands and Consultation Command and Control (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. The Chairpersons for the SC at Principal's level, the SC in Security Policy Format (SC (SP)), and the SC in Communications and Information Systems (CIS) Security Format (SC (CISS)) are provided by the NOS.

7. 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 or endorsement to the NAC;

(b) examining questions concerning NATO Security Policy;

(c) reviewing and approving the supporting directives and guidance documents published in support of NATO Security Policy;[5] and

[5] A NATO Nation may request that a supporting directive also be approved by the NAC.

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

NATO Office of Security (NOS)

8. The NOS is established within the NATO International Staff as part of the Joint Intelligence and Security Division. It is composed of personnel experienced in security matters in both military and civil spheres. The NOS maintains close liaison with the NSAs/DSAs of NATO Nations, and with NATO Civil and Military bodies. The NOS may also, as required, request NATO 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 NOS would not be justified.

9. The NOS is responsible for:

(a) examining any questions affecting NATO security;

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

(c) the overall co-ordination of security for NATO among NATO Nations and NATO Civil and Military bodies;

(d) ensuring the implementation and oversight of NATO Security Policy, including the provision of such advice as may be requested by NATO 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 Chair of the MC of the state of security within NATO, and the progress made in implementing NAC decisions regarding security;

(f) carrying out periodic inspections of security systems for the protection of NATO Classified Information in NATO Nations, NATO Civil bodies, SHAPE and HQ SACT;[6]

(g) conducting security surveys in NNEs with whom NATO has a signed Security Agreement for the initial purpose of certification and periodically thereafter for ensuring ongoing compliance with NATO Security Policy;

(h) co-ordinating, with NSAs/DSAs and NATO Civil and Military bodies, the investigation of cases relating to the actual or suspected loss or compromise of NATO Classified Information;

(i) informing NSAs/DSAs of any adverse information which comes to light concerning their nationals, where appropriate;

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

(k) supervising, under the direction and on behalf of the Secretary General, the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

6 NATO Nations may, upon request of the NOS, participate in the NOS' inspections to NATO Civil and Military bodies either as observers or as active members of the inspection team. However, this is not possible for civil bodies where not all NATO Nations are part of the constituting framework.

Military Committee and NATO Military bodies

10. As the highest military authority in NATO, the MC is responsible for the overall conduct of military affairs. The MC 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" to this C-M. In accordance with previously agreed policy and in compliance with paragraphs 8 and 9 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chair of the MC informed.

11. The Heads of NATO Military bodies established under the auspices of the MC are responsible for all security matters within their establishments. This includes the responsibility for ensuring that a security organization is set up, that appropriate security measures and procedures are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases where organizations hold 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.

NATO Civil bodies

12. 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 organization 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 organizations holding 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.

SECURITY OVERSIGHT FOR CENTRE OF EXCELLENCE (COE)[7] / MEMORANDUM OF UNDERSTANDING (MOU) BODIES

13. Security oversight is defined as the supervisory function to ensure that any organization which handles NATO Classified Information is correctly applying NATO Security Policy for the protection of such information. Security oversight for bodies that lie outside the NATO Command Structure (NCS) in respect of protecting NATO Classified Information shall be delivered as follows:

(a) Participating nations are responsible and shall make appropriate arrangements as to how to deal with security within their NATO Military Body (NMB). Unless there are specific agreements in place regarding how to deal with security oversight for these elements, the Nation in which the element(s) is/are situated, i.e. the Host Nation, shall take the lead for exercising security oversight.

(b) COE/MOU bodies can be NMB if there is a NAC activating decision. In such cases NATO Security Policy is applicable and the head of the COE/MOU body shall be responsible for all security matters within their establishment. Participating nations are responsible and shall make necessary arrangements to deal with security requirements within any COE/MOU body. The Host Nation shall take the lead for

[7] NAC-approved COEs in accordance with PO(2020)0038 (INV).

exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight.

(c) If a COE/MOU body is not activated as a NMB (and thus not granted international status by the NAC), but accredited as a NATO COE/MOU, NATO Security Policy applies. Although participating nations will be responsible for all security matters within the COE/MOU, the Host Nation shall take the lead for exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the COE/MOU body.

(d) If a multi-national entity within one of the NATO Nations is not accredited as a COE, nor activated as a NMB but uses NATO Classified Information, NATO Security Policy applies and the participating nations remain responsible for security matters. If there are non-NATO nations participating, a security agreement with those nations must be in place before classified information can be exchanged. In such circumstances the Host Nation shall take the lead for security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the multi-national entity.

SECURITY CO-ORDINATION

14. Any NATO security issue between NSAs/DSAs of NATO Nations, and NATO Civil and Military bodies that cannot be resolved, or any issue with implementing or interpreting NATO Security Policy, shall be referred to the NOS. In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences shall be submitted by the NOS to the SC for consideration.

SECURITY POLICY MODIFICATIONS

15. Any proposals by NATO Nations and NATO Civil and Military bodies to modify NATO Security Policy should be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. Proposals will be considered by the NOS and if necessary raised to the SC for further discussion. This paragraph does not preclude the NSAs/DSAs from NATO Nations formally making proposals to the SC if they wish.

ENCLOSURE "C"
PERSONNEL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for Personnel Security. Additional details and requirements are found in the supporting Directive on Personnel Security (AC/35-D/2000).

