NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

6 December 2010

DOCUMENT
AC/35-D/2004-REV2

NATO SECURITY COMMITTEE

PRIMARY DIRECTIVE on INFOSEC

Note by the Chairman

1. At Annex 1 is the second revision of the "Primary Directive on INFOSEC". The Primary Directive is published jointly by the NSC and the C3 Board (C3B) (AC/322-D/0052-REV2 refers). This directive is published in support of NATO Security Policy (C-M(2002)49).

2. This document replaces AC/35-D/2004-REV1 which should be destroyed. In addition, it should be noted that this directive has been downgraded to NATO UNCLASSIFIED.

3. This directive, approved by both the NSC and the C3B under the silence procedure, will be subject to periodic review.

(Signed) Michael T. Evanoff

Annex : 1

Action officer: D.C. Murphy, NOS/POB, ext. 4592
Original: English

ANNEX 1
AC/35-D/2004-REV2

PRIMARY DIRECTIVE on INFOSEC

TABLE OF CONTENTS

SECTION I - INTRODUCTION

I.1 Purpose

1. This directive provides the connection between NATO Security Policy and the specific INFOSEC Management directives and guidance published by the NATO Security Committee (NSC), and INFOSEC Technical and Implementation directives and guidance published by the C3 Board (C3B). This directive sets out the security activities in the life-cycle of communication and information systems (CIS) and other electronic systems (hereafter referred to as *systems*) and their relationship to supporting INFOSEC Management and INFOSEC Technical and Implementation directives and guidance. Specifically, this Primary Directive is published in support of Enclosure "F" to NATO Security Policy (C-M(2002)49).

2. This Primary Directive on INFOSEC is published by both the NSC and the C3B, in support of the NATO Information Management Policy (NIMP) and the NATO policy for the protection of NATO classified information.

3. In addition, this directive provides information on, and an outline of the inter-relationships between the NATO committees, NATO civil and military bodies, and National bodies with a NATO INFOSEC responsibility; and the INFOSEC documentation structure of directives and guidance.

I.2 Scope

4. This Primary Directive is mandatory and binding upon *systems* storing, processing or transmitting NATO information. It is supported by INFOSEC Management and INFOSEC Technical and Implementation directives and guidance. In this directive, where it states “for NATO *systems*”, it is only mandatory and binding upon *systems* in NATO civil and military bodies and NATO *systems* extended into national or multi-national bodies.

5. National Security Authorities (NSAs), Strategic Command (SC) Security Authorities, and the NATO Office of Security (NOS) are responsible for ensuring the implementation of this directive.

I.3 Policy Requirements

6. The requirement to protect NATO information, and its supporting system services and resources, is based upon the principles set out in the following policies :

(a) NATO Information Management Policy (NIMP) (C-M(2007)0118); and

(b) NATO Policy for the protection of NATO classified (C-M(2002)49) information.

SECTION II - SECURITY ACTIVITIES IN THE *SYSTEM* LIFE-CYCLE

II.1 General

7. Security is a dynamic issue throughout the *system* life-cycle. Its requirements and effects shall be reviewed in each stage of the *system* life-cycle, from inception to disposal.

8. Security aspects shall be considered from the very beginning of a *system* life-cycle. Security may restrict the number of solutions that can be implemented. It has an impact on the associated civil works, the organisation of the operation and maintenance, on personnel requirements and costs. Security planning shall therefore involve the close interaction between the operational user, *system* planning and implementation authorities, *system* operating authorities and the appropriate security approval or accreditation authorities.

9. In order to counter threats and reduce or eliminate vulnerabilities, security shall be addressed at project inception so that cost-effective countermeasures can be provided to meet the security risks anticipated during the development and operation phases of the *system* life-cycle. Countermeasures introduced retrospectively will inevitably be more expensive, and may well be less effective, than those identified and addressed at the inception of the project. *System* planners shall ensure that sufficient funding and resources are available and allocated for the security aspects of the *system*, at the appropriate stages. *System* planners shall also ensure that the requirements for INFOSEC products (for example, cryptographic mechanisms / products, and security tools) are clearly identified.

II.2 Capability Packages (CPs) and Associated Documents

10. Capability Packages (CPs) and associated documents (for example, Crisis Response Operations Urgent Requirements (CURs)) are a major step towards the acquisition of NATO *systems*. They are developed on the basis of NATO operational requirements and shall address, coordinated by the appropriate planning, implementation, operating and security authorities, the required INFOSEC aspects.

II.3 Security Risk Assessment and Risk Management

11. For NATO *systems*, security risk assessment shall be embedded in the *system* development process. It is conducted jointly by representatives of the user, *system* planning, operating and the security approval or accreditation communities, using an agreed security risk assessment methodology. It involves assessment of existing, enhanced or new options, including balanced sets of technical and non-technical security measures. The aim is to select a solution which results in a satisfactory trade-off between user requirements, cost and residual security risk; whilst ensuring that minimum standards are applied for the protection of NATO information, in accordance with the requirements of NATO security policies and supporting directives.

12. The residual security risk is that risk which remains after implementing the security measures in a *system*, based on the understanding that not all threats can be countered and

not all vulnerabilities can be eliminated or reduced. Threats and vulnerabilities are dynamic, therefore the residual risk is subject to change. For that reason, risk shall be managed throughout the life cycle of NATO *systems*, implying that resources will be required to address security risk management.

