NATO STANDARD

ADatP-4774

CONFIDENTIALITY METADATA LABEL SYNTAX

Edition A Version 1

DECEDMBER 2017

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED DATA PROCESSING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

20 December 2017

1. The enclosed Allied Data Processing Publication ADatP-4774, Edition A, Version 1, CONFIDENTIALITY METADATA LABEL SYNTAX, which has been approved by the nations in the Consultation, Command, and Control Board (C3B), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4774.

2. ADatP-4774, Edition A, Version 1, is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
DNK	Under certain exceptional circumstances exemptions may be made where compliance to STANAG 4774 adversely affect the accomplishment of missions or would cause major adverse financial impact which may also impact acquisitions of systems, equipment and services of C4IS.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

1 Introduction

1.1 Background

The NATO Information Management Policy [C-M(2007)0118] guides the establishment of an IM Framework for 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. The NATO Security Policy [C-M(2002)0049] and supporting directives cover all aspects concerning the secure handling of information.

In accordance with the NATO Interoperability Policy [Source C-M(2009)0145] standards are to support interoperability between NATO, the Nations and their respective Communities of Interest to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objective, especially to support the achievement of Information Superiority within an information sharing networked environment.

This ADatP-4774 is published by the Consultation, Command and Control Board (C3B) and is authorized for public disclosure. It supports the cooperation with external actors in line with the Lisbon Summit decisions on the Comprehensive Approach as well as the following principles of the NATO Information Management Policy and NATO Network Enabled Capability (NNEC) Strategies for Data and Technical Services [AC/322-D(2005)0053-REV2, dated14 Sept 2009]:

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

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.

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

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.

Data Assurance. The authority of the source and integrity of the data can be determined and assessed because of the history, security level, and access control level of each data asset is known and available.

The Military Committee recommendation on the Implementation of the NATO Federated Mission Networking Capability [MCM-0106-2014] provides the framework for establishing information sharing in a federated networked environment in support of coalition operations. The NATO mission environment is evolving from network-centric based security architecture to Data-Centric based security architecture.

1.2 Objective

The objective of this document is to provide common XML-based formats and syntax for security policies and confidentiality metadata. Information objects and data assets can be labelled to support access and release decisions in a manner that is understandable to all coalition partners.

This document provides the semantics for a common security policy based on agreed NATO Security Policy and supporting directives.

1.3 Scope

This document addresses aspects of information management that are required to enable the security of information sharing. Technical implementation of this standard will require detailed implementation profiles specific to usage scenarios where technology permits. These profiles are published in ADatP-34 (NATO Interoperability Standards and Profiles).

1.4 Assumptions

This document was developed using the following assumptions and constraints:

- National Security Policies will not change through the application of this standard;
- This standard must reflect National Security Policies;
- Information sharing in a federated networked environment is based on an agreed Common Security Policy;
- A Common Security Policy must be adjustable to reflect event specific requirements; and
- Equivalencies between National Security Policies and a commonly agreed security policy can be defined.

2 Confidentiality Metadata Label Requirements

2.1 Overview

Nations and some organisations implement organisational specific information security policies. Typically these policies support one or more of the following objectives:

- Achieve and maintain protection of information determined by its confidentiality;
- Ensure that information receives an appropriate level of protection;
- Prevent unauthorized disclosure, modification, removal or destruction of information, and interruption to the organisation's activities.

In the physical paper-based information environment, confidentiality is represented by markings[1], usually at the top and bottom of a page, and sometimes also applied to portions of the information such as titles or paragraphs, also known as portion-marking. Those markings are typically specific to the language and context of the originating organisation and not universally understood (e.g. CONFIDENTIAL, ПОВЕРИТЕЛНО, 机密). Under NATO policy, marking shall be displayed in English or French, see Ref 1.

In the digital environment, confidentiality must be encoded as a machine-readable *confidentiality metadata label.* A confidentiality metadata label may be used to:

- Determine access limitations;
- Support appropriate protection during transmission of information;
- Enable appropriate markings to be rendered for display, printing, etc.;
- Support the selection of the appropriate retention and disposition procedures;
- Support the redaction and sanitization of information.

Typically, the information owner has the authority for setting the rules for handling the information and for protecting the integrity and confidentiality throughout its lifecycle. If the information owner shares the information with another entity, that entity (information custodian) is responsible to the information owner for the agreed level of protection of the received information.

2.2 Common Security Policy

When information is shared between different entities three general scenarios are possible:

1. Sharing of information between entities governed by different security policies;
2. Sharing of information between entities governed by the same security policies;

[1] Security Markings are defined in Reference 2, Appendix A. These are often referred to as Security Markings with no differentiation in meaning or intent.

3. Sharing of information with entities not governed by a formally defined security policy.

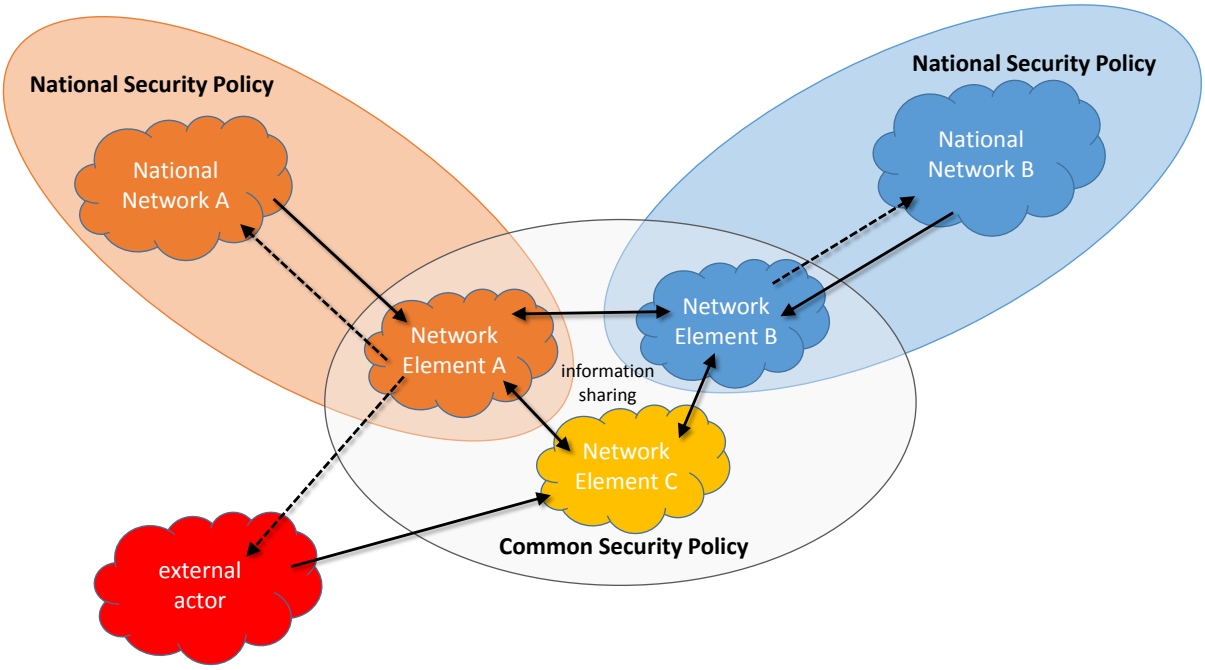

Figure 1: Information sharing scenarios

Before information is shared between entities that are governed by different security policies, formal agreements for the exchange of information are established. Information Exchange Agreements typically include a minimum set of security or protection controls that reflect the organisational information security policies and the type of the information involved. These agreements are the prerequisite to information sharing and thereby contribute to the establishment of a trust between entities; however, they must be enabled through a common understanding, by all entities, of each other's confidentiality metadata labels.

If there are multiple entities (*n* = number of entities) that want to share information the approach of individual bilateral agreements would result in each entity would need to understand *n* confidentiality metadata labels, i.e. n*(n-1)/2 agreements. When a new entity enters this circle of trust all existing entities are affected and *n* new bilateral agreements would have to be established. Even for a group as small as three entities it would be more effective to establish a single common security policy for that group, each entity would then only have to understand its own and the common policy and would be unaffected by new entities joining the group.

Note that in the common security policy case, information may be exchanged in a circular way, which would result in an information owner receiving their own information from another entity. This situation leads to a requirement for information to permanently maintain its original confidentiality metadata label.

2.3 Requirements

To enable information sharing in the different scenarios described above, this standard meets the following minimum requirements:

1. Express the confidentiality requirements throughout the IM lifecycle, regardless of the format of the information, or the medium on which it is processed and transmitted;
2. Provide the ability to express security policies in a common syntax;
3. Provide the ability to designate the security policies to be applied to the handling of information (i.e. policy identifier) (See Appendix 1);
4. Support at least two security policies in parallel (See Appendix 1 and the Alternative Confidentiality Label);
5. Express agreed equivalency relationship between different security policies to support the concept of Alternative Confidentiality Label(s) (See Appendix 1);
6. Provide a security policy for information from external actors that do not have a recognized security policy (See Appendix 2, Annex C and D);
7. Provide the ability to indicate the ownership of the information (See Appendix 1 and the concept of Context or Ownership);
8. Provide the ability to indicate categories required to specify protection and distribution in accordance with the approved security policies including classification, releasability, privacy mark, need-to-know, Community of Interest and administrative designators (See Appendix 2);
9. Provide the ability for applications and services to create confidentiality metadata labels at any point in the information life-cycle;
10. Provide the ability to render human readable markings consistent with the respective security policies (See Appendix 1 and Appendix 2);
11. Support automated handling decisions including release of information (See Appendix 2 and the Release To category type); and
12. Provide the ability to indicate changes to protection of the confidentiality of the information due to succession requirements such as downgrading and distribution reduction or expansion (See Appendix 1).

INTENTIONALLY BLANK

3 Terms and Definitions

Alternative Confidentiality Label: An Alternative Confidentiality Label is assigned to a data object when that data object is shared across boundaries that have different Governing Security Policies. In this case, the Alternative Confidentiality Label provides the equivalent labelling information in the recipient Governing Security Policy. The Alternative Confidentiality Label is provided in addition to the Originator Confidentiality Label.

Attributes: Named properties of an element that may carry different values depending upon the context in which they occur. Attributes modify the meaning of the elements to which they apply. [Library of Congress/Society of American Archivists].

Binding: A relationship between information and its metadata such as confidentiality metadata labels that provides an appropriate level of assurance of the integrity of the association between the information and the metadata.

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. [Source: C-M(2008)0113]

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes. [Source: C-M(2007)0118]

Confidentiality Metadata Label: A set of metadata representing the collection of confidentiality elements and attributes that indicate the sensitivity of the information. It is represented with a structure and a controlled Value Domain that can be automatically processed to determine the sensitivity of the information to which it refers.

Need-to-Know (Principle): 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 [Source: C-M(2009)0035 (INV)].

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 audio-visual forms. [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 information. [Source: C-M(2007)0118]

Integrity: The property that information (including data) has not been altered or destroyed in an unauthorized manner. [Source: C-M(2008)0113]

Metadata: Structured information that describes, explains, locates and otherwise makes it easier to retrieve and use an information resource (i.e. data object). The structure consists of ‘elements’, each of which contains ‘values’. The values relate to the resource itself; there may be controls over what the actual values can be. [C-M(2002)049]

Security Marking: A visual (i.e. displayable) representation of the sensitivity of an object intended for human processing e.g. the Security Marking associated with a document as indicated by information inserted in the header and footer, a visual marking attached to a device, etc. A Security Marking may be rendered from the Confidentiality Metadata Label associated with an object.

Value Domain: The set of permissible values for an element or attribute. Value domains for Confidentiality Metadata Labels and Security Markings are specified in Reference 1 that is considered the authoritative source.

3.1 Abbreviations

C3	Consultation, Command and Control
COI	Community of Interest
NNEC	NATO Network Enabled Capability
NATO	North Atlantic Treaty Organization
URL	Uniform Resource Locator
XML	eXtensible Markup Language
JPEG	Joint Photographic Experts Group

4 Labelling

4.1 Introduction

This chapter addresses the labelling requirements specified in the References. It defines the syntax for confidentiality metadata labels that satisfy the following primary requirements:

- Can be bound to any type of information;
- Is adaptable to Security Policy changes;
- Supports the recognized security requirements for all types of information (unmarked, unclassified and classified);
- Supports the protection of information from creation to deletion, regardless of the format of the information, or the medium on which it is processed and transmitted;
- Supports Alliance coalitions, missions and exercices;
- Indicates the security policy to be applied (i.e. policy identifier);
- Indicates the classification of the information;
- Indicates categories required to specify distribution in accordance with the approved security policy including ownership, releasability, dissemination limitation, need-to-know and administrative designators;
- Indicates the succession requirements for future information handling e.g. downgrading and reduced or expanded distribution; and
- Supports the handling of information originating from other security domains.

This chapter uses the key words (e.g., SHALL, SHOULD, MAY) defined in RFC 2119 [10] to define the requirement levels for specific parts of confidentiality metadata label syntax.

4.2 Concepts and Terminology

Security Marking: Physical objects (documents, devices and equipment) carry a security marking that identifies the sensitivity of the information and, in the case of a document, is normally written on the front coversheet and in page headers and footers. Some documents carry additional marking abbreviations (e.g. NU, NR, NS) at the start of each paragraph, diagram or section. Problematically, these security markings are manually applied and therefore subject to variation.

