

NATO UNCLASSIFIED

27 February 2012

DOCUMENT
C-M(2012)0014
Silence Procedure ends:
16 Mar 2012 – 16:00

**Directive on the Management of Records Generated
on Operational Deployment**

Note by the Secretary General

1. In June 2011 the NATO Records Policy (NRP) was approved by the North Atlantic Council (C-M(2011)0043 refers). The NRP establishes the framework for managing NATO records. The NRP is an up-to-date and comprehensive Policy that applies to all NATO Civil and Military Bodies. The NRP has already been incorporated across NATO into information management training programmes and reform activities.
2. As a follow up and in the wake of Operation Unified Protector (OUP) and in anticipation of the completion of the transition process in Afghanistan, the Archives Committee (AC/324) was tasked to develop a supporting Directive on the Management of Records Generated on Operational Deployment. The purpose of this Directive is to:
 - Establish ownership and custodianship of operational records in a coalition environment;
 - Define roles and responsibilities with regard to operational records;
 - Support the planning and decision making at the strategic, operational and tactical levels;
 - Protect the interest of those contributing to and impacted by an operation;
 - Support the evaluation of a NATO operation and to provide input for “lessons learned activities”; and
 - Preserve operational records of permanent value.
3. Following its approval by the Archives Committee, in January 2012 the Military Committee endorsed the Directive and the recommendation to maintain an operational diary at the Operational Command level (IMSM-0008-2012 refers).
4. The Council is invited, under the silence procedure, to:

NATO UNCLASSIFIED

-1-



- Approve the Directive on the Management of Records Generated on Operational Deployment at annex and the recommendation to maintain an Operational Diary at the Operational Command level;
- Authorize the Directive for public disclosure.

5. Unless I hear to the contrary **by 16:00 hours on Friday, 16 March 2012**, I shall take it the Council has approved the actions in paragraph 4 above.



Anders Fogh Rasmussen

DIRECTIVE ON THE MANAGEMENT OF RECORDS GENERATED ON OPERATIONAL DEPLOYMENT

REFERENCES

- (a) C-M(2011)0043, NATO Records Policy (NRP), dated 17 June, 2011.
- (b) C-M(2007)0118, NATO Information Management Policy (NIMP), dated 11 December, 2007;
- (c) C-M(2008)0113, The Primary Directive on Information Management (PDIM), dated 18 December, 2008;
- (d) C-M(2002)49 NATO Security Policy, dated 17 June, 2002;
- (e) C-M(2009)0021, Policy on the Retention and Disposition of NATO Information, dated 2 March, 2009
- (f) AC/324-D(2011)0002, Directive on the Handling of Records During the Closure of a NATO Civil or Military Body, dated 04 July 2011

INTRODUCTION

BACKGROUND

1. Records are critical to a reliable assessment of operations both during their conduct and after their completion. Neglecting to capture, manage and preserve operational records has severe consequences for the planning and conduct of the operations. Operational records will support accountability, will help to protect the interests of the Organization, and the rights of those impacted by operations. They also assist in responding to inquiries and media requests. It is therefore NATO policy to manage and preserve operational records.

2. Records created and/or received by NATO in the context of a NATO operation are NATO records and therefore shall be managed in accordance with the NATO Records Policy (NRP). However, the complexity of military and political interrelationships at the international level and the wide spectrum of crisis situations in which these operational records are generated require specific procedures for their management. Furthermore the multinational character of NATO operations may create specific types of records which are unique to such operations¹.

¹ Examples of operational records include but are not limited to: Operational Plans (OPLANs), operational orders, incident reports, graphic intelligence summaries, battle briefings, after action reviews, situation reports and operational diaries.

3. Within this Directive, an operational record is defined as “information created or received in the course of a NATO operation and maintained as evidence and information by NATO in pursuance of legal obligations, and the conduct of military or civil emergency operations”².

4. Records management pertains to the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records. The management of records occurs during every phase of a NATO operation: planning, conduct and post-operation assessment.