13. Security risk management processes shall be applied to monitor, reduce, eliminate, avoid or accept risks associated with NATO *systems*. Security risk management is the process which balances the costs of applying additional security countermeasures with their benefits. In some cases, security risk management may result in accepting greater risk to save on the cost of countermeasures, provided that minimum standards are applied.

II.4 Threats and Vulnerabilities

14. The security risk assessment shall address the impact of threats and vulnerabilities on achieving the security objectives. A threat may be defined, in general terms, as the potential for the accidental or deliberate compromise of security. In the case of INFOSEC, such a compromise involves loss of one or more of the properties of confidentiality, of integrity and of availability, the three security objectives of INFOSEC. A vulnerability may be defined as a weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency; and may be technical, procedural or operational in nature.

15. Within NATO, there are a significant number of *systems* storing, processing or transmitting NATO information, ranging from stand-alone PCs and workstations, through small networked configurations of PCs and workstations (Local Area Networks (LANs)), to large and complex networks (for example, Wide Area Networks (WANs)) of information systems.

16. NATO information, in a concentrated form designed for rapid retrieval, communication and use, may be vulnerable to access by unauthorised users, to denial of access to authorised users, and to corruption, unauthorised modification and unauthorised deletion. Furthermore, the complex and sometimes fragile *system* equipment is expensive and often difficult to repair or replace rapidly.

17. *Systems* are attractive targets for intelligence gathering operations, especially if security measures are thought to be ineffective. They can enable large quantities of NATO information to be obtained quickly and surreptitiously. Any operation carried out by intelligence services (or subversive organisation's and terrorist group's members or sympathisers) targeting the NATO Alliance and its member nations is likely to be well planned and executed. Denial of authorised access to *systems* or corruption of the data within them may be an equally attractive target, and no less harmful to the effectiveness of NATO fulfilling its missions, whether or not the information involved is classified.

18. Security education shall make users aware of the general threats and vulnerabilities applicable to the *systems* they use, in order that they understand the rationale for the protective security measures in place.

II.5 Security Modes of Operation

19. NATO *systems* storing, processing or transmitting information classified NATO CONFIDENTIAL and above, or Special Category information, shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation :

(a) "dedicated" – a mode of operation in which ALL individuals with access to the *system* are cleared to the highest classification level of information stored, processed or transmitted within the *system*, and with a common need-to-know for ALL of the information stored, processed or transmitted within the *system*; or

(b) "system high" - a mode of operation in which ALL individuals with access to the *system* are cleared to the highest classification level of information stored, processed or transmitted within the *system*, but NOT ALL individuals with access to the *system* have a common need-to-know for the information stored, processed or transmitted within the *system*; approval to access information may be granted at an informal or individual level; or

(c) "compartmented" – a mode of operation in which ALL individuals with access to the *system* are cleared to the highest classification level of information stored, processed or transmitted within the *system*, but NOT ALL individuals with access to the *system* have a formal authorisation to access ALL of the information stored, processed or transmitted within the *system*; or

[Note. Formal authorisation indicates that there is a formal central management of access control as distinct from an individual's discretion to grant access.]

(d) "multi-level" - a mode of operation in which NOT ALL individuals with access to the *system* are cleared to the highest classification level of information stored, processed or transmitted within the *system*, and NOT ALL individuals with access to the *system* have a common need-to-know for ALL of the information stored, processed or transmitted within the *system*.

20. NATO *systems* storing, processing or transmitting (at the highest) NATO RESTRICTED information shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation :

(a) "dedicated" – a mode of operation in which ALL individuals with access to the *system* have a common need-to-know for ALL of the information stored, processed or transmitted within the *system*; or

(b) "system high" - a mode of operation in which ALL individuals with access to the *system* do NOT have a common need-to-know for ALL of the information stored, processed or transmitted within the *system*.

[Note. These interpretations of the modes of operation are included to show that a security clearance is not required for access to NATO RESTRICTED information.]

21. The Information Category Designation, US-Single Integrated Operation Plan (SIOP), shall only be processed in the "dedicated" security mode of operation.

II.6 Security Objectives

22. NATO security policy sets out a number of security objectives, as follows :

- **confidentiality** - to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO information, and supporting system services and resources;
- **integrity** - to ensure the integrity of NATO information, and supporting system services and resources; and
- **availability** - to ensure the availability of NATO information, and supporting system services and resources.

II.7 Security Principles

23. In order to the meet the objectives of confidentiality, integrity and availability, the following security principles shall be applied :

- **Security Risk Management** – for NATO *systems*, security risk management processes shall be applied to monitor, reduce, eliminate, avoid or accept risks;
- **Minimality** – only the functions, protocols, and services required to carry out the operational mission shall be installed and used;
- **Least Privilege** – *system* users shall only be given privileges and authorisations they require to perform their tasks and duties;
- **Self-protecting Node** – each *system* shall treat other *systems* as untrusted and implement protection measures to control the exchange of information with other *systems;*
- **Defence-in-Depth** – protection measures shall be implemented on various components to the extent possible so that there is not one single line of defence; and
- **Security Implementation Verification** – the application of these principles and the subsequent implementation of the protection measures shall be initially and periodically verified by the security approval or accreditation authority(s).

