NATO OTAN

NORTH ATLANTIC COUNCIL

CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

7 May 2013

DOCUMENT
C-M(2002)49-COR10

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION

Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 10

1. This document has been approved by the North Atlantic Council[1] under the silence period.

2. On January 24, 2013, Iceland deposited its instrument of ratification of the Agreement between the Parties to the North Atlantic Treaty for the Security of Information (Brussels, March 6, 1997). This means that now all 28 Allies have ratified this Agreement and that the condition in the footnote under Enclosure "A" to C-M(2002)49 is fulfilled. Considering that this note is a part of a formally agreed document by the NAC, it is appropriate to notify Nations that the Security Agreement is now in full effect for all Allies and that as a result the footnote can be deleted.

3. The Security Committee has approved the revision of Enclosure "B" to C-M(2002)49 under silence procedure on 22 March 2013. AC/35-WP(2013)0003 refers in this respect. The amendment concerns new sub-paragraph 5.1(e) of the Basic Security Principles in order to provide a legal basis for coordinating and managing the Insider Threat.

4. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosures "A" and "B" and destroy the previous versions.

5. This amendment bears serial number 10. Holders of C-M(2002)49 are therefore requested to strike out number 10 on the "Record of Amendments" which can be found on the opposite side of the cover page.

---

[1] C-M(2013)0018-AS1 refers

Annexes: Enclosure "A"
Enclosure "B"

Action Officer: Robert Keil, NOS/PSE, Ext. 4034
Original: English

ENCLOSURE "A"
C-M(2002)0049

ENCLOSURE "A"

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

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

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

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

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

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

ARTICLE 1

The Parties shall:

(i) protect and safeguard:

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

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

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

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

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

May 2013
Amdt. n° 10

ARTICLE 2

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

ARTICLE 3

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

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

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

ARTICLE 4

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

ARTICLE 5

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

ARTICLE 6

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

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

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

ARTICLE 7

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

ARTICLE 8

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

ARTICLE 9

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

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

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

ANNEX 1

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

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

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

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

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

ANNEX 2

This Annex forms an integral part of the Agreement.

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

ANNEX 3

This Annex forms an integral part of the Agreement.

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

ENCLOSURE "B"

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

1. INTRODUCTION

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

2. AIMS AND OBJECTIVES

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

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

3. APPLICABILITY

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

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

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

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

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

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

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

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

4. AUTHORITY

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

5. BASIC PRINCIPLES

5.1. The following basic principles shall apply:

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

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

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

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

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

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

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

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

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

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

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

5.2. The foundations of sound national security are:

(a) a security organisation responsible for:

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

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

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

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

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

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

5.3. Personnel Security

5.3.1. Personnel security procedures shall be designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorised to have initial and continued access to classified information without constituting an unacceptable risk to security. All individuals,

civilian and military, who require access to, or whose duties or functions may afford access to information classified CONFIDENTIAL or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know.

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

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

5.4. Physical Security

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

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

5.5. Security of Information

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

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

5.5.3. NATO security classifications and their significance are:

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

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

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

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

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

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

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

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

5.6. CIS Security

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

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

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

5.7. Industrial Security

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

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

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

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

6. PROTECTION OF INFORMATION ON KEY POINTS

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

7. SECURITY RESPONSIBILITIES

7.1. National Security Authority (NSA)

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

7.1.2. The NSA is responsible for:

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

(b) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organisations at all levels, both military and civil, to determine that such arrangements are adequate and in accordance with current NATO security regulations. In the case of organisations holding CTS or ATOMAL information, security inspections shall be made at least every 24 months, unless, during that period, they are carried out by the NOS;

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

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

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

7.2. Designated Security Authority (DSA)

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

7.3. Security Committee (SC)

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

7.3.2. The SC is responsible directly to the NAC for:

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

(b) examining questions concerning NATO Security Policy;

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

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

7.4. NATO Office of Security (NOS)

7.4.1. The NOS is established within the NATO International Staff. It is composed of personnel experienced in security matters in both military and civil spheres. The Office maintains close liaison with the NSA of each member nation, and with NATO civil and military bodies. The Office may also, as required, request member nations and NATO civil and military bodies to provide additional security experts to assist it for limited periods of time when full-time additions to the Office would not be justified. The Director, NOS, serves as Chairman to the SC.

7.4.2. The NOS is responsible for:

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

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

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

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

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

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

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

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

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

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

(k) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the NAC and under its authority, responsibilities for supervising the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement and supporting Administrative Arrangements referenced at paragraph 3.2 above.

7.5. NATO Military Committee and NATO Military Bodies

7.5.1. As the highest military authority in NATO, the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is consequently responsible for all security matters within the NATO military structure including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO classified information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure "F". In accordance with previously agreed policy and in compliance with its Terms of Reference in paragraph 7.4.2 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

7.5.2. The Heads of NATO military bodies established under the aegis of the NAMILCOM are responsible for all security matters within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.6. NATO Civil Bodies

7.6.1. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL

information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.7. CIS Security

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

8. SECURITY CO-ORDINATION

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

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