A Confidentiality Metadata Label is a set of metadata representing the collection of confidentiality elements and attributes of the information that indicate the security safeguards applied to the information. A Confidentiality Metadata Label is represented with a structure and a controlled Value Domain that can be

electronically processed. The Confidentiality Metadata Label which is the subject of this standard is detailed in Appendix 1.

Confidentiality Metadata Labels may be bound to portions of the information, including paragraphs, sections, figures and tables. The following primary elements are included in the Confidentiality Metadata Label:

a. Governing Security Policy – the Security Policy Authority is identified within each label;

b. Classification – since information may be classified, unclassified or unmarked, every label includes a single value identifying the classification level of the information;

c. Privacy Mark – is used to convey operational instructions, warnings or notifications of significance to the user or custodian of the data object. Privacy Mark is a legacy element that is used for backward compatibility;

d. Category – provides restriction and/or expansion of the dissemination within the scope of the classification of the information.
The categories are:

- Restrictive – e.g. BOHEMIA
- Permissive – e.g. RELEASABLE TO ISAF
- Informative – e.g. PERSONAL

The definition of these categories can be seen in Table 7: Category Types. The Category element allows subcategories to be defined. The subcategories defined for the purpose of this standard are identified in Table 1: Defined Subcategories below.

Table 1: Defined Subcategories

Context	In combination with the Governing Security Policy context indicates the "Ownership", as defined in (Reference 1). Information can be created in the context of co-operative activities, e.g. EAPC, in which the Governing Security Policy is applied.
Releasable To	Used to expand the dissemination of information to additional entities outside of the context for which that information was created.

Only	Used to restrict or limit the dissemination of information to specific entities and a sub-set of the entities within the context for which that information was created.
Additional Sensitivity	Used to indicate the sensitive nature of certain NATO information not conveyed by the Ownership or Classification; meaning that it is subject to additional stringent security regulations and procedures.
Administrative	Used to indicate discretionary handling according to local, non-automated procedures or provide guidance about the disposition of information

4.3 Succession Handling

The Succession Handling provides a mechanism to indicate the confidentiality metadata label that will be applicable at a certain time in the future. This can be used to meet Information Management requirement to capture the expected downgrading of the data object prior to the policy default (e.g. 30 years)

The access control decision, in accordance with the Governing Security Policy, may need to take into account the Succession Handling.

In the absence of any *SuccessionHandling* element, a *ReviewDateTime* SHALL be specified to indicate when the confidentiality metadata label shall be reviewed.

The review process SHOULD append Succession Handling elements in order to maintain a confidentiality metadata label history.

The Succession Handling consequently also includes the confidentiality metadata label history, including the original confidentiality metadata label that was specified.

4.4 Syntax

The Confidentiality Metadata Label Syntax is based upon the label description from IETF RFC 2634 (Reference [8]) and includes additional refinements to support requirements for Information Assurance and Information Management (i.e. succession handling for disposition and retention).

The Confidentiality Metadata Label Syntax utilises the eXtensible Markup Language (XML) to represent a confidentiality metadata label.

An XML representation provides an open and flexible mechanism that can be integrated with a wide variety of data types and is aligned with the federation approach for Alliance coalitions.

An XML schema is defined which contains each of the elements of the Confidentiality Metadata Label.

The elements of the XML schema are described in the Appendix 1.

INTENTIONALLY BLANK

5 Policy

5.1 Introduction

For confidentiality metadata labels to be used effectively and consistently within a networking environment, there must be a well-defined mapping of the security policy onto the appropriate confidentiality metadata label elements. This ensures that the appropriate semantics (according to the security policy) are observed and applied.

This chapter describes the Value Domains for the *ConfidentialityInformation* and its child elements in order to support effective and consistent application.

The NATO Security Policy has been adopted as the basis for the Governing Security Policy for this chapter and subsequent appendixes.

A second Security Policy is defined to support the ingestion of information from public sources or private sources where confidentiality metadata labels are not provided. This decision supports the initiation of a coalition, mission or exercise at Day-0.

ConfidentialityInformation

Table 2 specifies the *ConfidentialityInformation* elements and the defined *Category* elements, in support of the NATO Security Policy. The Value Domains for these elements are provided in Reference 1.

Table 2: *Confidentiality Information* Elements in the NATO Security Policy

Element	
PolicyIdentifier	
Classification	
Privacy Mark	
Category	**tagName**
	"Context"
	"Only"
	"Releasable To"
	"Additional Sensitivity"
	"Administrative"

Table 3: Value Domains for Confidentiality Information Elements in the PUBLIC Policy

Element		Value Domain
PolicyIdentifier		"PUBLIC"
Classification		"UNMARKED"
Privacy Mark		Not Used
Category	**tagName**	
	"Administrative**"**	Reference 1 & C-M(2002)60 Para 9

All values within the *ConfidentialityInformation* element are treated as case insensitive during processing.

For example, "Top Secret" and "TOP SECRET" are equivalent.

All values used in the *ConfidentialityInformation* element use the English terms.

NATO policy states that markings must be English or French however the confidentiality metadata label will enable security markings to be generated in any alternate language through the appropriate conversion of label values.

Each of the *ConfidentialityInformation* elements as used for the NATO Security Policy are described in further detail in Appendix 2.

For specific coalitions, missions or exercises, it is expected that the Value Domain for the Context subcategory will be extended. Value domain extensions may also be provided for the Releasable To, Limited Dissemination, Additional Sensitivity or Administrative categories.

Within the NATO enterprise, the Context along with the Governing Security Policy, indicates the dissemination of NATO information to NATO nations, or non-NATO nations depending upon the context in which the NATO information was created.

The use of the "NATO Security Policy" as the "Governing Security Policy" has the following constraints:

- The *CreationDateTime* element SHALL be present in a confidentiality metadata label;
- In the absence of any *SuccessionHandling* element, a *ReviewDateTime* SHALL be specified to indicate when the confidentiality metadata label shall be reviewed;
- The *ReviewDateTime* attribute SHALL be present when no *SuccessionHandling* element is present;

- If the *ReviewDateTime* attribute does not impact the validity of the Confidentiality Metadata Label i.e. if the *ReviewDateTime* attribute specifies a date in the past, the *ConfidentialityLabel* element SHALL still be deemed valid.; and
- The URI, if it is present, SHALL use the urn scheme with an oid namespace identifier to provide an equivalent of the policy identified by the *PolicyIdentifier* element content.

If the *SuccessionHandling* element is not present then the *ReviewDateTime* attribute SHALL be present.

INTENTIONALLY BLANK

6 References

[1] Guidance on the Marking of NATO Information, June 2011, AC/322-N(2011)0130 REV1.

[2] The Primary Directive on Information Management, 18 December 2008, C-M(2008)0113 (INV).

[3] Security Within the North Atlantic Treaty Organisation, 17 June 2002, C-M(2002)049.

[4] C-M(2002)60 The management of Non-Classified NATO Information, 11 July 2002

[5] Directive on the Security of Information, 17 January 2012, AC/35-D/2002-REV4.

[6] AC/322-D(2004)0021 (INV), “INFOSEC Technical and Implementation Guidance for Electronic Labelling of NATO Information”, March 2004

[7] NATO Core Metadata Specification (NCMS), AC/322-D(2014)0010, 14 January 2014.

[8] IETF RFC 2634, “Enhanced Security Services for S/MIME”, at http://tools.ietf.org/html/rfc2634, June 1999.

[9] IETF RFC 5913, “Clearance Attribute and Authority Clearance Constraints Certificate Extension”, at http://tools.ietf.org/html/rfc5913, June 2010.

[10] IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, at http://tools.ietf.org/html/rfc2119, March 1997.

[11] STANAG 4406 Edition 2, “Military Message Handling System (MMHS)”,Brussels, Belgium, (NATO/EAPC Unclassified)

INTENTIONALLY BLANK

APPENDIX 1: Confidentiality Metadata Label Schema

Introduction

This appendix defines the syntax of the Confidentiality Metadata Label for use within NATO Alliance coalitions, operations, exercises and training.

Metadata that uses the Confidentiality Metadata Label syntax SHALL be appropriately bound to the information to which it relates.

The Confidentiality Metadata Label syntax can be used to specify the o*riginatorConfidentialityLabel, metadataConfidentialityLabel* and an *alternativeConfidentialityLabel* metadata associated with Information.

The *originatorConfidentialityLabel* Element

The *originatorConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains the confidentiality label which the originator of a data object associated with that data object.

The *originatorConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *alternativeConfidentialityLabel* Element

The *alternativeConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains an equivalent representation, in an alternative policy, of the *originatorConfidentialityLabel*

The *alternativeConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *MetadataConfidentialityLabel* Element

The *metadataConfidentialityLabel* element is of type *ConfidentialityLabelType*. It contains the confidentiality label that is assigned to the metadata set associated with the data object.

The *metadataConfidentialityLabel* element may be used by reference in other XML schemas, or within XML documents whose schemas allow any XML elements.

The *ConfidentialityLabelType* Type

The *ConfidentialityLabelType* type is an extension of the *ConfidentialityLabelBaseType* type. It extends the *ConfidentialityLabelBaseType* by adding two optional attributes; *Id* and *ReviewDateTime (*see Figure 2*)*.

The optional *Id* attribute can be used to provide a unique identifier for the confidentiality metadata label. Uniqueness is only guaranteed within one instance XML document.

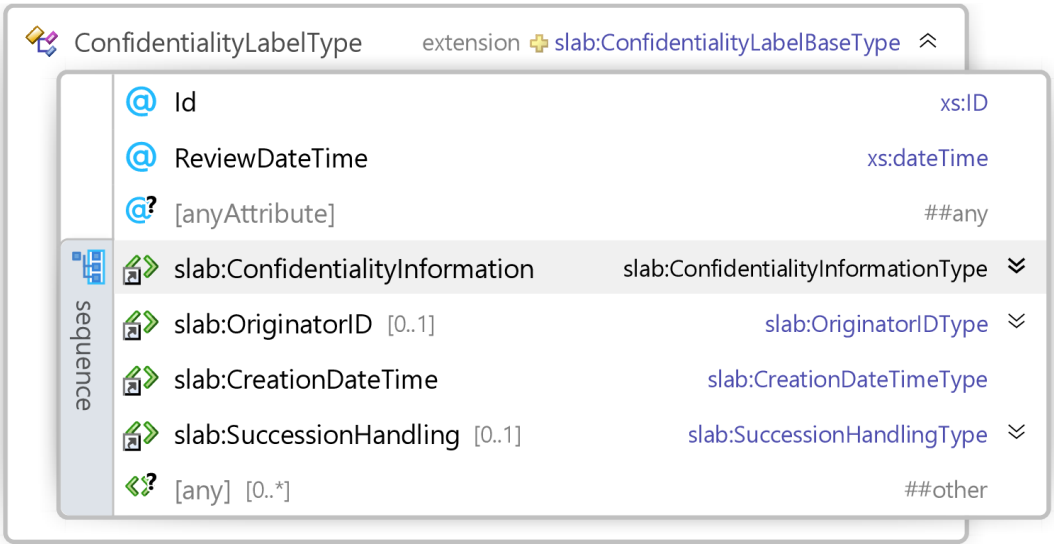

Figure 2: The ConfidentialityLabelType Type

The optional *ReviewDateTime* attribute, refers to the date when the confidentiality metadata label should be manually reviewed i.e. in support of archiving and disposition of the data object.

The *ReviewDateTime* attribute SHALL be present when no *SuccessionHandling* element is present.

The *ReviewDateTime* attribute SHALL not impact the validity of the confidentiality metadata label i.e. if the *ReviewDateTime* attribute specifies a date in the past, the confidentiality metadata label SHALL still be deemed valid.

Table 4: Attributes of the *ConfidentialityLabelType* Type prescribes the use of attributes of the *ConfidentialityLabelType* type:

Table 4: Attributes of the *ConfidentialityLabelType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
Id	Optional	Unique identifier of this element instance	“Label-3”, “958700be-280a-4758-a3c5-303c2d898b3e”

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
ReviewDateTime	Optional	XML schema type ‘dateTime’ . This attribute is mandatory if SuccessionHandling is not present.	“2015-01-01T09:00:00”, “2013-04-01T11:59:59”

The *ConfidentialityLabelBaseType* Type

The *ConfidentialityLabelBaseType* type contains a mandatory *ConfidentialityInformation* (of type *ConfidentialityInformationType*) and *CreationDateTime* (of type *CreationDateTimeType*) elements and optional *OriginatorID* (of type *OriginatorIDType*) and *SuccessionHandling* (of type *SuccessionHandlingType*) elements (see Figure 3).

The *OriginatorID* element SHOULD contain information about the originator of the confidentiality metadata label.

Note that the *OriginatorID* element may be different to the creator of the Information (for example, a service may create and bind a confidentiality metadata label to information created by another user or service).

The *CreationDateTime* element can be used to express the date and time of the original classification by the originator.

Note that the *CreationDateTime* of the confidentiality metadata label may be different to the time at which the information itself was created.

The *SuccessionHandling* element allows the originator to define a confidentiality metadata label that will succeed the current confidentiality metadata label at the specified date and time.

This meets the information management requirement for appraisal, retention and disposition of information and the operational requirement to indicate information that may have a temporal or transient value.