24. For NATO CIS and national CIS handling NATO classified information, there are minimum standards of security to be implemented in order that the security principles identified above are implemented. These minimum standards are set out in the latest versions of the INFOSEC Management directive for CIS and the C3B INFOSEC Technical and Implementation directives (for example, the Computer & LAN Security directive, the Interconnection of CIS directive, and the Security Tools directive).

II.8 Security-related Documentation

25. Security-related documentation shall be established in accordance with the requirements of the INFOSEC Management directive and the security approval or accreditation authority. Security-related documentation shall be required throughout the *system* life cycle, from the planning stage until the disposal stage. It is required for *systems* regardless of the funding source. The security-related documentation (for example, System-specific Security Requirement Statements (SSRSs) and Security Operating Procedures (SecOPs)) shall be developed in an iterative process throughout the *system* life cycle.

II.9 Security Approval or Accreditation Process

26. The security approval or accreditation process shall determine the extent to which INFOSEC measures are to be relied upon for the protection of NATO information and *system* assets, during the process of establishing the security requirements. The security approval or accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained. The security approval or accreditation process shall be carried out (for example, by Security Accreditation Authorities (SAAs)) in accordance with the requirements of the INFOSEC Management directive.

II.10 Security Education and Awareness

27. A major factor in achieving an adequate INFOSEC posture is an active security education and awareness programme for all *system* personnel and users of *system* facilities. To ensure that security responsibilities are clearly understood, INFOSEC education and awareness shall be available to senior level management; *system* planning, implementing and operating staffs; security staffs; and users. *System* personnel and users shall comply with the appropriate Security Operating Procedures (SecOPs).

II.11 Interconnection of CIS

28. NATO security policy requires security measures to control the connection of CIS handling NATO classified information. The supporting INFOSEC Management directive sets out the security approval or accreditation requirements and the supporting INFOSEC Technical and Implementation directives set out the measures to be implemented.

II.12 Connection of NATO CIS to Internet or Similar Networks in the Public Domain

29. NATO CIS may use the Internet or similar networks in the public domain purely as a bearer (as distinct from the contemporary use of the Internet), provided that the appropriate cryptographic protection is implemented. In this instance, the security objective of availability has to be seriously considered.

30. The requirement for protective measures for NATO CIS connected to Internet or similar networks in the public domain arises from the exceptional security risks posed by these types of public networks through their pervasive uncontrollable world-wide accessibility and the inherent susceptibility of their connectionless-oriented protocols and the vulnerabilities of the end *systems* to exploitation. NATO CIS, and the data they store and process, are at unacceptable security risk unless specifically protected.

31. The connection of NATO CIS storing, processing or transmitting (at the highest) NATO RESTRICTED information to Internet or similar networks in the public domain shall be controlled, to protect the NATO CIS from unauthorised external access or modification, and to prevent outgoing and incoming information from being illicitly read or modified. This control shall be applied in accordance with the requirements set out in the latest version of the “C3B INFOSEC Technical & Implementation Directive for the Interconnection of CIS" (AC/322-D/0030).

32. Where a NATO CIS storing, processing or transmitting NATO UNCLASSIFIED information, which is connected to Internet or similar networks in the public domain, is itself connected to a NATO CIS storing, processing or transmitting NATO RESTRICTED information, then that latter connectivity shall be in accordance with the requirements of connecting a NATO CIS storing, processing or transmitting NATO RESTRICTED information to Internet or similar networks in the public domain.

33. Where a NATO CIS storing, processing or transmitting (at the highest) NATO RESTRICTED information, which is connected to Internet or similar networks in the public domain, is itself connected to a NATO CIS storing, processing or transmitting CONFIDENTIAL / NATO SECRET information, then that latter connectivity shall be strictly controlled, shall be subject to the requirements of the appropriate security approval or accreditation authority, shall be subject to evaluation and certification by an appropriate National or NATO Evaluation Authority / Agency, and shall be subject to periodic Level 3 vulnerability assessments (see Section VII, INFOSEC Management Directive for CIS).

34. The connection of NATO CIS storing, processing or transmitting NATO CONFIDENTIAL / NATO SECRET information to Internet or similar networks in the public domain shall be strictly controlled, shall be subject to the requirements of the appropriate security approval or accreditation authority, shall be subject to evaluation and certification by an appropriate National or NATO Evaluation Authority / Agency, and shall be subject to periodic Level 3 vulnerability assessments (see Section VII, INFOSEC Management Directive for CIS).

35. The direct or cascaded connection of NATO CIS storing, processing or transmitting information classified COSMIC TOP SECRET, and/or Special Category information, to Internet or similar networks in the public domain is prohibited.

36. The principles of security risk management, minimality, self-protecting node and defence-in-depth (see paragraph 23) shall be applied to the connection of NATO CIS to Internet or similar networks in the public domain.

37. The connection of National CIS storing, processing or transmitting NATO information to Internet or similar networks in the public domain is subject to the appropriate National security rules and regulations.

38. The **ONLY** information which may be transmitted in clear (i.e., non-encrypted) text is the following :

(a) open source and public information, or NATO information specifically approved for disclosure to the public; and

(b) non-sensitive NATO UNCLASSIFIED; i.e., information that, as determined by the originator(s), bears no additional administrative marking (for example, in-confidence, or commercially sensitive) or dissemination limitation marking to indicate the sensitivity of the information.