SCOPE

5. This Directive is issued in support of the NATO Records Policy (ref a) and NATO’s Operations Planning³.

6. This Directive provides procedures for the management of records generated during operational deployment, regardless of media, which are related to the planning, conduct and support of NATO operations wherever that activity occurs.

7. This Directive supports the NATO Information Management Policy (NIMP) (ref b) and the Primary Directive on Information Management (PDIM) (ref c), which describe all aspects of information management at a high level.

8. Intelligence reports and assessments through and in the NATO-led chain of command that have a direct impact on the military assumptions, the planning for and the conduct of operations and activities are managed in accordance with this Directive. Raw intelligence data, will not be subject to this Directive⁴.

OBJECTIVE

9. The key purposes of operational records are:

² The term “operational record” is sometimes used in reference to the systematic recording of daily events and daily decision making process in the form of an operational diary. In this Directive however the term refers to all records created and/or received as part of a NATO operation. The operational diary of a NATO formation is an operational record and therefore shall be managed in accordance with this Directive.

³ MC 0133/4(Final) NATO’s Operational Planning.

⁴ Raw intelligence data is unprocessed data from various intelligence disciplines which may be used in the production of intelligence required for the planning and conduct of campaigns at the operational level (based on: AAP-6 (2010) NATO Glossary of Terms and Definitions) and MC 0128/7 Policy Guidance for NATO Intelligence). A separate directive on ownership, retention and disposition of intelligence information shall be developed in close cooperation with NATO intelligence and legal community.

- (a) to support planning and decision making at the strategic, operational and tactical levels;
- (b) to systematically document the activities and decisions of an operation;
- (c) to ensure accountability at all levels;
- (d) to protect the interests of the Organization;
- (e) to protect the interest of those contributing to and impacted by an operation;
- (f) to support an evaluation of a NATO operation or provide input for “lessons learned activity; and,
- (g) to preserve the operational memory and history.

APPLICABILITY

10. This Directive applies to all deployed commands and sub-commands in the theatre of operations. It also applies to the records generated by NATO nations, non-NATO nations and non-NATO entities⁵ participating in and/or contributing to a NATO operation.

POLICY and PRINCIPLES

OWNERSHIP AND CUSTODIANSHIP

11. In this Directive, ownership and custodianship of operational records and their relationship to their originators are described in the following terms:

- (a) Records generated by NATO during a NATO operation are the property of NATO. These records are subject to the provisions of Article VII of the Ottawa Agreement and/or of Article XIII of the Paris Protocol. NATO is the originator, the information owner, and the information custodian;
- (b) Records originating from Member nations participating in a NATO operation and provided to the NATO chain of command shall be maintained by NATO in accordance with this Directive. NATO is the information custodian and maintains the records in accordance with this directive, subject to originator control regarding downgrading, release and public disclosure;
- (c) Records originating from non-NATO nations participating in and/or contributing to a NATO operation and provided to the NATO chain of command shall be maintained by NATO in accordance with this Directive. NATO is the information custodian and maintains the records in accordance with this Directive, subject to originator control regarding downgrading, release and public disclosure;
- (d) Records originating from non-NATO entities⁶ in the context of a NATO operation and provided to the NATO chain of command shall be maintained by NATO in accordance with this Directive. NATO is the information custodian and maintains

⁵ The provisions, mechanisms and procedures in respect of records of NATO classified information shared with non-NATO nations and non-NATO Entities (NNNEs) (See Definitions), are clarified in the NATO Security Policy and the supporting documents.