2. Personnel security processes shall be designed to determine whether an individual can, taking into account their assessed loyalty, trustworthiness and reliability, be authorised to have access to classified information without constituting an unacceptable risk to security. To achieve this, all individuals[1], civilian and military, whose duties or functions require access to information classified CONFIDENTIAL[2] and above shall be appropriately investigated to give a satisfactory level of confidence as to their eligibility for access to such information and as such possess a national Personnel Security Clearance (PSC).[3]

3. In terms of access to NATO Classified Information NATO CONFIDENTIAL (NC) and above an individual will require a valid national PSC at the appropriate level along with the confirmation from the appropriate NSA/DSA or other competent security authority that the individual in question may be authorised to access NATO Classified Information.

APPLICATION OF THE NEED-TO-KNOW PRINCIPLE

4. 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)

5. A PSC is not required by NATO Security Policy for access to information classified NATO RESTRICTED (NR).[4] Individuals who only require access to information classified NR shall have been briefed on their security obligations in respect to the protection of NATO Classified

1 Aside from those Senior Government Officials, referred to in the paragraph 7 of this Enclosure.

2 Some NATO Nations, as mandated by their national laws and regulations, require a PSC for access to classified information at the level of RESTRICTED or national equivalent.

3 A PSC is a positive determination by which an NSA/DSA or other competent security authority formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.

4 Some NATO Nations, in accordance with their national laws and regulations, may require a PSC for access to information classified NR.

Information[5], shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation and shall also have a need-to-know.

6. An appropriate PSC is required when individuals access information classified NC and above or may have access to such information during the course of their duties. In addition, individuals are required to:

(a) have a need-to-know;

(b) have been briefed on their security obligations in respect to the protection of NATO Classified Information;

(c) have acknowledged their responsibilities either in writing or an equivalent method which ensures non-repudiation.

7. As an exception to paragraphs 5 and 6 above, access to NATO Classified Information by Senior Government Officials (e.g. Heads of State and Government, Government Ministers, Members of Parliament, Members of the Judiciary) is determined by national laws and regulations; such officials shall be briefed on their security obligations and shall have a need-to-know.

8. The level of PSC required and, therefore, the extent of security clearance processes undertaken shall be determined by the level of classification of the NATO Classified Information to which the individual is to have access. There shall be an agreed standard of confidence regarding the eligibility of individuals granted access to, or whose duties or functions may afford access to, NATO Classified Information.

9. 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 is to be achieved through effective engagement and regular evaluation by security authorities and managers. This includes assessing any change in circumstance or behaviour with potential security implications. Additionally, the effective use of security education and awareness programme(s) shall be used in order to remind individuals of their security responsibilities and of the need to report, to their managers or security staff, information which may affect their security status.

Exceptional Circumstances

10. Circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 6 above cannot be met. Details in respect to provisional appointments, temporary and emergency access, are set out in the supporting Directive on Personnel Security.

Responsibilities

11. It is the responsibility of the NATO Nation, of which the individual is a national, to process PSC applications. This includes the requirement to ensure that their PSC process meets the minimum investigative requirements and criteria for assessing the loyalty, trustworthiness and reliability of an individual in order to be granted a PSC as well as the requirements for renewal of PSC as set out in the Directive on Personnel Security.

12. NATO Civil and Military bodies are responsible for submitting PSC applications and renewals for their staff to the relevant NSA/DSA or other competent security authority.

[5] Nations may use either NATO specific briefings or national equivalent if the latter highlights the differences between the requirements of the two security frameworks.

13. The detailed responsibilities of NSAs/DSAs or other competent security authorities, NATO Nations and the Heads of a NATO Civil or Military bodies are set out in the Directive on Personnel Security.

SECURITY EDUCATION AND AWARENESS

14. All individuals employed in positions where they have access to information classified NR, or hold a PSC 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 potential consequences to them when NATO 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.

15. All individuals who are authorised access to, or are required to handle NATO Classified Information, shall initially be made aware, and periodically reminded of the threats to security arising from but not limited to the following:

(a) personal conduct outside the office, including activity on social media;

(b) indiscreet conversations with individuals without the need-to-know;

(c) working outside the office and when travelling;

(d) cyber threats;

(e) their relationship with the media; and

(f) the threat presented by the activities of intelligence services which target NATO and its Nations.

16. Individuals shall report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

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. Additional details and requirements are found in the supporting Directive on Physical Security (AC/35-D/2001).

2. Physical security is the application of physical protective measures to sites, buildings, facilities or installations that contain classified information requiring protection against loss or compromise.

3. NATO Nations and NATO Civil and Military bodies shall establish physical security programmes, consisting of active and passive security measures, to provide a common degree of physical security consistent with the assessment of the threats, vulnerabilities, security classification and quantity of the information to be protected.

SECURITY REQUIREMENTS

4. All sites, buildings, facilities, offices, rooms, and other areas in which NATO Classified Information is stored, handled and/or discussed 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 security classification and category of information;

(b) the quantity and form of the classified information (hard copy, and/or electronic) stored, and/or handled;

(c) access control and enforcement of the need-to-know principle;

(d) the threat from hostile intelligence services which target NATO and/or its member Nations, and the locally-assessed threat of terrorism, espionage, sabotage, subversion and (organized) crime; and

(e) how the classified information will be stored (e.g. hard copy or electronic and encrypted).

