NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO/PFP UNCLASSIFIED

11 December 2007

DOCUMENT
C-M(2007)0118
Silence Procedure ends:
28 Jan 2008 18:00

NORTH ATLANTIC COUNCIL

THE NATO INFORMATION MANAGEMENT POLICY

Note by the Deputy Secretary General

1. The current NATO Information Management Policy was issued as an Annex to a Private Office document referenced PO(99)47 dated 17 May 1999. At the Riga Summit, Heads of State and Government agreed to support efforts to achieve Information Superiority, including the principles of the NATO Network Enabled Capability (NNEC). This agreement brought into yet sharper focus the importance of information and its effective and efficient management in a coherent, co-ordinated and synchronised manner within the Alliance, in order to support all NATO missions including NATO operations, projects, programmes, contracts and other related tasks.

2. One of the distinguishing characteristics of NNEC is the emphasis on the networking of national and NATO Consultation, Command and Control (C3) and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities to facilitate the seamless sharing of information and services to meet the Alliance's requirements. This increased emphasis on information sharing places a strain on the current NIMP, which was framed in a pre-NNEC era where the emphasis was more on information guarding rather than sharing. The current NIMP has been updated to reflect this shift in emphasis, and the resulting revised NIMP is at Annex 1.

3. The Council is invited, under the silence procedure, to:

- Approve the NATO Information Management Policy at Annex 1; and
- Agree that the NC3B is assigned as the lead Council Committee in NATO for information management.

4. Unless I hear to the contrary by **18.00 hrs on Monday, 28 January 2008**, I shall assume that the Council can agree to the actions in paragraph 3 above.

(Signed) Claudio Bisogniero

1 Annex

Original: English

ANNEX 1
C-M(2007)0118

NATO INFORMATION MANAGEMENT POLICY

INTRODUCTION

1. This C-M establishes the basic principles of information management to be applied by NATO nations and NATO civil and military bodies. This NATO Information Management Policy (NIMP) is published by the North Atlantic Council (NAC) and is authorised for public disclosure.

MISSION STATEMENT

To support NATO in the conduct of its mission by efficient and effective information management, enabling decision-making by the sharing of information within and between NATO, the Nations and their respective Communities of Interest

SCOPE

2. The NIMP establishes a framework to ensure that information is handled effectively, efficiently and securely in order to serve the interests of NATO. This includes managing all aspects of information throughout its life-cycle.

3. Within this policy, the term 'information' is used to embrace all information, including related data, required in support of NATO's missions[1], whether such information originates in NATO civil or military bodies or is received from member nations or non-NATO sources. Such information, and the media and resources used to record and process it, shall be managed in accordance with this Policy and other relevant NATO agreements and legal obligations.

OBJECTIVES

4. The key objectives of Information Management (IM) are:

   a. to support the achievement of Information Superiority primarily within an information sharing networked environment;

   b. to support the effective and efficient use of information resources in the conduct of the NATO mission; and

   c. to support the identification and preservation of information of permanent value to NATO.

PRINCIPLES

5. Information is a Corporate Resource. Information is a corporate resource and shall be managed as such to support NATO's missions, consultation, decision

[1] Missions include NATO operations, projects, programmes, contracts and other related tasks.

making processes, and operational requirements by organising and controlling information throughout its life-cycle regardless of the medium and format in which the information is held.

6. Information Ownership and Custodianship. Information shall have an originator, and clearly defined ownership and custodianship assigned throughout its life-cycle.

7. Leadership and Organisational Structure. Management of information is a fundamental responsibility, which shall require executive leadership, top-level involvement and the creation and maintenance of an effective organisational structure.

8. Information Sharing. Information shall be managed with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know', and managed to facilitate access, optimise information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations.

9. Information Standardisation. Information shall have standardised structures and consistent representations to enable interoperability, cooperation and more effective and efficient processes.

10. Information Assurance. Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.

11. Information Needs. Information needs shall be determined as part of the planning and architecture processes[2] to meet intended activities and effects.

ROLES AND RESPONSIBILITIES

12. It is the responsibility of:

a. individuals who produce or have authorised access to information to follow the principles of information management as set out in this C-M;

b. originators to apply relevant rules and standards to their product;

c. information owners[3]:

(1) to set the rules for handling the information throughout its life-cycle in line with the relevant policies and procedures;

[2] The activities of designing and maintaining a representation (i.e. blueprint) of components of a business (i.e. organisation, processes, information, technology) and their relationships in order to understand where, when and why information is required.

[3] In the NATO context, the roles of originator and owner are currently always performed by the same entity.

(2) to establish rules for the transfer of ownership.

d. Information custodians to manage and provide the information under their custodianship in accordance with the rules established by the information owners.

e. the Heads of NATO civil and military bodies:

(1) to ensure that this Policy, related policies and supporting directives are complied with within their organisation;

(2) to identify and protect essential information to ensure the continuity of key services and operations;

(3) to ensure the disposition of information in accordance with established policies and procedures;

(4) to assess the effectiveness and efficiency of the management of information throughout its life-cycle;

(5) to implement organisational, governance and accountability structures, and training programmes, for the management of information; and

(6) to appoint a senior official responsible for IM;

f. National Authorities to ensure that this Policy, related policies and supporting directives are complied with when dealing with information owned by NATO; and

g. the North Atlantic Council:

(1) to monitor compliance with, and ensure execution of, this Policy and supporting Directives by NATO civil and military bodies;

(2) to ensure the coordinated implementation of the objectives of this Policy through the offices with delegated authority for specific elements of IM including, but not limited to, the NATO Archivist and the NATO Office of Security; and

(3) to ensure appropriate coordination among all NAC Policy bodies[4] that have responsibilities for the individual elements of IM.

[4] NATO Military Committee, Political Committee, NATO Security Committee, NATO C3 Board, NATO Archives Committee

RELEASE AND PUBLIC DISCLOSURE OF INFORMATION

13. Release and public disclosure of information shall be in accordance with applicable policies and directives.

DEFINITIONS

Access:
The right, opportunity, and means of finding, using, or retrieving information.

Availability:
The property of information and material being accessible and usable upon demand by an authorised individual or entity.

Authentication:
The act of verifying the claimed identity of an entity.

Community of Interest:
A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions or business processes and who therefore must have shared vocabulary for the information they exchange.

Confidentiality:
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Disposition:
The appraisal of information to determine its long-term value and the subsequent actions (archiving or destruction) when the information is no longer needed for the conduct of the current business.

Governance
Governance is the structures and processes for decision-making, accountability, control and behaviour within organisations.

Information:
Any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Custodian:
The nation or organisation which receives information and makes it visible and is responsible to the information owner for the agreed level of safe-keeping and availability of information.

Information Management:
Information Management is a discipline that directs and supports the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organisation.

Information Owner:

The nation or organisation which creates and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions, and is the authority for the life-cycle of information.

Information Superiority:

State of relative advantage in the information domain achieved by getting the right information to the right people at the right time in the right form whilst denying an adversary the ability to do the same.

Integrity:

The property that information (including data) has not been altered or destroyed in an unauthorised manner.

Life-cycle:

The life-cycle of information encompasses the stages of planning, collection, creation or generation of information; its organisation, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition.

NATO

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

Need-to-know

The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.

Non-repudiation

Non-repudiation is the measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipient(s).

Originator:

The nation or international organisation under whose authority the information has been produced or introduced into NATO.

Responsibility-to-share

The individual and collective obligation to make information available, discoverable and accessible for those entities that require the information to perform their official tasks and services.