39. **ONLY** open source and public information, or NATO information specifically approved for disclosure to the public, may be posted on publicly-accessible bulletin boards, web sites or web pages; and shall be subject to the integrity requirements of the originator(s) of the information.

40. For all connections of NATO CIS storing, processing or transmitting NATO classified information to Internet or similar networks in the public domain, the following shall be subject to the approval of the security approval or accreditation authority :

(a) the method of connection, and the services provided;

(b) the security risk assessment and risk management methodology to be utilised, and the results of the security risk assessment;

(c) the procedures and mechanisms for ensuring that NATO classified information is not transmitted over unprotected communications;

(d) the mechanisms and/or procedures for ensuring the confidentiality, integrity and/or availability of the information, and supporting system services / resources;

(e) the mechanisms and/or procedures to meet the accountability requirements; and

(f) the security-related documentation, including the security test plan and the results of the security testing.

41. The security approval or accreditation authority shall be responsible for the initial security implementation verification and the periodic re-verification.

II.13 Access by Non-NATO Nationals to NATO CIS

42. Where access by non-NATO nationals to NATO communication and information systems (CIS) is authorised in support of NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) (Enclosure “B” to C-M(2002)49 refers), measures shall be applied to restrict access to the NATO classified information required to support the mission. Access by non-NATO nationals to NATO CIS shall be in accordance with the latest version of AC/35-D/1040, Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (NNEs).

43. The appropriate NATO security approval or accreditation authority shall exercise oversight of those measures, including the review of the periodic re-assessment of the security risks associated with access by non-NATO nationals to NATO CIS.

SECTION III - *SYSTEM* LIFE-CYCLE INFOSEC-RELATED ACTIVITIES

44. This section addresses the minimum INFOSEC-related activities, and their associated responsible authorities and staffs, that shall be undertaken during the *system* life-cycle. These activities are based upon the requirements established in more detail in the supporting directives. The following generic stages of the *system* life-cycle are identified, which may be adapted according to NATO and national requirements :

(a) *system* planning;

(b) *system* development and procurement;

(c) *system* implementation and security approval or security accreditation;

(d) *system* operation

(e) *system* enhancement; and

(f) *system* withdrawal from service, and disposal of equipment.

45. The INFOSEC-related activities highlight the context in which NATO security policy and its supporting “INFOSEC Management” and “INFOSEC Technical & Implementation” directives and guidance are to be utilised, in order to assess the security approval or accreditation, and implementation requirements. A "Roadmap" to NATO Security Policy, supporting directives, supporting documents and guidance documents is available from the NATO Security Accreditation Authorities and the NATO HQ C3 Staff Information Assurance Branch, to assist in determining the specific policy, directive and guidance applicable to each phase of the *system* life-cycle (see Section V – NATO INFOSEC Documentation Structure).

III.1 *System* Planning

46. The following INFOSEC-related activities and responsible authorities are associated with the planning stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) Identify and notify the appropriate security approval or accreditation authority (e.g., Security Accreditation Authority (SAA) or Security Accreditation Board (SAB)) of *system* plans	CIS planning & implementation authority or project staffs	INFOSEC Management directive and guidelines
(2) Establish a *system* security organisation (or ensure that an existing organisation is valid) and identify the INFOSEC-related tasks	CIS planning & implementation authority / project staffs / CIS operating authority, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines
(3) Establish the basis for security approval or accreditation, or establish a security approval or accreditation strategy	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority or project staffs	INFOSEC Management directive and guidelines
(4) For NATO *systems*, identify the security risk assessment requirement and the security risk assessment and management methodology to be utilised	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority or project staffs	INFOSEC Management directive and guidelines
(5) For NATO *systems*, undertake an initial security risk assessment in accordance with the requirements of the security approval or accreditation authority	CIS planning & implementation authority or project staffs (for INFOSEC technical & implementation aspects), coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines
(6) For NATO *systems*, approve the results of the initial security risk assessment	Security approval or accreditation authority	INFOSEC Management directive and guidelines

Activity	Responsible Authority / Staffs	Document(s)
(7) Identify initial requirement for cryptographic products and mechanisms	CIS planning & implementation authority or project staffs, coordinating with the appropriate security approval or accreditation authority(s) and AC/322(SC/4)	INFOSEC Technical & Implementation directives
(8) Develop the initial SRS(s) (or national equivalent(s)), or, where appropriate for NATO *systems*, address the required INFOSEC aspects of Capability Packages (CPs) and associated documents; using, where appropriate, applicable Protection Profiles, Packages, Common Criteria terminology and concepts	CIS planning & implementation authority or project staffs, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives and guidelines Reference Architecture Documents
(9) Approve the initial SRS(s) (or national equivalent(s)) or, where appropriate for NATO *systems*, approve the required INFOSEC aspects of Capability Packages (CPs) and associated documents	Security approval or accreditation authority	INFOSEC Management directive and guidelines