5. Physical security measures shall be designed to:

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

(b) deter, impede and detect actions from the insider threat;

(c) allow for segregation of personnel in their access to NATO Classified Information in accordance with their level of Personnel Security Clearance (PSC) and the need-to-know principle; and

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

GENERAL PHYSICAL SECURITY REQUIREMENTS

6. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and Communication and Information Systems (CIS) security measures. Sensible management of security risks will involve establishing the most proportionate, efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these domains. 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.

7. Physical security programmes shall be based on the principle of "defence in depth", using an appropriate combination of complementary physical security measures which provide a degree of protection meeting the requirements associated with the criticality and vulnerability of the organization and its information.

8. Although physical security measures are site-specific, and determined by a number of factors, the following general principles shall apply:

(a) it is first necessary to identify the assets that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors;

(b) the outermost physical security measures shall define the protected area and deter unauthorised access;

(c) the next layer of measures shall detect unauthorised or attempted access and alert the guard force; and

(d) the innermost layer 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.

9. Equipment that provides physical security (e.g. CCTV, IDS, secure cabinets) shall be maintained regularly or in response to a specific cause to ensure that it operates at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures as well as the complete security system. This is particularly important if there is a change in use of the site or specific elements of the security system. This can be achieved by regularly exercising security plans.

Security Areas

10. Areas**,** either fixed or temporary, in which information classified NATO CONFIDENTIAL (NC) and above is stored, handled and/or discussed shall be organised and structured so as to correspond to one of the following:

(a) **NATO Class I Security Area**: a particularly sensitive area in which information classified NC and above is stored, handled and/or discussed in such a way that entry into the area constitutes, for all practical purposes, access to NATO Classified Information and therefore unauthorised entry would constitute a Security Breach.

Such areas may include operations rooms, communications centres or archive facilities and require:

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

(ii) an entry control system which grants access only to those individuals appropriately cleared and specifically authorised[1] to enter the area;

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

(iv) a clear indication that entrance into such areas requires specific authorisation by the local security authority. This indication may include the level of security classification and/or the sensitivity of the area.

(b) **NATO Class II Security Area:** an area in which information classified NC and above is stored, handled and/or discussed in such a way that it can be protected from access by unauthorised individuals through utilizing controls established internally. Such areas may include working offices or meeting rooms where NATO Classified Information is stored, handled and/or discussed. These areas require:

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

(ii) an entry control system which permits unescorted access only to those individuals who are security cleared and authorised to enter the area; and

(iii) an escort or equivalent control mechanism to deal with those individuals who do not meet the criteria described in sub-paragraph (b) (ii) above in order to prevent unauthorised access to NATO Classified Information and uncontrolled entry to areas which have been specifically designated as protected against technical attacks and eavesdropping.

Administrative Zone

11. An Administrative Zone shall be established around or leading to NATO Class I or Class II Security Areas. Only information classified NATO RESTRICTED (NR) may be stored, handled and/or discussed in Administrative Zones. Such areas require a visibly defined perimeter, within which the possibility exists for the control of individuals and vehicles. However, individuals are not required to be escorted.

Technically Secure Areas

12. Technically Secure Areas, either fixed or temporary, are areas which have been specifically identified as requiring protection against technical attacks and eavesdropping. Such areas shall be subject to regular physical and technical inspections and entry to them shall be strictly controlled. The following measures shall be applied to protect against technical attacks and eavesdropping:

[1] Specifically authorised refers to those personnel who have been formally recognised as having a need-to-know and access based on the nature of their employment responsibilities, and are included on an access control list, as well as individuals who have been formally authorised by the head of the organization in question on an ad hoc basis to perform a specific role or duty.

(a) Appropriate level of physical and technical security measures to enforce access control, based upon the risk. The responsibility for determining the risk is shared between the appropriate technical specialists and the security authority which provides advice to the risk owner for a decision/approval.

(b) Such areas shall be locked and/or guarded when not occupied and any keys shall be treated as security keys. Regular physical and/or technical inspections, in accordance with the requirements of the appropriate security authority, shall be undertaken. Such inspections shall also be conducted following any unauthorised entry or suspicion thereof, as well as following the entry by external personnel (e.g. for the purposes of maintenance work, redecoration).

(c) No item, furnishing or equipment shall be allowed into these areas until they have been thoroughly examined for eavesdropping devices by trained security staff. An appropriate record of items, furnishing and equipment moved into and out of these areas shall be maintained.

(d) The presence of any electronic systems or devices with recording and/or transmitting capabilities shall be prohibited.

(e) Telephones and other video conference devices shall normally not be installed in such areas. However, where their installation is unavoidable, they shall be physically disconnected when classified discussions take place. This does not apply to appropriately installed and approved communication devices.

SPECIFIC PHYSICAL SECURITY MEASURES

13. Various specific physical and technical security measures and procedures can contribute to the security framework of an organization or site. Such measures and procedures include but are not limited to: Perimeter, Intrusion Detection System (IDS), Access Control, Closed Circuit Television, Security Lighting, Secure Cabinets and Office Furniture, Locks, Control of Keys and Combinations, Visitor Control, Entry and Exit Searches. The supporting Directive on Physical Security provides detailed information on specific physical and technical security measures and procedures.