Additional elements may be included in the *ConfidentialityLabel* element to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

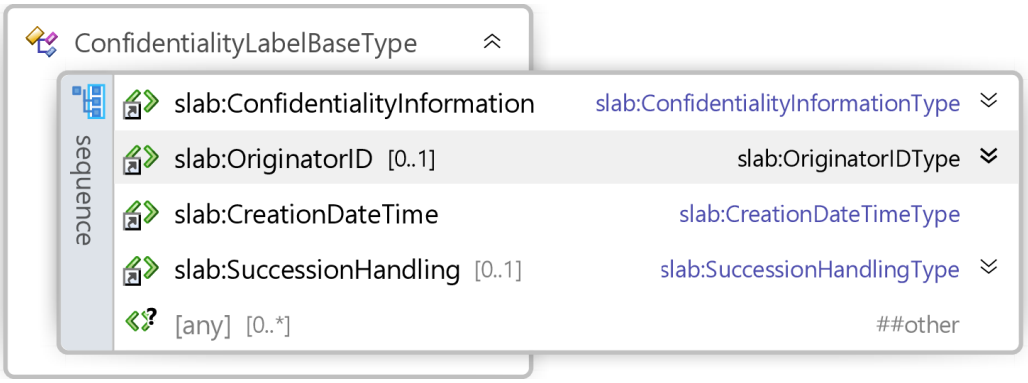

Figure 3: The ConfidentialityLabelBaseType Type

The *ConfidentialityInformationType* Type

The *ConfidentialityInformationType* type contains mandatory *PolicyIdentifier* (of type *PolicyIdentifierType*) and *Classification* (of type *ClassificationType*) elements and optional *PrivacyMark* (of type *PrivacyMarkType*) and *Category* (of type *CategoryType*) elements (see Figure 4).

The *PolicyIdentifier element* is used to uniquely identify the Governing Security Policy Authority which manages the security policy to which the confidentiality label relates and indicates the semantics of the other confidentiality label elements and attributes

The *PolicyIdentifier* element also provides an indication of the information domain that governed creation of the data item.

The set of values for the *Classification* element, and the use of these values, are defined by the Security Policy Authority (identified in the *PolicyIdentifier* element).

The set of values for the *PrivacyMark* element may be defined by the Governing Security Policy Authority (identified in the *PolicyIdentifier* element) in force (which may define a list of values to be used) or determined by the originator of the confidentiality label. The element may be used to convey information concerning operational instructions, warnings, notifications or other issues identified in the transmission or storage of the object.

The *PrivacyMark* content MAY be COI specific values (e.g. “CLEAR”) or an arbitrary string defined by the originator.

The *Category* elements provide further granularity for the sensitivity of the information, but may be conditional on the value of the *Classification* element, as determined by the Security Policy Authority (identified in the *PolicyIdentifier* element).

Additional elements may be included in the *ConfidentialityInformationType* type to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

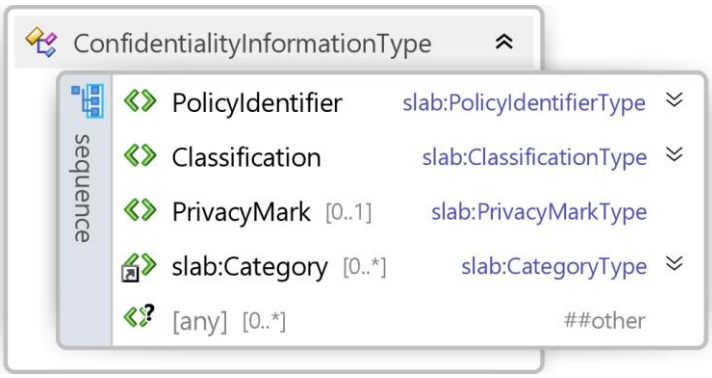

Figure 4: The ConfidentialityInformationType Type

The PolicyIdentifierType Type

The *PolicyIdentifierType* content is a textual identifier for the security policy.

The *PolicyIdentifierType* type contains a single optional attribute; *URI* (see Figure 5).

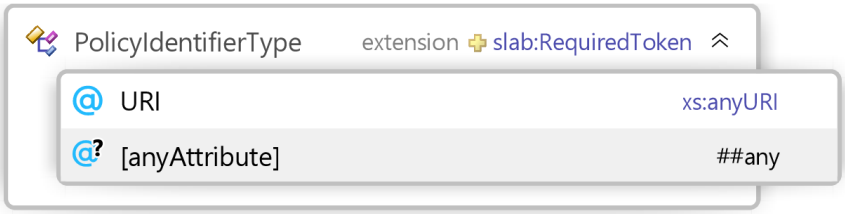

Figure 5: The *PolicyIdentifierType* Type

Additional attributes may be included in the *PolicyIdentifier* element to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The *URI* attribute provides the opportunity to use a unique identification of the policy without any ambiguity that may be associated with a textual identifier.

The *URI* attribute MAY be present, and if it is present, it SHALL use the urn scheme with an oid namespace identifier to provide an equivalent of the policy identified by the PolicyIdentifier element content.

Table 5 prescribes the use of attributes of the *PolicyIdentifierType* type:

Table 5: Attributes of the *PolicyIdentifierType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
URI	Optional	The URI SHALL follow the "urn" scheme using an "oid" namespace identifier.	"urn:oid:1.3.26.1.3.1" "urn:oid:1.2.840.113549.1.9.16.7.1"

The ClassificationType Type

The *ClassificationType* content is a registered textual identifier for the classification within the security policy.

Figure 6: The ClassificationType Type

The *Classification* element contains a single optional attribute; URI (see Figure 6). The optional URI attribute SHALL NOT be used.

Additional attributes may be included in elements of type *ClassificationType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

Table 6 prescribes the use of attributes of the *ClassificationType* type:

Table 6: Attributes of the *ClassificationType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
"URI"	Prohibited		N/A

The PrivacyMarkType Type

The *PrivacyMarkType* type is a simple string which contains no additional elements or attributes. The string contains the privacy mark value.

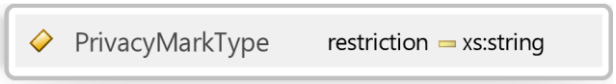

Figure 7: The *PrivacyMarkType* Type

The CategoryType Type

The *CategoryType* type contains one optional *CategoryValue* element.

The *CategoryType* type contains two mandatory attributes, *Type* and *TagName*, and one optional attribute, *URI* (see Table 8).

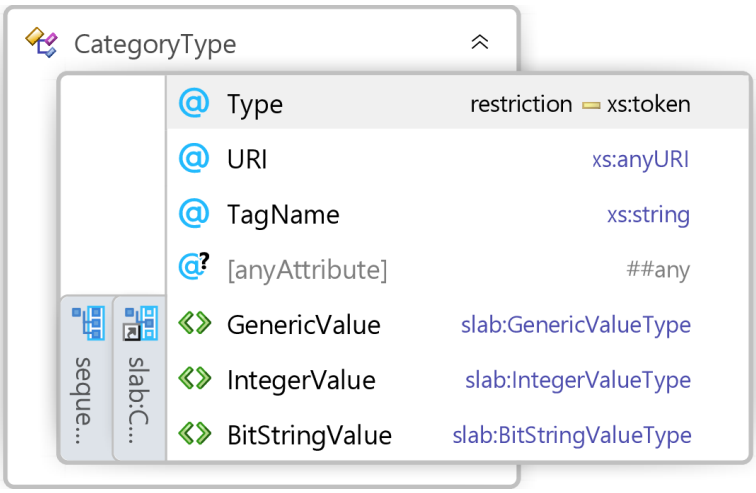

Figure 8: The *CategoryType* Type

Additional attributes may be included in elements of type *CategoryType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The mandatory *Type* attribute can take one of the three values; “RESTRICTIVE”, “PERMISSIVE” or “INFORMATIVE”.

Table 7: Category Types

Category Type	Description
RESTRICTIVE	Restrictive category types reduce the scope of dissemination. This type is used for access control decisions.
PERMISSIVE	Permissive category types are used to provide explicit inclusion sets for the purpose of access control

INFORMATIVE	Informative category types are not used for access control decisions and are provided to improve information handling.

The mandatory *TagName* attribute contains the name of the category tag that is applicable as specified in Table 2.

The set of values for the *TagName* attribute, and the use of these values, are defined by the security policy in force (identified in the *PolicyIdentifier* element) and generally refer to a grouping of categories (Table 2). The values for *TagName* attribute are addressed in Chapter 5.

The *URI* attribute provides the opportunity to use a unique identification of the category tag name without any ambiguity that may be associated with a textual identifier.

The *URI* attribute MAY be present and if it is present, it SHALL use the urn scheme with an OID namespace identifier to provide an equivalent of the policy identified by the *PolicyIdentifier* element content.

Table 8 prescribes the use of attributes of the *CategoryType* type:

Table 8: Attributes of the *CategoryType* Type

Attribute	Mandatory/ Optional/ Prohibited	Notes	Example values
Type	Mandatory		“PERMISSIVE”, “RESTRICTIVE”, “INFORMATIVE”
TagName	Mandatory		“Releasable to”, “Context”, “Only”, “Additional Sensitivity”, “Administrative”
URI	Optional	The URI SHALL adhere to the “urn” scheme using an “oid” namespace identifier to provide a machine-readable equivalent to the applicable category tag set.	“urn:oid:1.3.26.1.4.1”, “urn:oid:1.3.26.1.4.3”

The CategoryValueType Type

The *CategoryValueType* type is declared to be abstract and so cannot be present in a confidentiality label directly.

The *CategoryValueType* type contains three elements in a substitution group; *GenericValue*, *IntegerValue* and *BitStringValue*.

The *GenericValue* element SHALL be used as the substitution for the *CategoryValueType* of a *CategoryValue* element.

The *IntegerValue* and *BitStringValue* elements SHALL NOT be used as a substitution for the *CategoryValue* element.

The set of values for the *GenericValue* elements, and the use of these values, are defined by the security policy in force (identified in the *PolicyIdentifier* element) and the category tag (identified in the *TagName* attribute).

The *OriginatorIDType* Type

The *OriginatorIDType* type contains one mandatory attribute, *IDType* (see Figure 9).

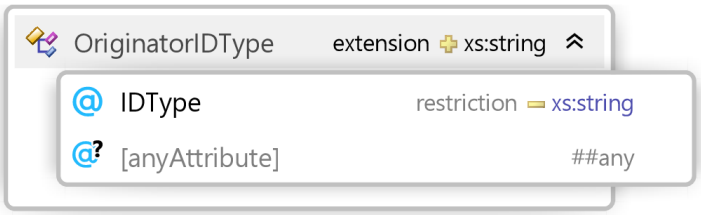

Figure 9: The *OriginatorIDType* Type

Additional attributes may be included in the elements of type *OriginatorIDType* to support COI and National features and requirements.

These additional attributes are for local use and MAY be ignored by other systems.

The allowed values for the *IDType* attribute, together with a brief description and an example for the *OriginatorID* value are shown below:

Table 9: Values for the IDType Attribute of OriginatorID

IDType	Description	Example Value
“rfc822Name”	An Internet electronic mail address.	john.doe@ncia.nato.int
“dNSName”	An Internet domain name.	ncia.nato.int
“directoryName”	A distinguished name encoded as a string.	cn=John Doe, ou=NCIA, o=NATO

IDType	Description	Example Value
“uniformResource Identifier”	A Uniform Resource Identifier (URI) for the World Wide Web.	http://www.ncia.nato.int/
“iPAddress”	An Internet Protocol address.	192.168.0.1
“x400Address”	An O/R address encoded as a string.	/cn=John Doe /OU=NCIA /O=NATO /PRMD=NMS /C=OO/
“jID”	An XMPP address.	doe@ncia.nato.int/mobile
“userPrincipalNam e”	An Internet-style user name format defined by Microsoft.	john.doe@nr.ncia.nato.int

The *SuccessionHandlingType* Type

The SuccessionHandlingType type contains mandatory *SuccessionDateTime* (of type *SuccessionDateTimeType*) and *SuccessorConfidentialityLabel* (of type *ConfidentialityLabelBaseType*) elements (see Figure 10).

Additional elements may be included to support COI and National features and requirements.

These additional elements are for local use and MAY be ignored by other systems.

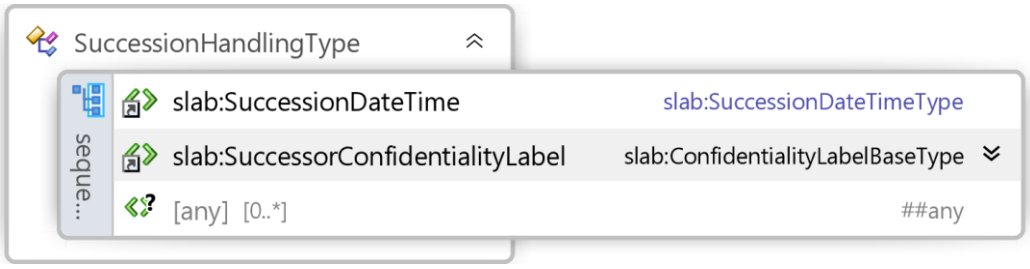

Figure 10: The SuccessionHandlingType Type

The SuccessionDateTime Type

The *SuccessionDateTime* type is an XML datetime string which contains no additional elements or attributes (see Figure 11). The datetime string contains the succession date time value.