III.2 *System* Development and Procurement

47. The following INFOSEC-related activities and responsible authorities are associated with the development and procurement stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) For NATO *systems*, refine the security risk assessment in accordance with the requirements of the security approval or accreditation authority	CIS planning & implementation authority or project staffs, in conjunction with the security approval or accreditation authority	INFOSEC Management directive and guidelines
(2) Check the CIS security architecture against reference security architecture(s) to ensure, where possible, security interoperability and integration of new CIS in existing infrastructure(s)	CIS planning & implementation authority or project staffs	Reference Architecture Documents
(3) For NATO *systems*, approve the results of the refined security risk assessment	Security approval or accreditation authority	INFOSEC Management directive and guidelines
(4) Develop a detailed specification of INFOSEC (computer, transmission, cryptographic and emission security) measures, in accordance with the requirements of the security approval or accreditation authority, addressing security functionality and assurance and, where appropriate, the interconnection of *systems*; using, where appropriate, applicable Protection Profiles	CIS planning & implementation authority(s), coordinating with the CIS operating authority, the site Security Authority, and the security approval or accreditation authority	INFOSEC Technical & Implementation directives and guidelines
(5) Review INFOSEC products lists for products which can meet the INFOSEC requirement(s)	CIS planning & implementation authority(s), coordinating with the CIS operating authority and the security approval or accreditation authority	NATO Information Assurance Products Catalogue (NIAPC)

Activity	Responsible Authority / Staffs	Document(s)
(6) Where appropriate, develop the operational requirements for cryptographic products and mechanisms; using, where appropriate, Common Criteria terminology and concepts; and, for NATO *systems* under NATO common funding, notify AC/322(SC/4) of requirements	CIS planning & implementation authority, coordinating with the CIS operating authority and the security approval or accreditation authority	INFOSEC Technical & Implementation directives
(7) Where appropriate, for NATO *systems* under NATO common funding, develop the technical characteristics for cryptographic products and mechanisms	AC/322(SC/4), on behalf of the C3B	INFOSEC Technical & Implementation directives
(8) Develop a detailed specification of security measures covering personnel, physical, and security of information aspects	CIS planning & implementation authority(s), coordinating with the CIS operating authority and the security approval or accreditation authority	NATO Security Policy & Supporting Directives
(9) Where appropriate, advise NCSAs, through the C3B Information Assurance Sub-committee (AC/322(SC/4)), of the requirement for cryptographic products and mechanisms	CIS planning & implementation authority or project staffs	INFOSEC Technical & Implementation directives
(10) Where appropriate, establish an evaluation / selection timetable for cryptographic products and mechanisms	AC/322(SC/4) supporting staffs, coordinating with the NCSAs, SECAN, the CIS planning & implementation authority or project staffs, and the CIS operating authority	INFOSEC Technical & Implementation directives
(11) Where appropriate, undertake evaluation, approval and selection of cryptographic products and mechanisms.	AC/322(SC/4) supporting staffs (supported by NITC / NATO CIS Services Agency), in conjunction with SECAN, with approval by NAMILCOM	INFOSEC Technical & Implementation directives

Activity	Responsible Authority / Staffs	Document(s)
(12) Establish requirement for security test and evaluation (ST&E) of the *system* or, where appropriate, of the interconnection of *systems* For NATO systems, ensure that the Type "B" Cost Estimate (TBCE) identifies any requirement for evaluation and certification in order to establish the appropriate funding	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority(s) or project staffs. CIS planning & implementation authority or project staffs, coordinating with the security approval or accreditation authority	INFOSEC Management directive INFOSEC Technical & Implementation directives and guidelines
(13) On-going development of the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles, Packages, Common Criteria terminology and concepts	CIS planning & implementation authority or project staffs, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives and guidelines
(14) On-going approval of the SRS(s) (or national equivalent(s))	Security approval or accreditation authority	INFOSEC Management directive and guidelines

III.3 *System* Implementation and Security Approval or Security Accreditation

48. The following INFOSEC-related activities and responsible authorities are associated with the implementation and security approval or security accreditation stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) Refine security test and evaluation (ST&E) requirements of the *system* or, where appropriate, the interconnection of *systems*	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority & CIS operating authority	INFOSEC Management directive INFOSEC Technical & Implementation directives and guidelines
(2) Develop security test and evaluation (ST&E) plan	CIS planning & implementation authority(s), coordinating with the CIS operating authority and the security approval or accreditation authority	INFOSEC Management directive
(3) Undertake, where required, an evaluation and certification of the *system* or, where appropriate, of the interconnection of *systems*; in accordance with, where appropriate, the Common Criteria Evaluation Methodology	NATO or National Evaluation & Certification Authority, coordinating with the CIS planning & implementation authority(s), the CIS operating authority and the security approval or accreditation authority	INFOSEC Technical & Implementation directives and guidelines
(4) Undertake security testing, in accordance with an agreed ST&E plan	CIS operating authority (or independent authority acting on behalf of the CIS operating authority), coordinating with the CIS planning & implementation authority(s) and the security approval or accreditation authority	INFOSEC Management directive

Activity	Responsible Authority / Staffs	Document(s)
(5) Review results of security testing	Security approval or accreditation authority	INFOSEC Management directive
(6) Identify, as a result of the security testing, any additional security countermeasures to be implemented	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority and the CIS operating authority	INFOSEC Management directive
(7) For NATO *systems*, identify and agree the residual risks to be accepted	Security approval or accreditation authority, in conjunction with the CIS operating authority	INFOSEC Management directive and guidelines
(8) For NATO *systems*, identify and agree the on-going security risk management processes	Security approval or accreditation authority, in conjunction with the CIS operating authority	INFOSEC Management directive and guidelines
(9) Complete the SRS(s) (or national equivalent(s))	CIS planning & implementation authority or project staffs, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines
(10) Formulate the Security Operating Procedures (SecOPs) (or national equivalent(s)) for the CIS	CIS operating authority, coordinating with the security management staffs	INFOSEC Management directive and guidelines
(11) Approve the SRS(s) and SecOPs (or national equivalent(s))	Security approval or accreditation authority	INFOSEC Management directive and guidelines