MINIMUM STANDARDS FOR STORAGE OF NATO CLASSIFIED INFORMATION

14. NATO Classified Information shall be stored in areas, secure cabinets and/or office furniture designed to deter and detect unauthorised access to the information.

15. **COSMIC TOP SECRET (CTS).** Information classified CTS shall be stored within a Class I or Class II Security Area under one of the following conditions:

(a) in an approved secure cabinet with one of the following supplemental controls:

(i) continuous protection by cleared guard or duty personnel;

(ii) inspection of the secure cabinet not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or

(iii) an approved IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed to remove or break open the secure cabinet, or overcome the physical security measures in place;

(b) in an open storage area constructed in accordance with the requirements set out in the supporting Directive on Physical Security, which is equipped with an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry; or

(c) in an IDS-equipped vault in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

16. **NATO SECRET (NS).** Information classified NS shall be stored within a Class I or Class II Security Area by one of the following methods:

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

(b) in an approved secure cabinet or vault without supplemental controls; or

(c) in an open storage area, in which case one of the following supplemental controls is required:

(i) the location that houses the open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) cleared guard or duty personnel shall inspect the open storage area not less than once every four hours; or

(iii) an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

17. **NATO CONFIDENTIAL (NC).** Information classified NC shall be stored in a Class I or Class II Security Area in an approved secure cabinet.

18. **NATO RESTRICTED (NR).** Information classified NR shall be stored in a locked cabinet or office furniture (e.g. office desk drawer) within an Administrative Zone, Class I Security Area, or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher.

19. Additional details and requirements for the storage of NATO Classified Information are set out in the supporting Directive on Physical Security.

PHYSICAL PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS

20. 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 in a way that the aggregate requirement for confidentiality, integrity and availability is met.

21. 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.

22. Access to areas where critical CIS components are housed and managed shall be specifically controlled and limited to only authorised personnel associated with security and system/network/crypto administration.

PROTECTION AGAINST TECHNICAL ATTACKS

23. 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 co-ordinated with technical specialists and decided by the appropriate security authority. The supporting Directive on Physical Security provides details on protection against passive and active eavesdropping.

APPROVED EQUIPMENT

24. NATO Nations shall only use equipment which has been approved for the protection of NATO Classified Information by an appropriate security authority. NATO Civil and Military bodies shall ensure that any equipment purchased has been approved for use by one of the NATO Nations in similar conditions. NATO Civil and Military bodies may also purchase equipment approved for use by an appropriate security authority based on a completed risk assessment that supports the reduction or mitigation of the identified risk(s).

ENCLOSURE "E"

SECURITY OF NATO CLASSIFIED INFORMATION

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information. Additional details and requirements are found in the supporting Directive on the Security of NATO Classified Information (AC/35-D/2002).

2. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information. Classified information shall be protected throughout its life cycle to a level commensurate with its security 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. Security of information shall be complemented by Personnel, Physical and Communication and Information Systems (CIS) Security in order to ensure a balanced set of measures for the protection of NATO Classified Information.

NATO SECURITY CLASSIFICATIONS, SPECIAL DESIGNATORS, MARKINGS AND GENERAL PRINCIPLES

3. The originator is responsible for determining the security classification and initial dissemination of classified information.

4. The security classification shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, the originator shall indicate, where possible, whether their classified information can be downgraded or declassified on a certain date or event.

5. The security classification assigned determines the physical and CIS Security provided to the information in storage, transfer and transmission, its circulation, destruction and the Personnel Security Clearance (PSC) required for access. Therefore, both over-classification and under-classification shall be avoided in the interests of effective security as well as efficiency.

6. Security classifications shall be applied to classified Information in order to indicate the possible damage to the security of NATO and/or its member Nations if the information is subjected to unauthorised disclosure. It is the prerogative of the originator of the classified information to determine or modify the security classification. 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.

7. NATO security classifications indicate the sensitivity of NATO Classified Information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure.

8. NATO UNCLASSIFIED information and Information releasable to the Public shall be protected and handled in accordance with the NATO Information Management Policy (C-M(2007)0118) and The Management of Non-Classified NATO Information (C-M(2002)60).

9. 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 (AC/35-D/1040) contains security provisions and guidance applicable in these circumstances.

10. NATO Nations and NATO Civil and Military bodies shall introduce measures to ensure that classified information created by, or provided to NATO is assigned the correct security classification, and is protected in accordance with the requirements of the supporting Directive on the Security of NATO Classified Information.

11. 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 and NS information no less frequently than every 10 years in order to ascertain whether the security classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific NATO Classified Information shall be automatically downgraded after a predetermined period and the classified information has been so marked.

12. The overall security classification of a document shall be at least as high as that of its most highly classified component. Covering documents shall be marked with the overall NATO security classification of the information to which they are attached. Where possible, component parts like paragraphs, enclosures, annexes, etc., of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination.

13. When a large amount of NATO Classified Information is collated together, the original security classification markings shall be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Qualifying Markings

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

Special Category Designators

15. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement between the Parties to

the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

16. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information Within NATO C-M(71)27(Revised)”.