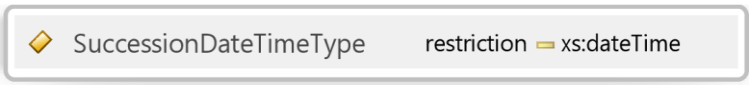

Figure 11: The *SuccessionDateTime* Type

The CreationDateTime Type

The *CreationDateTime* type is an XML datetime string which contains no additional elements or attributes (see Figure 12). The datetime string contains the creation date time value.

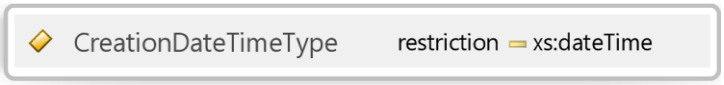

Figure 12: The *CreationDateTime* Type

INTENTIONALLY BLANK

ANNEX A: Schema

A schema has been defined that may be used to verify the validity of the confidentiality label.

The schema has the following namespace urn:nato:stanag:4774:confidentialitymetadatalabel:1:0.

The schema is registered in the NATO Metadata Registry and Repository (NMRR) and also the U.S. Metadata Repository (US MDR) using the above namespace.

The schema for the Confidentiality Metadata Label is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
**************************************************************************

                NATO UNCLASSIFIED

XML Schema for capturing the Confidentiality Label specification for
confidentiality labels and their succession history.

        I
       / \
      -< + >-
       \ /
        I             NCI AGENCY
  ##   #   ####   #     P.O. box 174
  ##   #   #   #   #     2501 CD The Hague
  # # #   #       #
  # # #   #   #   #     Core Enterprise Services
  #   ##   ####   #
    A  G  E  N  C  Y

**************************************************************************
-->

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  targetNamespace="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
  version="1.3"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:annotation>
    <xs:appinfo>
      <UniqueIdentifier>
                urn:nato:stanag:4774:confidentialitymetadatalabel:1:0
            </UniqueIdentifier>
      <Name>Confidentiality Label Schema</Name>
      <Definition>Schema for a confidentiality label</Definition>
      <VersionIndicator>1.3</VersionIndicator>
      <UsageGuidance>
                Used within NATO for representing a confidentiality label.
            </UsageGuidance>
      <RestrictionType/>
```

```
      <RestrictionValue/>
      <ConfidentialityLabel ReviewDateTime="2019-04-01T09:00:00Z">
        <ConfidentialityInformation>
          <PolicyIdentifier>NATO</PolicyIdentifier>
          <Classification>UNCLASSIFIED</Classification>
          <Category Type="PERMISSIVE" TagName="Context">
            <GenericValue>NATO</GenericValue>
          </Category>
        </ConfidentialityInformation>
        <CreationDateTime>2014-04-01T09:00:00Z</CreationDateTime>
      </ConfidentialityLabel>
    </xs:appinfo>
    <xs:documentation>
      The schema can be used with the metadata binding schema to bind confidentiality label metadata (such as
those defined in the NATO Core Metadata Specification NCMS)) to data objects.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="ConfidentialityLabelType" id="confidentialityLabelType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityLabelType
          </UniqueIdentifier>
        <Name>Confidentiality Label Type</Name>
        <Definition>
A type that is used as the base for the confidentiality label metadata elements.
        </Definition>
        <VersionIndicator>1.3</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
      <xs:extension base="slab:ConfidentialityLabelBaseType">
        <xs:attribute name="Id" type="xs:ID"/>
        <xs:attribute name="ReviewDateTime" type="xs:dateTime"/>
        <xs:anyAttribute processContents="lax"/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <!-- For backwards compatibility only -->
  <xs:element name="ConfidentialityLabel" type="slab:ConfidentialityLabelType"/>

  <!-- Standard NCMS metadata -->
  <xs:element name="originatorConfidentialityLabel"
    type="slab:ConfidentialityLabelType"/>
  <xs:element name="alternativeConfidentialityLabel"
    type="slab:ConfidentialityLabelType"/>
  <xs:element name="metadataConfidentialityLabel"
    type="slab:ConfidentialityLabelType"/>

  <xs:complexType name="ConfidentialityLabelBaseType"
    id="confidentialityLabelBaseType">
```

```
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityLabelBaseType
        </UniqueIdentifier>
        <Name>Confidentiality Label Base Type</Name>
        <Definition>
A type that is used as the base for the confidentiality label and successor confidentiality label elements.
        </Definition>
        <VersionIndicator>1.3</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="slab:ConfidentialityInformation"/>
      <xs:element ref="slab:OriginatorID" minOccurs="0"/>
      <xs:element ref="slab:CreationDateTime"/>
      <xs:element ref="slab:SuccessionHandling" minOccurs="0"/>
      <xs:any processContents="lax" namespace="##other" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="ConfidentialityInformation"
    type="slab:ConfidentialityInformationType"/>

  <xs:complexType name="ConfidentialityInformationType"
    id="confidentialityInformationType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:confidentialityInformationType
        </UniqueIdentifier>
        <Name>Confidentiality Information Type</Name>
        <Definition>
A type that describes the basic sensitivity information of policy, classification, privacy mark and categories.
        </Definition>
        <VersionIndicator>1.2</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="PolicyIdentifier" type="slab:PolicyIdentifierType"/>
      <xs:element name="Classification" type="slab:ClassificationType"/>
      <xs:element name="PrivacyMark" type="slab:PrivacyMarkType" minOccurs="0"/>
      <xs:element ref="slab:Category" minOccurs="0" maxOccurs="unbounded"/>
      <xs:any processContents="lax" namespace="##other" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
```

```
  </xs:complexType>

  <xs:element name="PolicyIdentifier" type="slab:PolicyIdentifierType"/>

  <xs:complexType name="PolicyIdentifierType" id="policyIdentifierType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:policyIdentifierType
        </UniqueIdentifier>
        <Name>Policy Identifier Type</Name>
        <Definition>
The Security Policy Authority, which in trun defines the value domain for the other elements within the
Confidentiality Information.
        </Definition>
        <VersionIndicator>1.2</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
      <xs:extension base="slab:RequiredToken">
        <xs:attribute name="URI" type="xs:anyURI"/>
        <xs:anyAttribute processContents="lax"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:simpleType name="RequiredToken" id="requiredToken">
    <xs:restriction base="xs:token">
      <xs:minLength value="1"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="Classification" type="slab:ClassificationType"/>

  <xs:complexType name="ClassificationType" id="classificationType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:classificationType
        </UniqueIdentifier>
        <Name>Classification Type</Name>
        <Definition>The basic hierarchical indication of  sensitivity.</Definition>
        <VersionIndicator>1.2</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
      <xs:extension base="slab:RequiredToken">
```

```
      <xs:attribute name="URI" type="xs:anyURI"/>
      <xs:anyAttribute processContents="lax"/>
    </xs:extension>
  </xs:simpleContent>
 </xs:complexType>

 <xs:element name="PrivacyMark" type="slab:PrivacyMarkType"/>

 <xs:simpleType name="PrivacyMarkType" id="privacyMarkType">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:privacyMarkType
    </UniqueIdentifier>
    <Name>Privacy Mark Type</Name>
    <Definition>
Additional information for the end user on the handling of the associated data object.
    </Definition>
    <VersionIndicator>1.2</VersionIndicator>
    <UsageGuidance></UsageGuidance>
    <RestrictionType></RestrictionType>
    <RestrictionValue></RestrictionValue>
   </xs:appinfo>
   <xs:documentation>

   </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:string"/>
 </xs:simpleType>

 <xs:element name="Category" type="slab:CategoryType"/>

 <xs:complexType name="CategoryType" id="categoryType">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:categoryType
    </UniqueIdentifier>
    <Name>Category Type</Name>
    <Definition>
The more granular indication of sensitivity, over and above the classification.
    </Definition>
    <VersionIndicator>1.2</VersionIndicator>
    <UsageGuidance></UsageGuidance>
    <RestrictionType></RestrictionType>
    <RestrictionValue></RestrictionValue>
   </xs:appinfo>
   <xs:documentation>

   </xs:documentation>
  </xs:annotation>
  <xs:sequence minOccurs="0" maxOccurs="unbounded">
   <xs:element ref="slab:CategoryValue"/>
  </xs:sequence>
  <xs:attribute name="Type" use="required">
   <xs:simpleType>
    <xs:restriction base="xs:token">
     <xs:enumeration value="RESTRICTIVE"/>
     <xs:enumeration value="PERMISSIVE"/>
```

```
        <xs:enumeration value="INFORMATIVE"/>
       </xs:restriction>
     </xs:simpleType>
   </xs:attribute>
   <xs:attribute name="URI" type="xs:anyURI" use="optional"/>
   <xs:attribute name="TagName" type="xs:string" use="required"/>
   <xs:anyAttribute processContents="lax"/>
 </xs:complexType>

 <xs:element name="CategoryValue" type="slab:CategoryValueType" abstract="true"/>

 <xs:simpleType name="CategoryValueType" id="categoryValueType">
   <xs:restriction base="xs:string"/>
 </xs:simpleType>

 <xs:element name="GenericValue" type="slab:GenericValueType"
   substitutionGroup="slab:CategoryValue"/>

 <xs:simpleType name="GenericValueType" id="genericValueType">
   <xs:restriction base="slab:CategoryValueType"/>
 </xs:simpleType>

 <xs:element name="IntegerValue" type="slab:IntegerValueType"
   substitutionGroup="slab:CategoryValue"/>

 <xs:simpleType name="IntegerValueType" id="integerValueType">
   <xs:restriction base="slab:CategoryValueType">
     <xs:pattern value="[0-9]+"/>
   </xs:restriction>
 </xs:simpleType>

 <xs:element name="BitStringValue" type="slab:BitStringValueType"
   substitutionGroup="slab:CategoryValue"/>

 <xs:simpleType name="BitStringValueType" id="bitStringValueType">
   <xs:restriction base="slab:CategoryValueType">
     <xs:pattern value="[0-1]+"/>
   </xs:restriction>
 </xs:simpleType>

 <xs:element name="OriginatorID" type="slab:OriginatorIDType"/>

 <xs:complexType name="OriginatorIDType" id="originatorIDType">
   <xs:annotation>
     <xs:appinfo>
       <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:originatorIDType
       </UniqueIdentifier>
       <Name>Originator ID Type</Name>
       <Definition>
The originator of the confidentiality label, which may be different to the originator of the data object.
       </Definition>
       <VersionIndicator>1.2</VersionIndicator>
       <UsageGuidance></UsageGuidance>
       <RestrictionType></RestrictionType>
       <RestrictionValue></RestrictionValue>
     </xs:appinfo>
     <xs:documentation>
```

```
      </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="IDType" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="rfc822Name" />
              <xs:enumeration value="dNSName" />
              <xs:enumeration value="directoryName" />
              <xs:enumeration value="uniformResourceIdentifier" />
              <xs:enumeration value="iPAddress" />
              <xs:enumeration value="x400Address" />
              <xs:enumeration value="userPrincipalName" />
              <xs:enumeration value="jID" />
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute processContents="lax"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:element name="CreationDateTime" type="slab:CreationDateTimeType"/>

  <xs:simpleType name="CreationDateTimeType" id="creationDateTime">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:creationDateType
        </UniqueIdentifier>
        <Name>Creation Date Time Type</Name>
        <Definition>The time at which the confidentiality label was created, which may be different to the time the
data object was created.</Definition>
        <VersionIndicator>1.2</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:dateTime"/>
  </xs:simpleType>

  <xs:element name="SuccessionHandling" type="slab:SuccessionHandlingType"/>

  <xs:complexType name="SuccessionHandlingType" id="successionHandlingType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:successionHandlingType
        </UniqueIdentifier>
        <Name>Classification Type</Name>
        <Definition>
The proposed confidentiality label at a subsequent date.
        </Definition>
        <VersionIndicator>1.2</VersionIndicator>
```

```
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="slab:SuccessionDateTime"/>
      <xs:element ref="slab:SuccessorConfidentialityLabel"/>
      <xs:any namespace="##any" processContents="skip" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="SuccessionDateTime" type="slab:SuccessionDateTimeType"/>

  <xs:simpleType name="SuccessionDateTimeType" id="successionDateTimeType">
    <xs:annotation>
      <xs:appinfo>
        <UniqueIdentifier>
urn:nato:stanag:4774:confidentialitymetadatalabel:1:0:appinfo:successionDateTimeType
        </UniqueIdentifier>
        <Name>Succession Date Time Type</Name>
        <Definition>
The proposed date at which a proposed successorConfidentialityLabel should come in to force.
        </Definition>
        <VersionIndicator>1.2</VersionIndicator>
        <UsageGuidance></UsageGuidance>
        <RestrictionType></RestrictionType>
        <RestrictionValue></RestrictionValue>
      </xs:appinfo>
      <xs:documentation>

      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:dateTime"/>
  </xs:simpleType>

  <xs:element name="SuccessorConfidentialityLabel" type="slab:ConfidentialityLabelBaseType"/>

</xs:schema>
```

ANNEX B: Examples

This section contains fictitious examples that illustrate the use of the confidentiality label.

The values shown in these examples follow those defined in Reference 1

This example shows the use of permissive categories with the *GenericValue* elements grouped according to the category tag name:

```
<slab:originatorConfidentialityLabel
  xmlns:slab=”urn:nato:stanag:4774:confidentialitymetadatalabel:1:0”>
      <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
            <slab:Classification>UNCLASSIFIED</slab:Classification>
            <slab:Category Type="PERMISSIVE" TagName="Releasable to">
                  <slab:GenericValue>SWE</slab:GenericValue>
                  <slab:GenericValue>FIN</slab:GenericValue>
                  <slab:GenericValue>RUS</slab:GenericValue>
            </slab:Category>
      </slab:ConfidentialityInformation>
      <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of restrictive and informative categories; the *GenericValue* elements are grouped according to category tag name:

```
<slab:originatorConfidentialityLabel
  xmlns:slab=”urn:nato:stanag:4774:confidentialitymetadatalabel:1:0”>
      <slab:ConfidentialityInformation>
            <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
            <slab:Classification>CONFIDENTIAL</slab:Classification>
            <slab:Category Type="RESTRICTIVE" TagName="Special Category Designators">
                  <slab:GenericValue>ATOMAL</slab:GenericValue>
                  <slab:GenericValue>CRYPTO</slab:GenericValue>
            </slab:Category>
            <slab:Category Type="INFORMATIVE" TagName="Administrative">
                  <slab:GenericValue>MEDICAL</slab:GenericValue>
            </slab:Category>
      </slab:ConfidentialityInformation>
      <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of the *OriginatorID* elements.