Activity	Responsible Authority / Staffs	Document(s)
(12) Approve or accredit the *system* or, where appropriate, the interconnection of *systems*; and publish an approval or accreditation statement	Security approval or accreditation authority	INFOSEC Management directive and guidelines
(13) Establish the re-approval or re-accreditation conditions	Security approval or accreditation authority	INFOSEC Management directive and guidelines

III.4 *System* Operation

49. The following INFOSEC-related activities and responsible authorities are associated with the operation stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) Store, process or transmit NATO information in the operational environment in accordance with the approved Security Operating Procedures (SecOPs) (or national equivalent(s)), including system and security administration	CIS operating authority, coordinating with the security management staffs	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives and guidelines
(2) For NATO *systems*, perform on-going security risk management, in accordance with the requirements of the security approval or accreditation authority	CIS operating authority, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines
(3) Detect and react to INFOSEC incidents, in accordance with the requirements of the SecOPs (or national equivalent(s)) and, where appropriate, the NATO Cyber Defence Management Authority (CDMA) CONOPS and NATO CIRC Handbook	CIS operating authority, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives and guidelines CDMA documents

Activity	Responsible Authority / Staffs	Document(s)
(4) Report INFOSEC incidents to security approval or accreditation authority, in accordance with the requirements of the SecOPs (or national equivalent(s)) and, where appropriate, the NATO CDMA CONOPS and NATO CIRC Handbook	CIS operating authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives CDMA documents
(5) For NATO *systems*, report incidents to the NATO Office of Security in accordance with the requirements of the NATO CDMA CONOPS and NATO CIRC Handbook	CIS operating authority, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives CDMA documents
(6) Undertake, in accordance with the requirements of the security approval or accreditation authority, periodic vulnerability assessments	CIS operating authority, or a separately established vulnerability assessment team, coordinating with the security approval or accreditation authority	INFOSEC Management directive INFOSEC Technical & Implementation directives and guidelines
(7) Undertake, in accordance with NATO security policy, periodic security inspections or reviews of the *system* or, where appropriate, the interconnection of *systems*	Security approval or accreditation authority, coordinating with the CIS operating authority	INFOSEC Management directive and guidelines

III.5 *System* Enhancement

50. The following INFOSEC-related activities and responsible authorities are associated with the enhancement stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) For NATO *systems*, refine the security risk assessment in accordance with the requirements of the security approval or accreditation authority	CIS planning & implementation authority or project staffs, in conjunction with the CIS operating authority and the security approval or accreditation authority	INFOSEC Management directive and guidelines
(2) For NATO *systems*, approve the results of the refined security risk assessment	Security approval or accreditation authority	INFOSEC Management directive and guidelines
(3) Identify any additional security countermeasures to be implemented. Where appropriate, develop the operational requirements for cryptographic products and mechanisms and follow the activities set out in the "*System* Development and Procurement" tables (see paragraph 47)	CIS planning & implementation authority or project staffs, in conjunction with the CIS operating authority and the security approval or accreditation authority	INFOSEC Technical & Implementation directives and guidelines
(4) Establish requirement for security test and evaluation (ST&E) of the *system* or, where appropriate, of the interconnection of *systems*	Security approval or accreditation authority, coordinating with CIS planning & implementation authority(s) & CIS operating authority	INFOSEC Management directive INFOSEC Technical & Implementation directives and guidelines
(5) Develop security test and evaluation (ST&E) plan	CIS planning & implementation authority(s), coordinating with the CIS operating authority and the security approval or accreditation authority	INFOSEC Management directive

Activity	Responsible Authority / Staffs	Document(s)
(6) Undertake, where required, a re-evaluation and re-certification of the *system* or, where appropriate, of the interconnection of *systems*; in accordance with, where appropriate, the Common Criteria Evaluation Methodology	NATO or National Evaluation & Certification Authority, coordinating with the CIS planning & implementation authority(s), the CIS operating authority and the security approval or accreditation authority	INFOSEC Technical & Implementation directives and guidelines
(7) Undertake security testing, in accordance with an agreed ST&E plan	CIS operating authority (or independent authority acting on behalf of the CIS operating authority), coordinating with the CIS planning & implementation authority(s) and the security approval or accreditation authority	INFOSEC Management directive
(8) Review results of security testing	Security approval or accreditation authority	INFOSEC Management directive
(9) Identify, as a result of the security testing, any additional security countermeasures to be implemented	Security approval or accreditation authority, coordinating with the CIS planning & implementation authority and the CIS operating authority	INFOSEC Management directive
(10) For NATO *systems*, review and agree the residual risks to be accepted	Security approval or accreditation authority, in conjunction with the CIS operating authority	INFOSEC Management directive and guidelines
(11) For NATO *systems*, review and agree the on-going security risk management processes	Security approval or accreditation authority, in conjunction with the CIS operating authority	INFOSEC Management directive and guidelines