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

18. 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 doctrine and the NACSI Guide to SIGINT Administration and Procedures which addresses administration and procedures.

Dissemination Limitation Markings

19. 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

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

21. 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;

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

(d) register accountable information that has been released to NNEs.

22. Information classified CTS, NS and ATOMAL shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting Directive on the Security of NATO Classified Information. Where required by national laws and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

23. The security procedures and requirements of the registry system apply equally across both the physical and electronic domains. Additional details and requirements concerning the electronic domain can be found within Enclosure "F" to this C-M and its supporting directives.

24. 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 information classified CTS and other special category information shall be maintained at all times, or by establishing separate registries and control points.

25. Each NATO Nation or NATO Civil or Military Body, as appropriate, shall establish a Central Registry(s) for information classified 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.

26. Registries and control points shall act as the responsible organization for the internal distribution of information classified CTS and NS and for keeping records of all accountable information 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 laws and regulations.

27. 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 that procedures are in place to ensure that the information remains under the control of the Registry System.

28. 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 Directive on the Security of NATO Classified Information. Regardless of the type of registry organization, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

29. The supporting Directive on the Security of NATO Classified Information sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for information classified CTS and NS, the procedures for reproductions, translations and extracts, the requirements for the dissemination and transfer, and the requirements for the disposal and destruction of NATO Classified Information.

30. The Military Committee (MC) has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system does not require accountability in the Registry System.

CONTINGENCY PLANNING

31. 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 will be based on periodically reviewed threat assessments and shall give highest priority to the most sensitive, and mission- or time-critical information.

SECURITY INCIDENTS

32. A Security Incident is an event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.

Security Breach

33. A Security Breach is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy that may result in the actual or possible compromise of NATO Classified Information or supporting services and resources.

Compromise

34. Compromise denotes a situation when, due to a Security Breach or adverse activity, 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, unauthorised modification, destruction in an unauthorised manner, or denial of service.

Infraction

35. Infraction is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy, that does not result in the actual or possible compromise of NATO Classified Information.

36. All Security Breaches or potential Security Breaches shall be reported immediately to the appropriate security authority. Each reported Security Breach 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 Security Breach. The supporting Directive on Security of NATO Classified Information provides details on actions to be taken upon discovery of a Security Breach or Infraction.

REPORTING

37. The main purpose of reporting Security Breaches and 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 by the NSA/DSA or Head of the NATO Civil or Military Body concerned.

38. 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 submitting reports to the NOS depends on the sensitivity of the information and the circumstances.

39. The NOS, on behalf of the Secretary General of NATO, may request the appropriate authorities to make further investigations and to report their findings back to the NOS. Depending upon the circumstances and severity of the compromise, the NOS may inform the Security Committee (SC).

40. The supporting Directive on the Security of NATO Classified Information sets out the detailed actions, records and reporting requirements for Security Breaches and compromises of security.

41. Separate provisions relating to the compromise of cryptographic material have been issued by the MC to communications security authorities of NATO Nations and NATO Civil and Military bodies.

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.

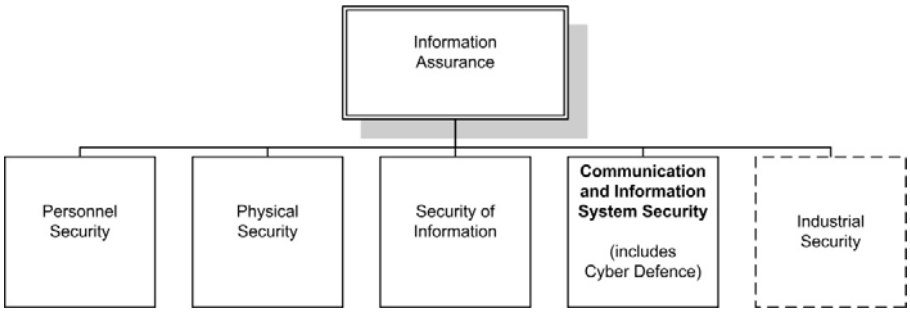

Figure 1 - Relationship between Information Assurance and CIS Security

---

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.

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.

---

[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

11.7. 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"

CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information within industry. Additional details and requirements are found in the supporting Directive on Classified Project and Industrial Security.

2. 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.

3. NSAs/DSAs 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.

FACILITY SECURITY REQUIREMENTS

4. All Contractors/Sub-contractors undertaking a contract involving NATO Classified Information requiring access to, or generation of information classified NATO CONFIDENTIAL (NC) or above shall hold a Facility Security Clearance (FSC) at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction over the Contractor/Sub-contractor's facility.

5. A FSC is not required for access to, or generation of information classified NATORESTRICTED (NR).

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

6. 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 information classified NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

7. 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 information classified NC or above at the premises of the contracting authority hold the appropriate PSC.

8. 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.

9. 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

10. 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 information classified NR 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".

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

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

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

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

13. 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. 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.

14. 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.

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

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

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

Facility Security Clearances (FSC)

17. 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.

18. 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. As a minimum the assessment shall cover aspects of the integrity and probity of the Contractor/Sub-Contractor, security status of its personnel and of other individuals who may, by virtue of their association be required to have access to NATO Classified Information, and aspects of the foreign ownership, control and influence.

19. 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 security 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.