```
<slab:originatorConfidentialityLabel
  xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
     Id="ID_1" ReviewDateTime="2001-12-17T09:30:47Z">
     <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
          <slab:Classification>RESTRICTED</slab:Classification>
          <slab:Category TagName="Releasable To" Type="PERMISSIVE">
               <slab:GenericValue>SWE</slab:GenericValue>
               <slab:GenericValue>FIN</slab:GenericValue>
          </slab:Category>
     </slab:ConfidentialityInformation>
  <slab:OriginatorID IDType="rfc822Name">lunt@ncia.nato.int</slab:OriginatorID>
     <slab:CreationDateTime>2015-01-01T09:00:00Z</slab:CreationDateTime>
</slab:originatorConfidentialityLabel>
```

This example shows the use of the *SuccessionHandling* element.

```
<slab:originatorConfidentialityLabel
  xmlns:slab=”urn:nato:stanag:4774:confidentialitymetadatalabel:1:0”>
     <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
          <slab:Classification>SECRET</slab:Classification>      </slab:ConfidentialityInformation>
     <slab:CreationDateTime>2015-08-29T16:15:00Z</slab:CreationDateTime>
     <slab:SuccessionHandling>
          <slab:SuccessionDateTime>2015-01-01T09:00:00Z</slab:SuccessionDateTime>
          <slab:SuccessorConfidentialityLabel>
               <slab:ConfidentialityInformation>
                    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
                    <slab:Classification>RESTRICTED</slab:Classification>
               </slab:ConfidentialityInformation>
          </slab:SuccessorConfidentialityLabel>
     </slab:SuccessionHandling>
</slab:originatorConfidentialityLabel>
```

APPENDIX 2: NATO Security Policy Confidentiality Labels

Introduction

The confidentiality label schema defined in Appendix 1 of this ADatP specifies the syntax for confidentiality labels and provides the semantics for the values a confidentiality label may contain. In other words, the confidentiality label schema is a generic framework for storing any confidentiality label values that supports multiple different security policies.

PolicyIdentifier

The *PolicyIdentifier* element indicates the security policy authority and the semantics of the values of the other *ConfidentialityInformation* elements.

A single policy is used across NATO and all North Atlantic Council (NAC)-approved activities and has the value "NATO"[2].

The corresponding attributes for Policy element are:

Table 10: Attributes for the Policy Element

Attribute	Value
URI	"urn:oid:1.3.26.1.3.1"

For example,

<PolicyIdentifier>NATO</PolicyIdentifier>

Classification

The *Classification* element indicates the sensitivity of the content of the data object to which the confidentiality label is bound.

The Value Domain for the Classification element within the NATO Security Policy are specified in Reference 1.

For example,

<Classification>RESTRICTED</Classification>

The *Category* elements that are valid within a *ConfidentialityInformation* element are dependent upon the selected values in the *Classification* element, as provided in Reference 1.

Note that when generating a security marking from a Confidentiality Label containing a "TOP SECRET" classification, the *PolicyIdentifier* element MUST be displayed as "COSMIC" instead of "NATO"

[2] When rendering the *PolicyIdentifier* element as a marking, if the *Classification* element is "Top Secret", it is rendered as "COSMIC" rather than "NATO".

PrivacyMark

The Value Domain of the privacy mark is the single value “CLEAR”

The “CLEAR” value is defined to support the Clear Service specified in STANAG 4406 Ed. 2 [11].

The privacy mark is used for information only and not used to make an access control decision.

For example,

<PrivacyMark>CLEAR</PrivacyMark>

Categories

Introduction

The NATO Security Policy [1] defines five Security categories:

Table 11: Security Categories for the NATO Security Policy

Value	Definition
“Context”	The context under which the NATO information was originated including NAC-approved activities.
“Releasable To”	Further dissemination of NATO information beyond the context in which it was created.
“Only”	Restriction of the dissemination of the NATO Information by the originator to some of the non-NATO members of the context.
“Additional Sensitivity”	Additional handling requirements.
“Administrative”	The type of the NATO Information and the corresponding need for limited access.

The “Context”, “Only” and “Releasable To” Category tags support the dissemination of NATO information Nations and groupings.

Figure 13 shows how these Categories and the PolicyIdentifier are used to support the dissemination of NATO information to Nations, together with example security markings.

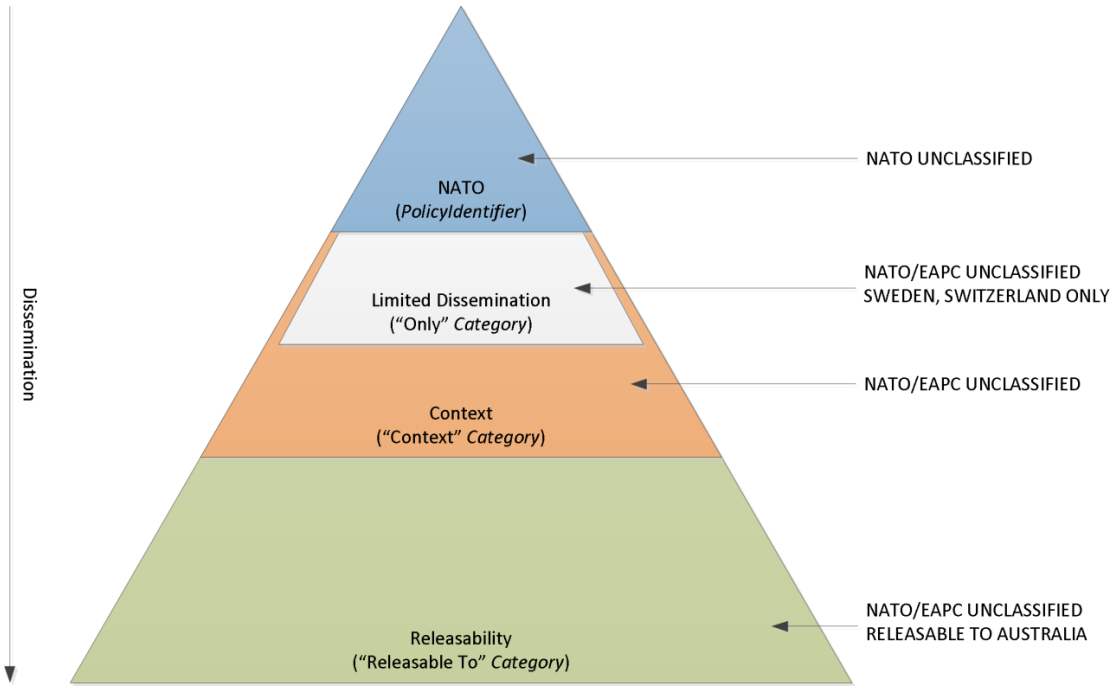

Figure 13: Category and PolicyIdentifier Role for Information Dissemination

The area of the triangle in Figure 13 represents the scope of the dissemination of the NATO information for the corresponding confidentiality label.

The *PolicyIdentifier* sets the dissemination to a core set of Nations, the NATO Nations.

The "Context" *Category* may refine the dissemination to a subset of the NATO Nations and a set of Non-NATO Entities.

The *"*Only*"* *Category* limits the dissemination to a sub-set of the Nations identified by the "Context" Category.

The "Releasable To" *Category* expands the dissemination to include additional Nations and grouping, in addition the Nations identified by the "Context" *Category*.

All of the categories are described in the following sections.

Context

NATO information may be originated in the context of a NAC approved activity with Nations, and in which the NATO Security Policy is still to be applied.

The context in which the NATO information is originated may determine the dissemination of the information, beyond the set of NATO Nations.

The combination of the NATO policy identifier and the context constitutes the "Ownership", as defined in Reference 4.

The context is held within a “Context” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Context” category element are:

Table 12: Attributes for the Context Category Element

Attribute	Value
tagName	“Context”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.4”

The “Context” category MUST be present within a NATO Security Policy *ConfidentialityInformation* element.

The “Context” category Value Domain relate to two specific elements:

1. A mandatory context identifying a set of Nations and optional a set of Non-NATO Entities;
2. An optional indication that the information may be released beyond the context.

The values in the “Context” Value Domain represent the context in which the information was created.

As the membership of NATO and NAC-approved activities has changed over time (and may again in the future) the dissemination of the NATO information originated in that context will also change.

For example, information generated before a Nation became a member of NATO should not automatically be disseminated to that Nation when it becomes a member of NATO.

Each value in the “Context” Value Domain therefore includes a suffix which distinguishes between the different memberships of NATO or the NAC-approved activities.

In general use, only the “Context” Category value for NATO or a NAC-approved activity with the highest suffix shall be used.

The Value Domain[3] of the “Context” Category within the NATO Security Policy is specified in Reference 1.

The “Context” Category SHALL contain a single value from the Value Domain.

Where a *ConfidentialityInformation* element contains a “Releasable To” Category the “Context” Category SHALL include the additional value “Releasable”.

[3] Note that these values within this value domain still need to be verified to ensure that all historical contexts have been identified.

For example,

```
<ConfidentialityInformation>
   <PolicyIdentifier>NATO</PolicyIdentifier>
   <Classification>RESTRICTED</Classification>
   <Category tagName=”Context” type=”PERMISSIVE”>
      <GenericValue>EAPC</GenericValue>
      <GenericValue>Releasable</GenericValue>
   </Category>
   <Category tagName=”Releasable To” type=”PERMISSIVE”>
      <GenericValue>EAPC</GenericValue>
      <GenericValue>JPN</GenericValue>
   </Category>
</ConfidentialityInformation>
```

Note, the “Releasable” value supports the release decision process and is not displayed with any corresponding security marking.

Only

The dissemination of information generated by NATO or a NATO approved activity may be limited by the originator to a subset of the Nations identified by the context.

The Limited Dissemination values are grouped into an “Only” category within the *ConfidentialityInformation* element.

The corresponding attributes for the Limited Dissemination category element are:

Table 13: Attributes for the Limited Dissemination Category Element

Attribute	Value
tagName	“Only”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.5”

The Value Domain for the “Only” category are those Nations that are members of the context identified by the “Context” *Category* together with the NATO Context values and the “Releasable To” category values.

For example, the following confidentiality label limits the distribution to only the NATO member Nations together with Armenia and Austria (and not the other Nations identified by the EAPC context).

```
<ConfidentialityInformation>
   <PolicyIdentifier>NATO</PolicyIdentifier>
   <Classification>RESTRICTED</Classification>
   <Category tagName=”Context”, type=”PERMISSIVE”>
      <GenericValue>EAPC</GenericValue>
   </Category>
   <Category tagName=”Only” type=”PERMISSIVE”>
      <GenericValue>ARM</GenericValue>
```

```
      <GenericValue>AUT</GenericValue>
      <GenericValue>NATO</GenericValue>
   </Category>
</ConfidentialityInformation>
```

There may be zero, one or more “Only” Category values within a NATO policy *ConfidentialityInformation* element.

Releasable To

NATO information that is intended to be further disseminated outside the context within which it was created shall include Releasability values.

The Releasability values are grouped into category element within the *ConfidentialityInformation* element.

The corresponding attributes for the Releasability category element are:

Table 14: Attributes for Releasability Category Element

Attribute	Value
tagName	“Releasable To”
type	“PERMISSIVE”
URI	“urn:oid:1.3.26.1.4.2”

The Value Domain for the “Releasable To” category are those Nations that are not members of the context, together with approved grouping of entities including entities in an accompanying “Only” category (see Reference 1).

For example, the following confidentiality label extends the dissemination to Georgia and New Zealand as well as the EAPC member Nations.