Activity	Responsible Authority / Staffs	Document(s)
(12) Revise the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles, Packages, Common Criteria terminology and concepts	CIS operating authority, coordinating with the security approval or accreditation authority	INFOSEC Management directive and guidelines INFOSEC Technical & Implementation directives and guidelines
(13) Revise the SecOPs (or national equivalent(s)) for the CIS	CIS operating authority, coordinating with the security management staffs and the security approval or accreditation authority	INFOSEC Management directive and guidelines
(14) Re-approve the SRS(s) and SecOPs (or national equivalent(s))	Security approval or accreditation authority	INFOSEC Management directive and guidelines
(15) Re-approve or re-accredit the *system* or, where appropriate, the interconnection of *systems*; and re-publish an approval or accreditation statement	Security approval or accreditation authority	INFOSEC Management directive and guidelines
(16) Review and re-establish the re-approval or re-accreditation conditions	Security approval or accreditation authority	INFOSEC Management directive and guidelines

III.6 *System* Withdrawal from Service, and Disposal of Equipment

51. The following INFOSEC-related activities and responsible authorities are associated with the withdrawal from service, and disposal of equipment stage of a *system* :

Activity	Responsible Authority / Staffs	Document(s)
(1) Undertake the appropriate archiving or de-classification and destruction of associated fixed and removable computer storage media, and information required for accounting purposes	CIS operating authority	INFOSEC Technical & Implementation directives and guidelines
(2) Undertake the appropriate procedures for the disposal and destruction of cryptoproducts and cryptosystems and their associated material	CIS operating authority	INFOSEC Technical & Implementation directives and guidelines
(3) Undertake the appropriate archiving or destruction of associated hard copy documentation	CIS operating authority	INFOSEC Technical & Implementation directives and guidelines

SECTION IV - NATO COMMITTEES, NATO CIVIL & MILITARY BODIES, and NATIONAL BODIES - INFOSEC RESPONSIBILITIES

52. The NATO and national bodies directly or indirectly involved in INFOSEC matters are listed below. Under the ultimate authority of the North Atlantic Council (NAC), NATO Committees and their Working Groups / Sub-committees, Commands, Agencies and Staffs may be identified as follows :

(a) NATO bodies directly responsible for INFOSEC policy, directives and guidance:

- the NATO Security Committee (NSC) (AC/35) where National Security Authorities (NSAs) are represented, and its Working Group 1 on Information Assurance (AC/35(WG/1));

- the C3 Board (C3B) (AC/322), and its Information Assurance Sub-committee (SC/4);
- the Military Committee (NAMILCOM) for military requirements; and
- various NATO civil committees for their civil requirements;

(b) NATO bodies indirectly concerned with INFOSEC resources :

- the financial committees, Senior Resource Board (SRB), Infrastructure Committee (IC), Military and Civil Budget Committees (MBC and CBC) for resource funding; and
- the NATO Defence Manpower Committee for personnel aspects, in military establishments;

(c) NATO staff support in NATO Headquarters :

- the NATO Office of Security (NOS);
- the NATO Headquarters C3 Staff (NHQC3S) and its Information Assurance Branch;
- the International Staff (IS) and International Military Staff (IMS);

(d) NATO bodies representing the users :

- Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for users in military establishments; and
- specific civil agencies for civil users;

(e) NATO bodies responsible for operational and technical support to INFOSEC policy, direction and implementation bodies :

- Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for military establishments;
- the four nationally manned Military Committee agencies, for security evaluation and certification, vulnerability assessment, keying material and accounting :
  - Communications and Information Systems Security and Evaluation Agency (SECAN) - organised and staffed by the United States;

- Distribution and Accounting Agency (DACAN) - organised and staffed by the United States;
- European Communications Security and Evaluation Agency (EUSEC) - organised and staffed by the United Kingdom;
- European Distribution and Accounting Agency (EUDAC) - organised and staffed by the United Kingdom;

- the NATO C3 Agency (NC3A) for acquisition management and contracting;
- the NATO CIS Services Agency (NCSA) for assigned systems and equipment;
- the NATO Information Assurance Technical Centre (NIATC), NCSA for INFOSEC implementation, operation and maintenance in support of NATO and its subordinate commands;
- the NATO CIS School (NCISS) for education and training;
- the NATO Public Key Infrastructure (PKI) Management Authority (NPMA);
- the NATO CIS Security Accreditation Board (NSAB); and
- the NATO Cyber Defence Management Authority (CDMA) and the NATO Computer Incident Response Capability (NCIRC).

(f) National authorities and agencies :

- National Security Authorities (NSAs);
- National Communication Security Authorities (NCSAs);
- National Distribution Authorities (NDAs); and
- National Security Approval or Accreditation Authorities.

53. The security responsibilities of the NATO Security Committee (NSC), the NATO Office of Security (NOS), the NATO Military Committee (NAMILCOM) and NATO Military bodies, the C3 Board (C3B), NATO Civil bodies and National Security Authorities (NSAs) are addressed in NATO Security Policy. The INFOSEC responsibilities of NATO committees, NATO Civil and Military bodies, and National bodies with NATO INFOSEC responsibilities are addressed in the appropriate NATO and National documents, including official Terms of Reference (TORs).