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

21. 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

22. 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 this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

23. Applications for the security clearance for Contractor employees shall be made to the NSA/DSA which is responsible for the facility.

24. 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” to this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

25. The release of NATO Classified Information in contracting can constitute either release to non-NATO nations and International Organizations 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 the Security of NATO Classified Information as well as the Directive on Classified Project and Industrial Security.

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

26. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO Classified Information. Enclosure “F” to this C-M, the “Primary Directive on CIS Security” (AC/35-D/2004), the “Management Directive on CIS security” (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.

27. The security accreditation of CIS handling information classified NR 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.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

28. 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.

29. Visits involving access to 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 information classified NR may be arranged directly between the sending and receiving facility without formal requirements.

30. 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

31. 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 Personnel Security Clearance Confirmation for the individual to the NSA/DSA of the facility to which they are to be loaned.

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

32. 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 security 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 a 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 the Security of NATO Classified Information.

33. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall be in force in order to minimize the likelihood of unauthorised access to classified material.

34. The security standards for the international transfer of NATO Classified Information can be found in the supporting Directive on the Security of NATO Classified 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.

[2] NU is not a NATO security classification.

ENCLOSURE "H"

SECURITY IN RELATION TO NON-NATO ENTITIES

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the protection of NATO Classified Information to be released to or accessed by non-NATO nations and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies (hereinafter referred to as non-NATO entities (NNEs)).

2. The sharing of NATO Classified Information with NNEs shall take place in the context of NATO cooperative activities approved by the North Atlantic Council (NAC). Any request to share NATO Classified Information with NNEs outside such cooperative activities shall be considered and approved by the NAC or the appropriate delegated authority on a case-by-case basis. Additional details and requirements for the protection of NATO Classified Information to be released or accessed by NNEs are found in the supporting Directive for NATO on Security in Relation to NNEs.

3. The term 7 Non-NATO Nations (7NNN) refers solely to the following countries and their citizens: Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.[1]

4. NNEs shall establish an appropriate security authority responsible for the security of NATO Classified Information. The Supporting Document for Non-NATO Entities on Security in Relation to NATO provides the NNEs with an overview of the basic principles and minimum standards of security to be applied to the protection and handling of NATO Classified Information, and national equivalents exchanged in the context of NATO cooperative activities approved by the NAC.

GENERAL REQUIREMENTS

5. The sharing of NATO Classified Information with NNEs may take place in the contexts of:

   (a) NAC-approved cooperative activities where the NNE's participation has been approved by the North Atlantic Council (NAC);

   (b) NATO activities (e.g. programme, project, operation, task) where the NNE's participation and the nature of its engagement in a specific aspect of an activity is deemed beneficial to NATO; or

   (c) bilateral engagements between a NATO Nation and an NNE, where sharing of NATO Classified Information with an NNE has been determined to be beneficial to NATO.

6. Prior to sharing NATO Classified Information with an NNE, the NNE and NATO shall have entered into a Security Agreement, the implementation of which shall be certified by the NATO Office of Security (NOS). In the absence of a Security Agreement, a Security Assurance shall be in place where there is a political or operational imperative to share NATO Classified Information in a timely manner in support of a NAC-approved cooperative activity or, in exceptional cases, outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs describes

[1] NSAs/DSAs may propose changes to the list of countries, for approval by the Security Committee.

detailed provisions applicable to sharing NATO Classified Information with NNEs in the contexts specified in paragraph 5.

SECURITY AGREEMENTS AND ADMINISTRATIVE ARRANGEMENTS

7. A Security Agreement is a mechanism used to enable the exchange of classified information with an identified NNE. It sets out high level strategic principles agreed between NATO and the NNE, providing the basis for the implementation of appropriate security measures to protect NATO Classified Information as well as the NNE's classified information, when required. The implementation of the Security Agreement by the NNE shall be certified by the NOS before any NATO Classified Information is released to an NNE.

8. The security principles identified in the Security Agreement shall be supported by an appropriate set of Administrative Arrangements. The Administrative Arrangements act in support of the implementation of a Security Agreement and are a set of provisions which outline the basic security requirements for the appropriate and mutually acceptable protection of the exchanged classified information. Once the Administrative Arrangements have been concluded their application shall be confirmed by the NOS through the conduct of a security survey.

9. The NOS shall carry out periodic security surveys, at least once every two years, based on a risk management approach, of the relevant bodies within the NNE to ensure continued compliance with the Security Agreement and the Administrative Arrangements.

SECURITY ASSURANCES

10. A Security Assurance is utilized in the absence of a certified Security Agreement between NATO and an NNE where there is a political or operational imperative that necessitates the sharing of NATO Classified Information in a timely manner in support of a NAC-approved cooperative activity, or in exceptional cases outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria to be fulfilled in cases when a Security Assurance is used.

11. A Security Assurance formalises the NNE's commitment to provide an appropriate degree of protection to any NATO Classified Information received. A Security Assurance is limited to the specific activity, for a specific period of time.

12. A Security Assurance from an NNE, signed by a representative duly mandated by the NNE, shall be provided to the NOS in cases where a Security Assurance is utilized for the purposes of enabling sharing of NATO Classified Information in support of a:

(a) NAC-approved cooperative activity, or

(b) NATO activity, where the NNE's participation has been approved by the NAC or the appropriate delegated authority, on a case-by-case basis.