```
<ConfidentialityInformation>
   <PolicyIdentifier>NATO</PolicyIdentifier>
   <Classification>RESTRICTED</Classification>
   <Category TagName=”Context”, Type=”Permissive”>
      <GenericValue>EAPC</GenericValue>
      <GenericValue>Releasable</GenericValue>
   </Category>
   <Category TagName=”Releasable To” Type=”PERMISSIVE”>
      <GenericValue>EAPC</GenericValue>
      <GenericValue>GEO</GenericValue>
      <GenericValue>NZL</GenericValue>
   </Category>
</ConfidentialityInformation>
```

There may be zero, two[4] or more “Releasable To” Category values within a NATO policy Confidentiality Label element.

Additional Sensitivity

The sensitive nature of certain NATO information means that it is subject to additional stringent security regulations and procedures.

The Additional Sensitivity values are grouped into an “Additional Sensitivity” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Additional Sensitivity” category element are:

Table 15: Attributes for the Additional Sensitivity Category Element

Attribute	Value
tagName	“Additional Sensitivity”
type	“RESTRICTIVE”
URI	“urn:oid:1.3.26.1.4.1”

Note that the tagName “Additional Sensitivity” corresponds to the “Category Designator” in Reference 4.

Reference 1 specifies the Value Domains for the “Additional Sensitivity” category.

For example,

```
<Category TagName=”Additional Sensitivity” Type=”RESTRICTIVE”>
   <GenericValue>ATOMAL</GenericValue>
   <GenericValue>BOHEMIA</GenericValue>
</Category>
```

There may be zero, one or more “Additional Sensitivity” category values within a NATO policy *ConfidentialityInformation* element.

Administrative

Administrative markings indicate discretionary handling according to local, non-automated procedures or provide information about the disposition of information.

Administrative values may only be applied to NATO information by the originator.

The Administrative values are grouped into an “Administrative” category within the *ConfidentialityInformation* element.

The corresponding attributes for the “Administrative” category element are:

[4]There will be at least one value to identify the context, and one value to identify the additional dissemination.

Table 16: Attributes for the Administrative Category Element

Attribute	Value
tagName	“Administrative”
type	“INFORMATIVE”
URI	“urn:oid:1.3.26.1.4.3”

Administrative Markings are defined in Reference 2 and are consequently valid only within *ConfidentialityInformation* elements that have a *Classification* element of “UNCLASSIFIED”.

Note that the *tagName* “Administrative” corresponds to the “Administrative Marking” in Reference 4.

Reference 1 specifies the Value Domain for the “Administrative” category.

For example,

```
<Category TagName=”Administrative” Type=”INFORMATIVE”>
   <GenericValue>COMMERCIAL</GenericValue>
   <GenericValue>MANAGEMENT</GenericValue>
</Category>
```

There may be zero, one or more “Administrative” category values within a NATO policy *ConfidentialityInformation* element.

Examples

Table 17 shows example markings from Reference 4, together with the equivalent confidentiality label.

Table 17: Example - Security Marking and Equivalent Confidentiality Label

Marking	Confidentiality Label
NATO UNCLASSIFIED Releasable to ISAF, KFOR, RESOLUTE SUPPORT	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName=”Releasable To” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>ISAF</GenericValue> <GenericValue>KFOR</GenericValue> <GenericValue>RESOLUTE SUPPORT</GenericValue> </Category> </ConfidentialityInformation>
NATO UNCLASSIFIED	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName=”Context” type=”PERMISSIVE”>

Marking	Confidentiality Label
	<GenericValue>NATO</GenericValue> </Category> </ConfidentialityInformation>
NATO UNCLASSIFIED – STAFF	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>UNCLASSIFIED</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> </Category> <Category tagName=”Administrative” type=”INFORMATIVE”> <GenericValue>STAFF</GenericValue> </Category> </ConfidentialityInformation>
NATO RESTRICTED Releasable to Japan, Switzerland, Ukraine	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>RESTRICTED</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName=”Releasable To” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>JPN</GenericValue> <GenericValue>CHE</GenericValue> <GenericValue>UKR</GenericValue> </Category> </ConfidentialityInformation>
NATO/EAPC CONFIDENTIAL Releasable to ISAF	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>EAPC</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName=”Releasable To” type=”PERMISSIVE”> <GenericValue>EAPC</GenericValue> <GenericValue>ISAF</GenericValue> </Category> </ConfidentialityInformation>
NATO/KFOR CONFIDENTIAL NATO, Ireland, Sweden, Ukraine Only	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>CONFIDENTIAL</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>KFOR</GenericValue> </Category> <Category tagName=”Only” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>IRL</GenericValue> <GenericValue>SWE</GenericValue> <GenericValue>UKR</GenericValue> </Category> </ConfidentialityInformation>

The following table shows a further example of markings, together with the equivalent confidentiality label, which shows the use of both the Only and Releasable To categories.

Table 18: Using Both Releasable To and Only Categories

Marking	Confidentiality Label
NATO RESTRICTED Canada, Germany, Spain, France, Italy, Netherlands, Norway, UK, USA Only Releasable to Sweden	<ConfidentialityInformation> <PolicyIdentifier>NATO</PolicyIdentifier> <Classification>RESTRICTED</Classification> <Category tagName=”Context” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>Releasable</GenericValue> </Category> <Category tagName=”Only” type=”PERMISSIVE”> <GenericValue>CAN</GenericValue> <GenericValue>DEU</GenericValue> <GenericValue>ESP</GenericValue> <GenericValue>FRA</GenericValue> <GenericValue>ITA</GenericValue> <GenericValue>NLD</GenericValue> <GenericValue>NOR</GenericValue> <GenericValue>GBR</GenericValue> <GenericValue>USA</GenericValue> </Category> <Category tagName=”Releasable To” type=”PERMISSIVE”> <GenericValue>NATO</GenericValue> <GenericValue>SWE</GenericValue> </Category> </ConfidentialityInformation>

ANNEX A: Example Clearances for Nations

Introduction

This Annex presents a number of example clearances that may be used when evaluating a confidentiality label in support of an access control decision.

The example clearances illustrate how the restrictive categories (Additional Sensitivity) and permissive categories (Only, Releasable To) are used to support the access control decision.

Clearances do not, in general, include informative categories (Administrative) as informative categories are not considered in the access control decision.

A clearance contains the same security marking elements as a confidentiality label, with the exception that a clearance contains multiple classification elements, where a confidentiality label contains a single element.

The example clearances consider:

1. A NATO member nation,
2. A partner nation and
3. A non-member, non-partner nation.

An XML schema for representing the example clearances used in this Annex is defined below. The clearance syntax is based upon the clearance attribute description from Clearance Attribute and Authority Clearance Constraints Certificate Extension RFC 5913 (Reference [9]) and imports the necessary security marking elements from the *ConfidentialityInformation* element required to represent a clearance.

Schema

A schema has been defined to represent a clearance.

The schema has the following namespace:
urn:nato:stanag:4774:confidentialityclearance:1:0.

The schema for the Confidentiality Clearance is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
**********************************************************************

                NATO UNCLASSIFIED

XML Schema for representing a Confidentiality Clearance.

        I
       / \
      -< + >-
       \ /
        I             NCI AGENCY
  ##   #    ####    #      P.O. box 174
  ##   #   #    #   #      2501 CD The Hague
```

```
  # # #  #      #
  # ##  #   #  #     Core Enterprise Services
  #  ##   ####   #
    A G E N C Y

*********************************************************************
-->


<xs:schema
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
 xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
 targetNamespace="urn:nato:stanag:4774:confidentialityclearance:1:0"
 version="1.2" elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:annotation>
  <xs:appinfo>
   <UniqueIdentifier/>
   <Name>Confidentiality Clearance Schema</Name>
   <Definition>Schema for a confidentiality clearance</Definition>
   <VersionIndicator>1.0</VersionIndicator>
   <UsageGuidance>
    Used within NATO for representing a confidentiality clearance.
   </UsageGuidance>
   <RestrictionType/>
   <RestrictionValue/>
   <ConfidentialityLabel ReviewDateTime="2020-03-24T00:00:00Z">
    <ConfidentialityInformation>
     <PolicyIdentifier>NATO</PolicyIdentifier>
     <Classification>UNCLASSIFIED</Classification>
     <Category Type="PERMISSIVE" TagName="Context">
      <GenericValue>NATO</GenericValue>
     </Category>
    </ConfidentialityInformation>
    <CreationDateTime>2015-03-24T00:00:00Z</CreationDateTime>
   </ConfidentialityLabel>
  </xs:appinfo>
  <xs:documentation>
   The schema can be used to convey X.501 clearance attribute Access Control Information (ACI) in XML.
  </xs:documentation>
 </xs:annotation>

 <!-- Import STANAG 4774 Confidentiality Metadata Label Schema -->
 <xs:import namespace="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0"
   schemaLocation="nl-cl.xsd"/>

 <xs:element name="ConfidentialityClearance" id="confidentialityClearance">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier> urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearance
    </UniqueIdentifier>
    <Name>Confidentiality Clearance</Name>
    <Definition>
     Confidentiality Clearance importing types from ConfidentialityLabel
    </Definition>
    <VersionIndicator>1.2</VersionIndicator>
    <UsageGuidance>Used to represent the ACI of any entity.</UsageGuidance>
    <RestrictionType/>
    <RestrictionValue/>
   </xs:appinfo>
```

```
  </xs:annotation>
  <xs:complexType>
   <xs:complexContent>
    <xs:extension base="sclr:ConfidentialityClearanceType">
     <xs:anyAttribute processContents="lax"/>
    </xs:extension>
   </xs:complexContent>
  </xs:complexType>
 </xs:element>
 <xs:complexType name="ConfidentialityClearanceType" id="confidentialityClearanceType">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier> urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearanceType
    </UniqueIdentifier>
    <Name>Confidentiality Clearance Type</Name>
    <Definition>
     A type that is used as the base for the confidentiality clearance elements.
    </Definition>
    <VersionIndicator>1.0</VersionIndicator>
    <UsageGuidance/>
    <RestrictionType/>
    <RestrictionValue/>
   </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
   <xs:element ref="slab:PolicyIdentifier"/>
   <xs:element ref="sclr:ClassificationList"/>
   <xs:element ref="slab:Category" minOccurs="0" maxOccurs="unbounded"/>
   <xs:element ref="sclr:ConfidentialityClearanceExtensions" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <xs:element name="ClassificationList" type="sclr:ClassificationListType"/>
 <xs:complexType name="ClassificationListType" id="classificationListType">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier>
urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:classificationListType
    </UniqueIdentifier>
    <Name>ClassificationList Type</Name>
    <Definition>A type that enumerates the classifications.</Definition>
    <VersionIndicator>1.0</VersionIndicator>
    <UsageGuidance/>
    <RestrictionType/>
    <RestrictionValue/>
   </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
   <xs:element ref="slab:Classification" maxOccurs="unbounded"/>
   <xs:element ref="sclr:ConfidentialityClearanceExtensions" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <xs:element name="ConfidentialityClearanceExtensions" type="sclr:ConfidentialityClearanceExtensionsType"/>
 <xs:complexType name="ConfidentialityClearanceExtensionsType"
id="confidentialityClearanceExtensionsType">
  <xs:annotation>
   <xs:appinfo>
    <UniqueIdentifier>
urn:nato:stanag:4774:confidentialityclearance:1:0:appinfo:confidentialityClearanceExtensionsType
    </UniqueIdentifier>
    <Name>ConfidentialityClearanceExtensions Type</Name>
```

```
    <Definition>A type that allows for extensibility.</Definition>
    <VersionIndicator>1.0</VersionIndicator>
    <UsageGuidance/>
    <RestrictionType/>
    <RestrictionValue/>
   </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
   <xs:any processContents="lax" namespace="##other" minOccurs="0" \
     maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
</xs:schema>
```

NATO Member Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are a current member of NATO.

Context Category

A nation which is a member of NATO will have a “Context” category value in their clearance for NATO and all NAC-approved activities of which they are a member.

Releasable To Category

A nation will have a “Releasable To” category value in their clearance for NATO and all NAC-approved activities of which they are a member, as well as their own national value.

Only Category

A nation will have an “Only” category value in their clearance for NATO as well as their own national value.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” categories values in their clearance.

Example

An example clearance for the United Kingdom, a founding member of NATO:

```
<sclr:ConfidentialityClearance
  xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
  xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <sclr:ClassificationList>
    <Classification>UNCLASSIFIED</Classification>
    <Classification>RESTRICTED</Classification>
    <Classification>CONFIDENTIAL</Classification>
    <Classification>SECRET</Classification>
    <Classification>TOP SECRET</Classification>
  </sclr:ClassificationList>
  <Category TagName="Context" Type="PERMISSIVE">
    <GenericValue>NATO</GenericValue>
```

```
    <GenericValue>EAPC</GenericValue>
    <GenericValue>GEORGIA</GenericValue>
    <GenericValue>ISAF</GenericValue>
    <GenericValue>KFOR</GenericValue>
    <GenericValue>PFP</GenericValue>
    <GenericValue>RUSSIA</GenericValue>
    <GenericValue>UKRAINE</GenericValue>
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category TagName="Releasable To" Type="PERMISSIVE">
    <GenericValue>NATO</GenericValue>
    <GenericValue>EAPC</GenericValue>
    <GenericValue>ISAF</GenericValue>
    <GenericValue>KFOR</GenericValue>
    <GenericValue>PFP</GenericValue>
    <GenericValue>GBR</GenericValue>
  </Category>
  <Category TagName="Only" Type="PERMISSIVE">
    <GenericValue>NATO</GenericValue>
    <GenericValue>GBR</GenericValue>
  </Category>
  <Category TagName="Additional Sensitivity" Type="RESTRICTIVE">
    <GenericValue>ATOMAL</GenericValue>
    <GenericValue>BOHEMIA</GenericValue>
    <GenericValue>CRYPTO</GenericValue>
  </Category>
</sclr:ConfidentialityClearance>
```

Partner Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are not a member of NATO, but are a NATO partner nation.