54. An outline of the inter-relationships of the committees and bodies is provided at Appendix 1 to this directive.

SECTION V - NATO INFOSEC DOCUMENTATION STRUCTURE

55. This “Primary Directive on INFOSEC” is supported by a number of INFOSEC directives and guidance documents addressing INFOSEC Management, and INFOSEC Technical and Implementation aspects. A "Roadmap" to NATO Security Policy, supporting directives, supporting documents and guidance documents is available from the NATO Security Accreditation Authorities and the NATO HQ C3 Staff Information Assurance Branch; and may also be accessed on the NATO SECRET Wide Area Network (WAN) at the NOS link on the NATO HQ web site.

56. The "Roadmap" provides access to the following :

(a) NATO UNCLASSIFIED and NATO RESTRICTED documents published by the NSC and the C3B, with respect to information management, security and cyber defence;

(b) NATO committees, and NATO civil and military bodies organisation with respect to information assurance;

(c) the CIS life-cycle INFOSEC-related activities with links to the relevant text of the security documents;

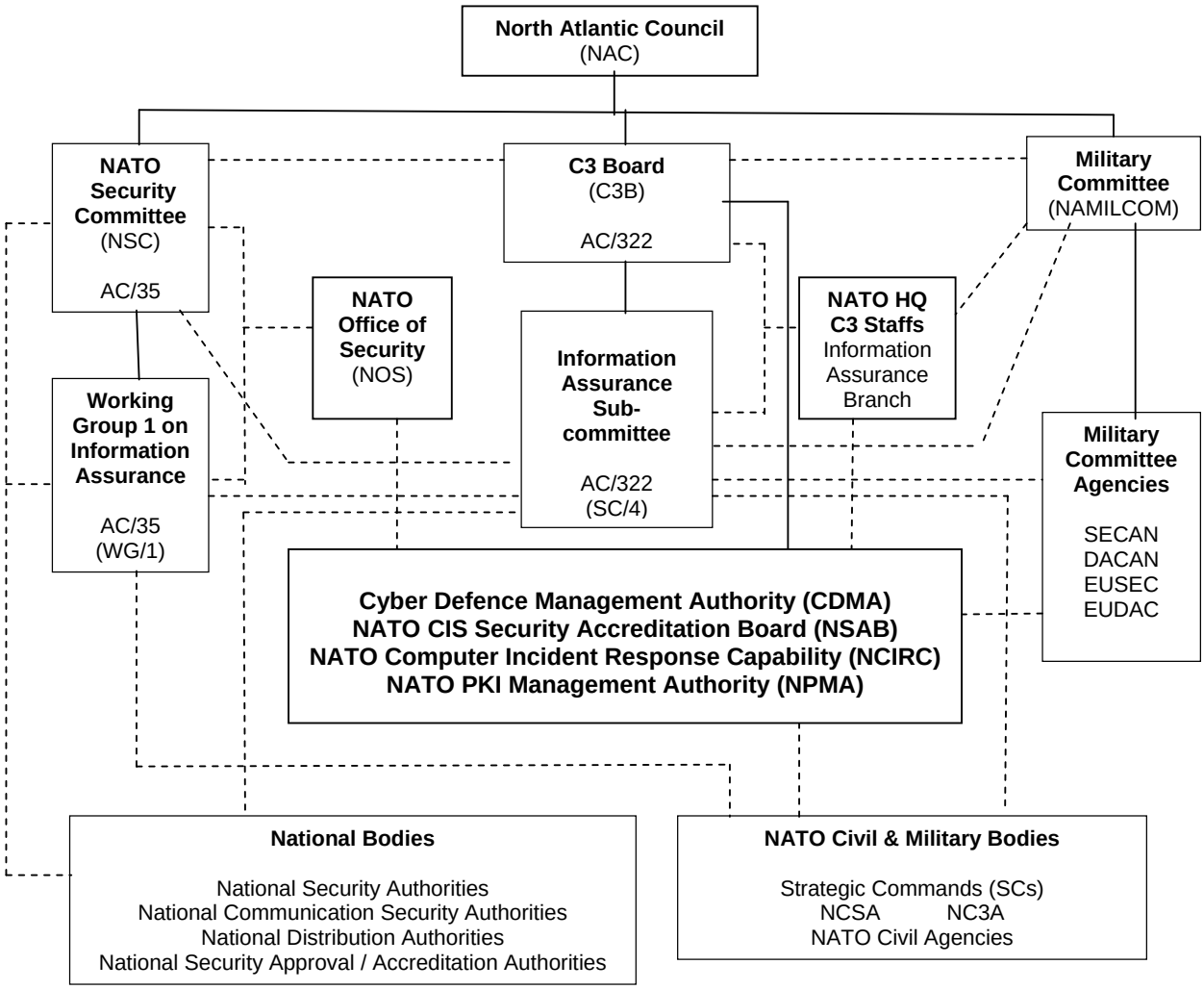
(d) contact information of NATO and National Security Authorities; and

(e) a “search by subject” index.

APPENDIX 1
ANNEX 1
AC/35-D/2004-REV2

NATO COMMITTEES, NATO CIVIL & MILITARY BODIES, NATIONAL BODIES

INTER-RELATIONSHIPS



Key ——— Committee hierarchy.

- - - - - - - Inter-relationships between committees, bodies involved in committees, working groups, Cyber Defence Management Authority (CDMA), NATO CIS Security Accreditation Board (NSAB), NATO Computer Incident Response Capability (NCIRC), and NATO PKI Management Authority (NPMA).