Sponsorship by a NATO Nation

13. Sharing of NATO Classified Information outside activities defined in 12 (a) or (b), further to a special request by a NATO Nation, requires sponsorship. A sponsorship means a form of support provided by a NATO Nation to an NNE in order to enable sharing of NATO Classified Information with an NNE in case of absence of a certified Security Agreement between NATO and the NNE.

14. In order for a NATO Nation to be able to act as a Sponsor there shall be an appropriate security framework (e.g. security agreement or other applicable arrangement) in place between the Sponsor and the NNE. The Sponsor shall provide a written Security Assurance, signed by a representative duly mandated by the NNE, to the NOS. The Security Assurance stipulates the minimum standards that the NNE shall apply for the protection of NATO Classified Information.

15. A sponsorship is limited to a specific activity, for a specific period of time.

SPECIFIC SECURITY PROVISIONS

16. When sharing NATO Classified Information with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs: access to NATO premises, access to NATO Classified Information, and release of NATO Classified Information. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria and the related specific measures and procedures applicable for each scenario.

Personnel Security

17. Before an NNE individual is granted access to information classified NC or above, the individual shall have successfully completed a PSC procedure no less rigorous than that required for a NATO national in accordance with NATO Security Policy and its supporting directives.

18. A PSC is not required for access to information classified NATO RESTRICTED (NR). However, the NNE individual shall have a need-to-know, shall be briefed on their security obligations in respect to the protection of NATO Classified Information and shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation.

19. A PSC may be required to access NATO premises based on specific criteria stipulated in the supporting Directive for NATO on Security in Relation to NNEs, and the relevant local security regulations.

Physical Security

20. Individuals from NNEs who, because of their assignment and official duties, need regular interface with NATO staff may be granted access to specific areas in which information classified NR and above is stored, handled and/or discussed. Such individuals may also be assigned office space within specific areas. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis.

21. The supporting Directive for NATO on Security in Relation to NNEs provides detailed information on the procedure, approval authorities and the criteria to be fulfilled for individuals from NNEs to be granted access to a NATO Class I or Class II Security Area, or to an Administrative Zone.

Security of Information

22. In the context of cooperation with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs:

(a) **Access to NATO premises**. A circumstance when an individual representing an NNE is authorised to physically access a specific NATO site, facility or specific area located within a facility. Physical access does not automatically include access to NATO Classified Information.

(b) **Access to NATO Classified Information.** A circumstance when an individual representing an NNE is authorised to access NATO Classified Information in order to fulfil their assignments and official duties when access is for NATO's benefit. Access is limited to the individual in question and they are not permitted to disseminate NATO Classified Information further to their NNE unless that information has been released in accordance with the established procedures.

(c) **Release of NATO Classified Information.** A circumstance when NATO Classified Information is authorised to be released to an NNE.

23. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria that needs to be fulfilled in specific circumstances when access to or release of NATO Classified Information is to be provided by NATO Civil or Military bodies, or by NATO Nations.

24. Release of NATO Classified Information to an NNE is always subject to receiving prior written consent of the originator(s).

25. NATO Classified Information may be released in the context of NAC-approved cooperative activity or in the context of NATO activities, where the NNE participants to that activity have been endorsed by the NAC or the appropriate delegated authority. The supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

26. For NATO Classified Information to be released on a special request from a NATO Nation (the Sponsor) to an NNE outside NAC-approved cooperative activities or NATO activities, where the NNE participants in that activity have been endorsed by the NAC or the appropriate delegated authority, the supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

27. Where a Security Agreement or Security Assurance is in force with an international organization, the release of NATO Classified 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. In the absence of a Security Agreement, where a Security Assurance is in place with an international organization, the release of NATO Classified Information to its non-NATO members shall be in accordance with the relevant provisions of the supporting Directive and the Security Assurance.

28. ATOMAL information of any security classification shall not be accessed by or released to any NNE which is not a party to the current Agreement Between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information C-M(64)39.

Release Authority

29. The NAC is the ultimate authority for the release of NATO Classified Information to NNEs. This authority respects the principle of originator consent and is delegated 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 information classified 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 staff to that committee;

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

(c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to the mission (XFOR), or is classified NATO/XFOR SECRET (mission SECRET), under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(d) SACT or D/SACT for information classified up to and including NS information, under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(e) the mission commander for an operation involving Non-NATO Troop Contributing Nations (NNTCN), 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 specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

(f) the NATO Production and Logistics Organization (NPLO), in coordination with the participating nations, for NATO Classified Information originated by and belonging to one or more of the nations participating in the NPLO.

30. With the exceptions applying to information classified NR stated in paragraphs 29 (a) and (b) above, delegated release authorities cannot further delegate their powers.

31. 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.

32. The Implementing Instructions on Intelligence Sharing Between NATO and NNEs (DSG(2015)0307-REV1) and the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (AC/35-D/1040) define the Release Authority in the environments of Operations, Training, Exercises, Transformation or Cooperation.

Records of Released Information

33. NATO Civil and Military bodies shall keep records of decisions of all information classified NC and above which they have released to an NNE and shall, at least every six months, report details of the reference number, title and release date to the NATO Central Registry, Brussels, unless otherwise directed by an appropriate Security Authority.