Context Category

A nation should have the “Context” category value in their clearance for each NAC approved activity in which they are a partner nation.

A nation should also have the “Context” category value of “Releasable” in their clearance, to support confidentiality labels generated outside of the NAC approved activities of which of the nation is a partner nation.

Releasable To Category

A nation should also have a “Releasable To” category value in their clearance for each NAC approved activity in which they were a partner nation.

A nation should have a “Releasable To” category value in their clearance for their nation, to support confidentiality labels generated outside of the NAC approved activities of which of the nation is a partner nation.

Only Category

A nation should have an “Only” category value in their clearance for their nation.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” category values in their clearance.

Example

An example clearance for the New Zealand, which is a partner nation in the ISAF NAC approved activity:

```
<sclr:ConfidentialityClearance
  xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
  xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <sclr:ClassificationList>
    <Classification>UNCLASSIFIED</Classification>
    <Classification>RESTRICTED</Classification>
    <Classification>CONFIDENTIAL</Classification>
    <Classification>SECRET</Classification>
  </sclr:ClassificationList>
  <Category TagName="Context" Type="PERMISSIVE">
    <GenericValue>ISAF</GenericValue>
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category TagName="Releasable To" Type="PERMISSIVE">
    <GenericValue>NZL</GenericValue>
    <GenericValue>ISAF</GenericValue>
  </Category>
  <Category TagName="Only" Type="PERMISSIVE">
    <GenericValue>NZL</GenericValue>
  </Category>
</sclr:ConfidentialityClearance>
```

Non-NATO, Non-Partner Nation

Introduction

The following sections discuss the category values a nation will have in their clearance if they are neither a member of NATO nor a NATO partner nation.

Context Category

A nation should have the “Context” category value of “Releasable” in their clearance.

Releasable To Category

A nation should have a “Releasable To” category value in their clearance for their nation.

Only Category

A nation should have no “Only” category values in their clearance, as they are not part of any NAC approved activities.

Additional Sensitivity Category

A nation will have the appropriate “Additional Sensitivity” category values in their clearance.

Example

An example clearance for the Samoa:

```
<sclr:ConfidentialityClearance
  xmlns:sclr="urn:nato:stanag:4774:confidentialityclearance:1:0"
  xmlns="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
  <PolicyIdentifier>NATO</PolicyIdentifier>
  <sclr:ClassificationList>
    <Classification>UNCLASSIFIED</Classification>
    <Classification>RESTRICTED</Classification>
    <Classification>CONFIDENTIAL</Classification>
    <Classification>SECRET</Classification>
  </sclr:ClassificationList>
  <Category TagName="Context" Type="PERMISSIVE">
    <GenericValue>Releasable</GenericValue>
  </Category>
  <Category TagName="Releasable To" Type="PERMISSIVE">
    <GenericValue>WSM</GenericValue>
  </Category>
</sclr:ConfidentialityClearance>
```

INTENTIONALLY BLANK

ANNEX B: Security Policy Information File

Introduction

A Security Policy Information File (SPIF) describes all of the allowable values within a security policy and the relationships between them.

The SPIF can also include information that defines how the allowable values should be rendered as a security marking.

The SPIF can include information for rendering in different languages.

An XML schema for representing a SPIF is defined at www.xmlspif.org.

Validation

The confidentiality label syntax defined in Appendix 2 allows a confidentiality label to be represented in a wide range of security policies including both NATO security policies and National security policies.

The confidentiality label syntax supports the Principle of Consistent Labelling by defining a schema for the confidentiality label, but does not, of itself, support the consistent application of a security policy.

In order to support the consistent generation of confidentiality labels with registered values, additional information is required about the specific policies that are being used.

Validation Approaches

There are number of validation languages and tools that can be implemented to make assertions about the presence or absence of patterns within XML documents. One such example of this is Schematron which is a rules based validation language which can be defined for specific security policy to ensure that all of the values present with a confidentiality label lie within the correct Value Domain.

Example

The following example SPIF uses the XMLSPIF schema to encapsulate the elements of the NATO Security Policy. The complete, up to date SPIF for the NATO Security Policy is held in the NMRR.

NATO SPIF

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  $Id: NATO Security Policy.xml 79 2015-11-06 15:54:38Z g.lunt $ -->
<spif:SPIF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:spif="http://www.xmlspif.org/spif"
   schemaVersion="2.1" version="79" creationDate="201511061430200Z"
   originatorDN="CN=Graeme Lunt,O=SMHS Ltd,C=GB"
   keyIdentifier="6AA4BA9F66BFCD44" privilegeId="2.16.840.1.101.2.1.8.3"
   rbacId="2.16.840.1.101.2.1.8.3">
  <spif:securityPolicyId name="NATO" id="1.3.26.1.3.1"/>
```

```
<spif:securityClassifications>
  <spif:securityClassification name="UNCLASSIFIED" lacv="1" hierarchy="1">
    <spif:markingData xml:lang="fr" phrase="SANS CLASSIFICATION">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="RESTRICTED" lacv="2" hierarchy="2">
    <spif:markingData xml:lang="fr" phrase="DIFFUSION RESTREINTE">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="CONFIDENTIAL" lacv="3" hierarchy="3">
    <spif:markingData xml:lang="fr" phrase="CONFIDENTIEL">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="SECRET" lacv="4" hierarchy="4">
    <spif:markingData xml:lang="fr" phrase="SECRET">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
  <spif:securityClassification name="TOP SECRET" lacv="5" hierarchy="5">
    <spif:markingData phrase="COSMIC">
      <spif:code>replacePolicy</spif:code>
    </spif:markingData>
    <spif:markingData xml:lang="fr" phrase="TRES SECRET">
      <spif:code>documentStart</spif:code>
    </spif:markingData>
  </spif:securityClassification>
</spif:securityClassifications>
<spif:securityCategoryTagSets>
  <spif:securityCategoryTagSet name="Additional Sensitivity" id="1.3.26.1.4.1">
    <spif:securityCategoryTag name="Additional Sensitivity" tagType="restrictive"
      singleSelection="false">
      <spif:tagCategory name="ATOMAL" lacv="1">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
        <spif:excludedClass>RESTRICTED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="CRYPTO"  lacv="2">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
        <spif:excludedClass>RESTRICTED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="SIOP" lacv="3"/>
      <spif:tagCategory name="SIOP ESI" lacv="4" obsolete="true"/>
      <spif:tagCategory name="EXCLUSIVE" lacv="5"  obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="INTELLIGENCE" lacv="6" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="LOGISTICS" lacv="7" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="OPERATIONS" lacv="8" obsolete="true">
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="BOHEMIA" lacv="9" >
        <spif:excludedClass>UNCLASSIFIED</spif:excludedClass>
      </spif:tagCategory>
```

```
    <spif:markingQualifier markingCode="pageTop">
      <spif:qualifier markingQualifier=" " qualifierCode="separator"/>
    </spif:markingQualifier>
  </spif:securityCategoryTag>
</spif:securityCategoryTagSet>
<spif:securityCategoryTagSet name="Releasable To" id="1.3.26.1.4.2">
  <spif:securityCategoryTag name="Releasable To" tagType="enumerated"
    enumType="permissive" singleSelection="false">
    <spif:tagCategory name="ALB" lacv="008">
      <spif:markingData phrase="Albania">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Albanie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="DZA" lacv="012">
      <spif:markingData phrase="Algeria">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Algérie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="ARM" lacv="051">
      <spif:markingData phrase="Armenia">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Arménie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AUS" lacv="036">
      <spif:markingData phrase="Australia">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Australie">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AUT" lacv="040">
      <spif:markingData phrase="Austria">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Autriche">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="AZE" lacv="031">
      <spif:markingData phrase="Azerbaijan">
        <spif:code>documentStart</spif:code>
      </spif:markingData>
      <spif:markingData xml:lang="fr" phrase="Azerbaïdjan">
        <spif:code>documentStart</spif:code>
```

```
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BAH" lacv="048">
  <spif:markingData phrase="Bahrain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bahreïn">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BLR" lacv="112">
  <spif:markingData phrase="Belarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bélarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BEL" lacv="056">
  <spif:markingData phrase="Belgium">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Belgique">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="BIH" lacv="070">
  <spif:markingData phrase="Bosnia and Herzegovina">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bosnie-Herzégovine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BGR" lacv="100">
  <spif:markingData phrase="Bulgaria">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bulgarie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CAN" lacv="124">
  <spif:markingData phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>

<spif:tagCategory name="HRV" lacv="191">
```

```
  <spif:markingData phrase="Croatia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Croatie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="CZE" lacv="203">
  <spif:markingData phrase="Czech Republic">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tchèque, République">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DNK" lacv="208">
  <spif:markingData phrase="Denmark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Danemark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EGY" lacv="818">
  <spif:markingData phrase="Egypt">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Égypte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="EST" lacv="233">
  <spif:markingData phrase="Estonia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Estonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FIN" lacv="246">
  <spif:markingData phrase="Finland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Finlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FRA" lacv="250">
  <spif:markingData phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="France">
```

```
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GEO" lacv="268">
   <spif:markingData phrase="Georgia">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Géorgie">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DEU" lacv="276">
   <spif:markingData phrase="Germany">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Allemagne">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GRC" lacv="300">
   <spif:markingData phrase="Greece">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Grèce">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="HUN" lacv="348">
   <spif:markingData phrase="Hungary">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Hongrie">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISL" lacv="352">
   <spif:markingData phrase="Iceland">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Islande">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="IRL" lacv="372">
   <spif:markingData phrase="Ireland">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Irlande">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:tagCategory name="ISR" lacv="376">
  <spif:markingData phrase="Israel">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Israël">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ITA" lacv="380">
  <spif:markingData phrase="Italy">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Italie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JPN" lacv="392">
  <spif:markingData phrase="Japan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Japon">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JOR" lacv="400">
  <spif:markingData phrase="Jordan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Jordanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KAZ" lacv="398">
  <spif:markingData phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KOR" lacv="410">
  <spif:markingData phrase="Korea, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Corée, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KWT" lacv="414">
  <spif:markingData phrase="Kuwait">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Koweït">
```

```
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KGZ" lacv="417">
  <spif:markingData phrase="Kyrgyzstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kirghizistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LVA" lacv="428">
  <spif:markingData phrase="Latvia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lettonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LTU" lacv="440">
  <spif:markingData phrase="Lithuania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lituanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LUX" lacv="442">
  <spif:markingData phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>


<spif:tagCategory name="MLT" lacv="470">
  <spif:markingData phrase="Malta">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Malte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MRT" lacv="478">
  <spif:markingData phrase="Mauritania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mauritanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
```

```
</spif:tagCategory>
<spif:tagCategory name="MDA" lacv="498">
  <spif:markingData phrase="Moldova, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Moldova, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNG" lacv="496">
  <spif:markingData phrase="Mongolia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mongolie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNE" lacv="499">
  <spif:markingData phrase="Montenegro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Monténégro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MAR" lacv="504">
  <spif:markingData phrase="Morocco">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Maroc">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NLD" lacv="528">
  <spif:markingData phrase="Netherlands">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pays-Bas">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NZL" lacv="554">
  <spif:markingData phrase="New Zealand">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Nouvelle-Zélande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NOR" lacv="578">
  <spif:markingData phrase="Norway">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:markingData xml:lang="fr" phrase="Norvège">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>

<spif:tagCategory name="POL" lacv="616">
  <spif:markingData phrase="Poland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pologne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PRT" lacv="620">
  <spif:markingData phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="QAT" lacv="634">
  <spif:markingData phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ROU" lacv="642">
  <spif:markingData phrase="Romania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Roumanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RUS" lacv="643">
  <spif:markingData phrase="Russian Federation">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Russie, Fédération de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SRB" lacv="688">
  <spif:markingData phrase="Serbia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Serbie">
```

```
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SVK" lacv="703">
  <spif:markingData phrase="Slovakia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovaquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="SVN" lacv="705">
  <spif:markingData phrase="Slovenia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovénie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ESP" lacv="724">
  <spif:markingData phrase="Spain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Espagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="SWE" lacv="752">
  <spif:markingData phrase="Sweden">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suède">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CHE" lacv="756">
  <spif:markingData phrase="Switzerland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suisse">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TJK" lacv="762">
  <spif:markingData phrase="Tajikistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tadjikistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FYR" lacv="807">
```

```
  <spif:markingData phrase=" the former Yugoslav Republic of Macedonia">
          <!--Turkey recognises the Republic of Macedonia with its constitutional name-->
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="l'ex-République yougoslave de Macédoine">
         <!-- La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.-->
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TUN" lacv="788">
  <spif:markingData phrase="Tunisia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tunisie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TUR" lacv="792">
  <spif:markingData phrase="Turkey">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TKM" lacv="795">
  <spif:markingData phrase="Turkmenistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Turkménistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UKR" lacv="804">
  <spif:markingData phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ukraine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ARE" lacv="784">
  <spif:markingData phrase="United Arab Emirates">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Émirats Arabes Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GBR" lacv="826">
  <spif:markingData phrase="United Kingdom">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:markingData xml:lang="fr" phrase="Royaume-Uni">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="USA" lacv="840">
  <spif:markingData phrase="United States of America">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="États-Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UZB" lacv="860">
  <spif:markingData phrase="Uzbekistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ouzbékistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NATO" lacv="1001">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="EAPC" lacv="1101">
  <spif:markingData phrase="EAPC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISAF" lacv="1201">
  <spif:markingData phrase="ISAF">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IP" lacv="1301">
  <spif:markingData phrase="IP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ICI" lacv="1401">
  <spif:markingData phrase="ICI">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
```

