NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

09 April 2010

DOCUMENT
C-M(2002)49-COR8

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION

Corrigendum to C-M(2002)49 dated 17 June 2002
Amendment 8

1. This document is the result of a review of Enclosures “B” and “E” to C-M(2002)49 by the NATO Security Committee and has been approved by Council[1] under the silence period. These amendments concern the handling and protection of NATO signals intelligence marked COSMIC TOP SECRET – BOHEMIA. They are reflected in paragraph 8 of Enclosure “B” and in paragraph 13 of Enclosure “E”.

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

3. This amendment bears serial number 8. Holders of C-M(2002)49 are therefore requested to strike out number 8 on the "Record of Amendments" which can be found on the opposite side of the cover page.

[1] C-M(2010)0033 refers

Annexes: Enclosure "B"
Enclosure ”E”

Action Officer: Robert Keil, NOS/POB, E HQ - QG OTAN
Original: English

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

ENCLOSURE "B"

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

INTRODUCTION

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

AIMS AND OBJECTIVES

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

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

APPLICABILITY

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

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

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

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

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

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

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

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

AUTHORITY

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

BASIC PRINCIPLES

10. The following basic principles shall apply :

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

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

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

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

(e) NATO Nations and NATO Civil and Military Bodies shall establish Security Awareness and Training Programmes related to all security aspects as described in paragraph 10 (d) above;

(f) 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;

(g) 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;

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

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

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

11. The foundations of sound national security are :

(a) a security organisation responsible for :

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

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

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

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

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

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

Personnel Security

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

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

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

Physical Security

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

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

Security of Information

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

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

19. NATO security classifications and their significance are :

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

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

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

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

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

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

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

23. 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.

INFOSEC

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

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

Industrial Security

26. 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.

27. 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.

28. 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.

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

PROTECTION OF INFORMATION ON KEY POINTS

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

SECURITY RESPONSIBILITIES

National Security Authority (NSA)

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

32. 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.

Designated Security Authority (DSA)

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

NATO Security Committee (NSC)

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

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

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

(b) examining questions concerning NATO Security Policy;

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

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

NATO Office of Security (NOS)

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

37. The NOS is responsible for :

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

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

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

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

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

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

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

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

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

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

(k) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the NAC and under its authority, responsibilities for supervising the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement and supporting Administrative Arrangements referenced at paragraph 5 above.

NATO Military Committee and NATO Military Bodies

38. 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 36 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

39. 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.

NATO Civil Bodies

40. 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.

INFOSEC

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

SECURITY CO-ORDINATION

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

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

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

ENCLOSURE "E"

SECURITY OF INFORMATION

INTRODUCTION

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

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

CLASSIFICATION and MARKINGS

General

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

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

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

6. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

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

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

Qualifying Markings

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

Special Category Designators

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

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

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

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

Dissemination Limitation Markings

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

CONTROL AND HANDLING

Objectives of Accountability

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

16. Subordinate objectives are :

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

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

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

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

The Registry System

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

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

20. Registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information and for keeping records of all accountable documents held on that registry's or control point's charge; they may be

established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by National security rules and regulations.

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

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

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

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

CONTINGENCY PLANNING

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

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

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

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

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

29. When a compromise of NATO classified information has to be reported to the NOS, the report shall be forwarded through the NSA or the Head of the NATO civil or military body concerned. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances.

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

(iv) a Security Agreement, signed by the Secretary General on behalf of NATO and by a representative duly mandated[2] by the non-NATO recipient, shall have been concluded. In the absence of a Security Agreement and in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient, signed by a representative duly mandated[1] by the non-NATO recipient that any information received will be protected in accordance with its national laws and regulations and to a degree no less stringent than NATO minimum standards, shall have been provided to the NATO Office of Security;

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

(vi) the Security Assurance provided by the non-NATO recipient shall also identify the NATO security classifications and the equivalent security classifications of the non-NATO recipient. The Security Assurance shall be forwarded to the relevant committee responsible

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

for the approval of the release. Copies of the written Security Assurances shall be provided to the NATO Office of Security who shall maintain a database of Security Assurances;

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

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

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

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

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

(iii) the Sponsor shall be responsible for providing a written Security Assurance, signed by a representative duly mandated[3] by the non-NATO recipient, to NATO from the non-NATO recipient. The Security Assurance provided by the non-NATO recipient shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information. The NATO security classifications shall be identified with their equivalents to the national classifications cited in the bilateral Security Agreement / Arrangement;

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

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

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

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

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

Release Authority

37. The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated, taking into account the principles for authorising the release identified in paragraph 36 above, to :

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

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

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

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

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

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

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

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

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

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

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

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

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

39. With the exceptions applying to NR information stated in paragraphs 37(a) and (b) above, delegated release authorities cannot further delegate their powers, although they can entrust subordinate bodies with the implementation of the release decision.

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

Administrative Arrangements for the Implementation of a Security Agreement

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

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

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

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

Supporting Directive on the Security of Information

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

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

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

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

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

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