⁶ These include but are not limited to local governments, suppliers, non-NATO nations not participating in a NATO operation, international organisations and non-governmental organisations. See also Footnote 5.

the records in accordance with this Directive, subject to originator control regarding downgrading, release and public disclosure;

- (e) Records originating from Member nations in the context of a NATO operation but not provided to the NATO chain of command are the property of the originators and shall be managed in accordance with their relevant regulations, taking into account as appropriate the requirements of the NATO Security Policy (ref d). Nations are the originators, information owners and custodians of such records. If they are shared with NATO, NATO is the information custodian, and maintains the records in accordance with this Directive, subject to originator control regarding downgrading, release and public disclosure.
- (f) Records originating from non-NATO nations and/or non-NATO entities participating in and/or contributing to a NATO operation but not provided to the NATO chain of command are the property of the originators and shall be managed in accordance with their relevant regulations, taking into account as appropriate the requirements of the NATO Security Policy. Non-NATO nations and/or non-NATO entities are the originators, information owners and custodians of such records. If they are shared with NATO, NATO is the information custodian, and maintains the records in accordance with this Directive, subject to originator control regarding downgrading, release and public disclosure.

12. During the conduct of an operation:

- (a) The Strategic Command shall ensure that the arrangements for transfer and custodianship of the records are defined and implemented;
- (b) The NATO Operational Commander shall have custodianship of active and semi-active records including those received by subordinate commands and HQs in the theatre of operations;
- (c) Records generated in the theatre of operations that are no longer required for immediate and anticipated operational purposes and their custodianship shall be transferred through the NATO military chain of command.

13. Upon termination of an operation, operational records shall be transferred to the NATO Archives, unless they are needed for lessons learned or evaluation activities by the Strategic Command or by any other headquarters in the chain of command. In this case the records are transferred to the NATO Archives when no longer required for post operational activities by these commands. Once transferred, the NATO Archives will have custody of the records.

14. Within the context of a NATO operation, national commanders shall have custody of records that they receive. These records shall be kept in a manner that is consistent with the requirements of this Directive. NATO can request access to national records or records generated by external organisations related to NATO operations.

GUIDING PRINCIPLES OF OPERATIONAL RECORDS MANAGEMENT

15. Operational records management shall ensure that records are available when and where they are needed, in an organised and efficient manner, and in a well maintained environment. Operational records shall comply with the following guiding principles:

- (a) Usable and complete: Records created on operational deployment shall be traceable and sufficient in content, context and structure. The aim should be to reconstruct and represent as much as possible the relevant activities, decisions and transactions that they document. The links among records and their metadata shall be maintained.
- (b) Comprehensive: Records generated on operational deployment shall document the complete range of activities associated with the planning for and the conduct of an operation.
- (c) Reliable: Records generated on operational deployment shall accurately reflect the activities, decisions and transactions that they document. These records shall be created at the time of the transaction or incident to which they relate, or in the context of standard operational reporting on a transaction or incident. They shall be generated by individuals who have direct knowledge of the facts or captured by instruments and processes routinely used within the operation.
- (d) Authentic: It is necessary to protect an operational record against unauthorized alteration. Standard Operation Procedures (SOP) for an operation shall specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized and who is authorized to make them. Any authorized annotation, addition to or deletion of a record shall be explicitly indicated and traceable.
- (e) Compliant: Records generated on operational deployment shall comply with records management and information management requirements resulting from NATO policies, directives, guidelines and standards.
- (f) Secure: Records generated on operational deployment shall be securely maintained to prevent unauthorised access, alteration, damage or removal. They shall be stored in a secure environment that reflects the sensitivity and importance of the contents as well as the security environment of the storage location. Regular back-ups of material shall be made and transferred through the military chain of command to the Strategic Command conducting the operation.

PLANNING AND PRE-DEPLOYMENT STAGE

16. To meet the guiding principles as outlined in paragraph 15, procedures shall be established for the management of records generated on operational deployment during the operations execution stage of the OPLAN.

17. Records generated on operational deployment shall be kept in a format most appropriate for the information item. Where possible these records shall be kept in a format to ensure long-term preservation and which is consistent with the guiding principles set out in paragraph 15d.

MANAGEMENT PROCEDURES FOR RECORDS GENERATED ON OPERATIONAL DEPLOYMENT⁷

18. Capture: Information created or received in the course of a NATO operation shall be set aside⁸ as an operational record whilst the action is still occurring, or a decision is being taken, or soon afterwards.