Communication and Information Systems Security

34. The supporting Directive for NATO on Security in Relation to NNEs outlines specific requirements that shall be met in order for an NNE individual to be provided access to NATO Communication and Information System (CIS).

35. Interconnection of NATO CIS with an NNE's CIS shall be security accredited in accordance with the NATO Security Policy and its supporting directives.

SECURITY INCIDENTS

36. Security incidents involving an NNE's classified information in NATO's possession shall follow the provisions of the Directive on the Security of NATO Classified Information (AC/35-D/2002) and any additional provisions specified in the Security Agreement and the implementing Administrative Arrangements, or Security Assurance with the NNE.

37. Security incidents involving an NNE’s classified information shall be immediately reported to the NOS. The NOS is responsible for promptly informing the relevant NNE’s Security Authority on security incidents involving an NNE’s classified information in accordance with the Security Agreement and the implementing Administrative Arrangements, or Security Assurance.

GLOSSARY

Access to information	The granting of permission for an individual or individuals to be exposed to specific information in line with the required security parameters for the execution of their clearly defined and appropriately authorised duties. Access in such circumstances is the privilege of the individual in question where rights of further dissemination are not permitted.
Access to premises	The granting of permissions for the physical access to a defined location where a nominated individual or individuals will be allowed to be present either with or without a designated escort dependent upon specific security requirements and clearances.
Accountable Information	All information classified CTS and NS and all Special Category Information. (such as ATOMAL)
Administrative Zone	A clearly defined protected area in which individuals are not required to be escorted and to which access is subject to authorization.
Aggregation Principle	When a large amount of NATO Classified Information is collated together, the original security classification markings must be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.
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.
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 Security Authority (CSA)	An authority identified by the NSA which is authorised to carry out specific security roles including those relating to personnel security clearances in order to give their nationals access to NATO Classified Information.
Compromise	Compromise denotes a situation when - due to a Security Breach 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.
Communications Centre	An organization responsible for handling and controlling communications traffic, normally comprising a message centre, a cryptographic centre, and transmitting and receiving stations.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The contractor, facility or other organization receiving material from the consignor.
Consignor	The contractor, facility or other organization responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.
Contractor	An industrial, commercial or other entity that agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Courier Service	A service that provides personnel 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 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 security 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.
Hand Carriage	The transmission of information by an individual carrying that information on their person.
Host Nation	<u>General:</u> The nation in which a NATO Civil or Military body is located. <u>Industrial security:</u> 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. NATO Classified Information left unsecured inside a secure facility where all individuals are appropriately cleared, failure to double wrap NATO 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 organization, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction.
Machine Readable Medium	A medium that can convey data to a given sensing device.
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.
Military Committee (MC)	The highest military authority in NATO; the MC is responsible for the overall conduct of military affairs. The MC is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.

Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and “Permanent Residents in Canada”. “Permanent Residents in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
National Security Authority (NSA)	An authority which is responsible for the security of NATO Classified Information in national agencies and elements, military or civil, at home or abroad.
NATO	“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.
NATO Classified Contract	Any contract issued by a NATO Civil or Military Body or a NATO Nation in support of a NATO funded or administered programme/project that will require access to or 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 Information	NATO information embraces all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources.

NATO Production and Logistics Organization (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 organizational, 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.
NATO Project Management Agency	The executive body of a NPLO.
Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial “notification of intention to call for bids” to the final decision to let a contract or sub-contract.
Non-confidentiality services	Services for CIS Security assuring security objectives other than for Confidentiality, namely Availability, Integrity, Authentication, and Non-repudiation.
Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organization 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 authorised by the head of the civil or military body for open storage of Classified Information.
Originator	The nation or international organization under whose authority information has been produced or introduced into NATO.
Originator Control	The principle by which the nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.
Parent Nation	The Nation of which an individual is a national.

Personnel Security Clearance (PSC)	A PSC is a positive determination by which a NSA/DSA formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.
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.
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 programme lifecycle. For sub-contracts let within the program, the PSI constitutes the basis for the SAL.
Registered Mail	A mail service that enables the possibility to track the shipment from the sender to the recipient and allows the sender a proof of the delivery.
Release of information	The act of authorizing a recipient entity to receive information with the understanding that this information will be available to the entire entity. The release may be facilitated through an individual representing the entity in question.
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.

Risk Owner	The individual or body that is charged with the responsibility of assessing the threats, vulnerabilities and impacts of any given risk with a view to establishing an appropriate risk appetite based upon the implementation of mitigating factors.
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 Breach	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 individuals 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).
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.
Security Keys	Security keys are those which operate the locks fitted to: secure cabinets provided for the storage of classified material; doors of secure rooms or areas; doors of secure rooms or areas which have been subject to technical security inspections; and secure cabinets used for the circulation of classified documents.
Security Incident	An event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.
Special Category Information	Information such as ATOMAL, Single Integrated Operational Plan (SIOP), BOHEMIA or CRYPTO to which additional handling/protection procedures are applied.
Sponsor	A NATO Nation or a NATO Civil or Military body acting as a guarantor in providing the necessary assurance that a NNE in receipt of NATO Classified Information will afford that information the necessary protection in line with the basic principles and requirements as set out in NATO Security Policy and supporting directives.

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.