19. Organisation: Operational records shall be organised in a manner to ensure their retrievability, understandability, integrity and to facilitate their transfer and preservation.

20. Registration: Operational records shall be registered into a designated system to provide evidence of their creation and capture. Registration involves the recording of brief descriptive information or metadata about the operational record and the assignment of a unique identifier to facilitate its retrieval.

21. Metadata: Descriptive metadata which describes the context of a record, its content and relationships with other records shall be recorded at the time of capturing the record or as part of the registration and maintenance process. Additional metadata shall be added throughout the lifecycle of the record providing information on its use and disposition.

22. Emails, instant messages and other social media: Emails, instant messages, chats or any social media through the NATO certified communications/network environment documenting important actions or decisions relating to the operation are records and therefore shall be kept in accordance with this Directive and relevant NATO Policies.

⁷ This section has been largely based on the international standard for records and information management ISO 15489-1 (2002). Operational records management procedures are a means to capture, manage and provide access to operational records in an organised and structured fashion. It applies to both physical and electronic records. Implementing procedures will be developed to support the implementation of this section.

⁸ Set aside means saved and organized in the official repository of the operation, for example shared file servers, information, document or records management system or collaboration sites.

These messages shall be registered and captured alongside other records. This refers to both messages sent and received.

23. Emerging technologies: Information technology changes the ways and means of communication. Emerging communication tools⁹, when authorized by appropriate chain of command for use in the framework of a NATO operation, create records. These records shall be kept in accordance with this Directive.

CONTINGENCY PLANNING

24. Identifying and managing vital records: Business continuity planning and contingency planning shall ensure that records that are vital to the continued functioning of the operation are identified as part of the risk analysis, protected and recoverable when needed. These records shall be identified during the operational phase.

25. Emergency destruction: The destruction of records in case of an emergency shall be in accordance with the NATO Security Policy .

RETENTION AND DISPOSITION

26. Location: As long as actively needed for operations' purposes, operational records are available in their respective theatre of operations. Records and back-ups of the recordkeeping system no longer frequently consulted shall be transferred at regular intervals to the Strategic Command conducting the operation.

27. Life-cycle and record value¹⁰
The lifecycle of an operational record has three stages: active, semi-active and inactive. Active operational records that no longer have immediate administrative, operational and/or technical utility become semi-active, and are retained for a specific period of time in order to meet business responsibilities. After all operational needs are met, the operational record becomes inactive. Its final disposition is based on its identification as having permanent value¹¹ (transferred to and preserved by the NATO Archives) or temporary value (destroyed in compliance with the Policy on Retention and Disposition of NATO information and associated records retention schedules for operational records (ref e)).

⁹ Including but not limited to: Facebook, Twitter, Blogs and You Tube.

¹⁰ The life-cycle terminology used in the context of this Policy differs from the terms used in the NATO Information Management Policy (C-M(2008)0113), but the life cycle approaches are consistent.

¹¹ Records of permanent value include but are not limited to: Commander reports and correspondence, operation plans, incident reports, operational diary, daily intelligence summaries, battle briefings, after-action reviews, operational lessons-learned, situation reports (SITREPS), assessment reports, legal documents, logistics reports, SOPs, communication plans and command group orders.

28. Assistance: To assist with the preparation of the transfer and to facilitate records review, the NATO Archives are available to provide professional guidance and expertise on the appraisal and retention of operational records

ROLES AND RESPONSIBILITIES

Generic

29. It is the responsibility of all individuals working directly for a NATO operation or in support of a NATO-led operation to create or generate records which will adequately document the operations and activities in which they take part and to ensure that the records which they create are authentic, reliable and complete.

Specific roles

30. The Archives Committee, on behalf of the North Atlantic Council (NAC), monitors compliance with this Directive.

31. The NATO Strategic Commander is responsible for:

- (a) ensuring the compliance of this Directive;
- (b) ensuring the inclusion of operational records management principles and procedures in the applicable operational planning documents such as an OPLAN.

32. The Operational Commander and his delegates through the chain of command are responsible for:

- (a) ensuring the proper management of operational records;
- (b) ensuring the availability of resources to permit compliance with this Directive;
- (c) ensuring that records still needed for ongoing business are transferred through the chain of command in the event of the termination of an operation;
- (d) coordinating with the NATO Archivist to ensure that inactive records of permanent value which are no longer required by the Strategic Command and its subordinate headquarters are transferred to the NATO Archives in the event of the termination of a NATO operation.

33. Commanders of national formations are responsible for ensuring that operational records of the national formation pertaining to a NATO operation are maintained in a manner that is consistent with the requirements of this Directive or comparable national standards.

34. The NATO Archivist, on behalf of the Archives Committee, is responsible for:

- (a) developing, revising, implementing, monitoring and approving retention schedules applicable to operational records;
- (b) providing guidance to and coordinating with the commands involved in the operation on records matters, systems and programmes;

- (c) developing, implementing and monitoring records training programmes for information managers and archivists of NATO civil and military bodies;
- (d) raising awareness of the importance of operational records and their proper management, storage and disposition; and,
- (e) reporting regularly to the Archives Committee on operational records management.

35. Archivists or other personnel in positions with information management responsibilities within the NATO command structure are responsible for: establishing and maintaining the operational records management procedures and ensuring their implementation in any operational system that generates or holds NATO records.

DEFINITIONS

Authentic record

A record that can be proven to be what it purports to be, that has been created or sent by the person purported to have created or sent it, and that has been created or sent at the time purported (Source: ISO 15489-1 Records Management).

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 (Source: C-M(2007)0118).

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 (Source: C-M(2007)0118).

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 the information (Source: C-M(2007)0118).

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 29th 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.

NATO Archives

The service mandated, under the authority of the NATO Archivist, to identify, preserve and provide access to NATO information of permanent value, produced or received by the Organisation in the course of its activities or by its staff members in the performance of

their duties, irrespective of date, form and storage medium. The NATO Archives is currently based at NATO HQ (Source: C-M(2009)0021(INV)).

NATO Operation

Any NATO or NATO-led security, peace support, crisis response, and/or disaster relief operation involving NATO and/or Partners and other non-NATO nations.

Non-NATO entity

Categories of non-NATO entities are defined in AC/35-D/1040-REV2 Supporting Document on Information and Intelligence Sharing with non-NATO entities.

Operational Command (OPCOM)

The authority granted to a commander to assign missions or tasks to subordinate commanders, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as the commander deems necessary (Source: AAP- 06 (2010).

Operational Commander

The Commander granted the authority to assign missions or tasks to subordinate commanders, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as the commander deems necessary (Based on AAP- 06 (2010).

Operational record

Information created or received in the course of a NATO operation and maintained as evidence and information by NATO in pursuance of legal obligations, and the conduct of military or civil emergency operations (Based on: ISO 15489-1 Records Management).

Operation Plan (OPLAN)

A plan for a single or series of connected operations to be carried out simultaneously or in succession. It is usually based upon stated assumptions and is the form of directive employed by higher authority to permit subordinate commanders to prepare supporting plans and orders. The designation "plan" is usually used instead of "order" in preparing for operations well in advance. An operation plan may be put into effect at a prescribed time, or on signal, and then becomes the operation order (Source: AAP- 06 (2010).

Originators

The nation or international organisation under whose authority the information has been produced or introduced into NATO (Source: C-M(2007)0118).

Records management

Records management or also referred to as recordkeeping is a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of an information about business activities and transactions in the forms of records (Source: ISO 15489-1 Records Management).

Records life-cycle

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

Strategic Command

The command organization at the highest level of the NATO military command structure. Note: There are currently two strategic commands, namely, Allied Command Operations and Allied Command Transformation (Source: AAP- 06(2010)).

Strategic Commander

The commander at the highest level of the NATO military command structure. Note: The NATO strategic commander responsible for the planning and execution of NATO operations is SACEUR (Based on AAP- 06 (2010)).