```
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KFOR" lacv="1501">
  <spif:markingData phrase="KFOR">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MD" lacv="1601">
  <spif:markingData phrase="MD">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PATG" lacv="1701">
  <spif:markingData phrase="PATG">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PFP" lacv="1801">
  <spif:markingData phrase="PFP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RESOLUTE SUPPORT" lacv="1901">
  <spif:markingData phrase="RESOLUTE SUPPORT">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PARP" lacv="2001">
  <spif:markingData phrase="PARP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NGC" lacv="2101">
  <spif:markingData phrase="NGC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NUC" lacv="2201">
  <spif:markingData phrase="NUC">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
      <spif:tagCategory name="NRC" lacv="2301">
        <spif:markingData phrase="NRC">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:excludedClass>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:markingQualifier markingCode="pageTop">
        <spif:qualifier markingQualifier="Releasable To "
          qualifierCode="prefix"/>
        <spif:qualifier xml:lang="fr" markingQualifier="Communicable a "
          qualifierCode="prefix"/>
        <spif:qualifier markingQualifier="/" qualifierCode="separator"/>
      </spif:markingQualifier>
    </spif:securityCategoryTag>
  </spif:securityCategoryTagSet>
  <spif:securityCategoryTagSet name="Only" id="1.3.26.1.4.5">
    <spif:securityCategoryTag name="Only" tagType="enumerated"
      enumType="permissive" singleSelection="false">
>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="ALB" lacv="008">
        <spif:markingData phrase="Albania">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:markingData xml:lang="fr" phrase="Albanie">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:excludedClass>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="DZA" lacv="012">
        <spif:markingData phrase="Algeria">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:markingData xml:lang="fr" phrase="Algérie">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:excludedClass>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="ARM" lacv="051">
        <spif:markingData phrase="Armenia">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:markingData xml:lang="fr" phrase="Arménie">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:excludedClass>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="AUS" lacv="036">
        <spif:markingData phrase="Australia">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:markingData xml:lang="fr" phrase="Australie">
          <spif:code>documentStart</spif:code>
        </spif:markingData>
        <spif:excludedClass>TOP SECRET</spif:excludedClass>
      </spif:tagCategory>
      <spif:tagCategory name="AUT" lacv="040">
        <spif:markingData phrase="Austria">
          <spif:code>documentStart</spif:code>
```

```
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Autriche">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="AZE" lacv="031">
  <spif:markingData phrase="Azerbaijan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Azerbaïdjan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BAH" lacv="048">
  <spif:markingData phrase="Bahrain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bahreïn">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BLR" lacv="112">
  <spif:markingData phrase="Belarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bélarus">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BEL" lacv="056">
  <spif:markingData phrase="Belgium">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Belgique">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="BIH" lacv="070">
  <spif:markingData phrase="Bosnia and Herzegovina">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bosnie-Herzégovine">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="BGR" lacv="100">
  <spif:markingData phrase="Bulgaria">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Bulgarie">
    <spif:code>documentStart</spif:code>
```

```
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CAN" lacv="124">
  <spif:markingData phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Canada">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="HRV" lacv="191">
  <spif:markingData phrase="Croatia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Croatie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="CZE" lacv="203">
  <spif:markingData phrase="Czech Republic">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Tchèque, République">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DNK" lacv="208">
  <spif:markingData phrase="Denmark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Danemark">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EGY" lacv="818">
  <spif:markingData phrase="Egypt">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Égypte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="EST" lacv="233">
  <spif:markingData phrase="Estonia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Estonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FIN" lacv="246">
  <spif:markingData phrase="Finland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:markingData xml:lang="fr" phrase="Finlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="FRA" lacv="250">
  <spif:markingData phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="France">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GEO" lacv="268">
  <spif:markingData phrase="Georgia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Géorgie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="DEU" lacv="276">
  <spif:markingData phrase="Germany">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Allemagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GRC" lacv="300">
  <spif:markingData phrase="Greece">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Grèce">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="HUN" lacv="348">
  <spif:markingData phrase="Hungary">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Hongrie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISL" lacv="352">
  <spif:markingData phrase="Iceland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Islande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
```

```
<spif:tagCategory name="IRL" lacv="372">
  <spif:markingData phrase="Ireland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Irlande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISR" lacv="376">
  <spif:markingData phrase="Israel">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Israël">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ITA" lacv="380">
  <spif:markingData phrase="Italy">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Italie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JPN" lacv="392">
  <spif:markingData phrase="Japan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Japon">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="JOR" lacv="400">
  <spif:markingData phrase="Jordan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Jordanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KAZ" lacv="398">
  <spif:markingData phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kazakhstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KOR" lacv="410">
  <spif:markingData phrase="Korea, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:markingData xml:lang="fr" phrase="Corée, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KWT" lacv="414">
  <spif:markingData phrase="Kuwait">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Koweït">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KGZ" lacv="417">
  <spif:markingData phrase="Kyrgyzstan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Kirghizistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LVA" lacv="428">
  <spif:markingData phrase="Latvia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lettonie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LTU" lacv="440">
  <spif:markingData phrase="Lithuania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Lituanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="LUX" lacv="442">
  <spif:markingData phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Luxembourg">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="MLT" lacv="470">
  <spif:markingData phrase="Malta">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Malte">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
```

```
</spif:tagCategory>
<spif:tagCategory name="MRT" lacv="478">
  <spif:markingData phrase="Mauritania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mauritanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MDA" lacv="498">
  <spif:markingData phrase="Moldova, Republic of">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Moldova, République de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNG" lacv="496">
  <spif:markingData phrase="Mongolia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Mongolie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MNE" lacv="499">
  <spif:markingData phrase="Montenegro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Monténégro">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MAR" lacv="504">
  <spif:markingData phrase="Morocco">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Maroc">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NLD" lacv="528">
  <spif:markingData phrase="Netherlands">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pays-Bas">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NZL" lacv="554">
  <spif:markingData phrase="New Zealand">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:markingData xml:lang="fr" phrase="Nouvelle-Zélande">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NOR" lacv="578">
  <spif:markingData phrase="Norway">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Norvège">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="POL" lacv="616">
  <spif:markingData phrase="Poland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Pologne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PRT" lacv="620">
  <spif:markingData phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Portugal">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="QAT" lacv="634">
  <spif:markingData phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Qatar">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ROU" lacv="642">
  <spif:markingData phrase="Romania">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Roumanie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RUS" lacv="643">
  <spif:markingData phrase="Russian Federation">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Russie, Fédération de">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
```

```
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SRB" lacv="688">
  <spif:markingData phrase="Serbia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Serbie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>

<spif:tagCategory name="SVK" lacv="703">
  <spif:markingData phrase="Slovakia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovaquie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="SVN" lacv="705">
  <spif:markingData phrase="Slovenia">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Slovénie">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ESP" lacv="724">
  <spif:markingData phrase="Spain">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Espagne">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="SWE" lacv="752">
  <spif:markingData phrase="Sweden">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suède">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="CHE" lacv="756">
  <spif:markingData phrase="Switzerland">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Suisse">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="TJK" lacv="762">
  <spif:markingData phrase="Tajikistan">
```

```
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Tadjikistan">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="FYR" lacv="807">
   <spif:markingData phrase=" the former Yugoslav Republic of Macedonia">
          <!--Turkey recognises the Republic of Macedonia with its constitutional name-->
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr"
    phrase=" l'ex-République yougoslave de Macédoine">
          <!-- La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.-->
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>

  <spif:tagCategory name="TUN" lacv="788">
   <spif:markingData phrase="Tunisia">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Tunisie">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="TUR" lacv="792">
   <spif:markingData phrase="Turkey">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Turquie">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="TKM" lacv="795">
   <spif:markingData phrase="Turkmenistan">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Turkménistan">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="UKR" lacv="804">
   <spif:markingData phrase="Ukraine">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:markingData xml:lang="fr" phrase="Ukraine">
    <spif:code>documentStart</spif:code>
   </spif:markingData>
   <spif:excludedClass>TOP SECRET</spif:excludedClass>
  </spif:tagCategory>
  <spif:tagCategory name="ARE" lacv="784">
   <spif:markingData phrase="United Arab Emirates">
    <spif:code>documentStart</spif:code>
```

```
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Émirats Arabes Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="GBR" lacv="826">
  <spif:markingData phrase="United Kingdom">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Royaume-Uni">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="USA" lacv="840">
  <spif:markingData phrase="United States of America">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="États-Unis">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="UZB" lacv="860">
  <spif:markingData phrase="Uzbekistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:markingData xml:lang="fr" phrase="Ouzbékistan">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NATO" lacv="1001">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
</spif:tagCategory>
<spif:tagCategory name="EAPC" lacv="1101">
  <spif:markingData phrase="NATO">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ISAF" lacv="1201">
  <spif:markingData phrase="ISAF">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="IP" lacv="1301">
  <spif:markingData phrase="IP">
    <spif:code>documentStart</spif:code>
```

```
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="ICI" lacv="1401">
  <spif:markingData phrase="ICI">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="KFOR" lacv="1501">
  <spif:markingData phrase="KFOR">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="MD" lacv="1601">
  <spif:markingData phrase="MD">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PATG" lacv="1701">
  <spif:markingData phrase="PATG">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PFP" lacv="1801">
  <spif:markingData phrase="PFP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="RESOLUTE SUPPORT" lacv="1901">
  <spif:markingData phrase="RESOLUTE SUPPORT">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="PARP" lacv="2001">
  <spif:markingData phrase="PARP">
    <spif:code>documentStart</spif:code>
  </spif:markingData>
  <spif:excludedClass>RESTRICTED</spif:excludedClass>
  <spif:excludedClass>CONFIDENTIAL</spif:excludedClass>
  <spif:excludedClass>SECRET</spif:excludedClass>
  <spif:excludedClass>TOP SECRET</spif:excludedClass>
</spif:tagCategory>
<spif:tagCategory name="NGC" lacv="2101">
  <spif:markingData phrase="NGC">
```

```
      <spif:code>documentStart</spif:code>
     </spif:markingData>
     <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="NUC" lacv="2201">
     <spif:markingData phrase="NUC">
      <spif:code>documentStart</spif:code>
     </spif:markingData>
     <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="NRC" lacv="2301">
     <spif:markingData phrase="NRC">
      <spif:code>documentStart</spif:code>
     </spif:markingData>
     <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:markingQualifier markingCode="pageTop">
     <spif:qualifier markingQualifier=" ONLY" qualifierCode="suffix"/>
     <spif:qualifier xml:lang="fr" markingQualifier=" SEULEMENT"
      qualifierCode="suffix"/>
     <spif:qualifier markingQualifier="," qualifierCode="separator"/>
    </spif:markingQualifier>
   </spif:securityCategoryTag>
  </spif:securityCategoryTagSet>
  <spif:securityCategoryTagSet name="Administrative" id="1.3.26.1.4.3">
   <spif:securityCategoryTag name="Administrative" tagType="tagType7"
    tag7Encoding="bitSetAttributes" singleSelection="false">
    <spif:tagCategory name="MANAGEMENT" lacv="1"/>
    <spif:tagCategory name="STAFF" lacv="2"/>
    <spif:tagCategory name="PERSONAL" lacv="3"/>
    <spif:tagCategory name="MEDICAL" lacv="4"/>
    <spif:tagCategory name="COMMERCIAL" lacv="5"/>
    <spif:markingQualifier markingCode="pageTop">
     <spif:qualifier markingQualifier=" " qualifierCode="separator"/>
    </spif:markingQualifier>
   </spif:securityCategoryTag>
  </spif:securityCategoryTagSet>
  <spif:securityCategoryTagSet name="Context" id="1.3.26.1.4.4">
   <spif:securityCategoryTag name="Context" tagType="permissive" >
    <spif:tagCategory name="NATO" lacv="1001">
     <spif:markingData phrase="NATO">
      <spif:code>noNameDisplay</spif:code>
      <spif:code>replacePolicy</spif:code>
     </spif:markingData>
    </spif:tagCategory>
    <spif:tagCategory name="EAPC" lacv="1002">
     <spif:markingData phrase="NATO/EAPC">
      <spif:code>noNameDisplay</spif:code>
      <spif:code>replacePolicy</spif:code>
     </spif:markingData>
     <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="GEORGIA" lacv="1003">
     <!-- NATO + Georgia -->
     <spif:markingData phrase="NATO/GEORGIA">
      <spif:code>noNameDisplay</spif:code>
      <spif:code>replacePolicy</spif:code>
     </spif:markingData>
     <spif:excludedClass>TOP SECRET</spif:excludedClass>
```

```
    </spif:tagCategory>
    <spif:tagCategory name="ISAF" lacv="1004">
      <spif:markingData phrase="NATO/ISAF">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="KFOR" lacv="1005">
      <spif:markingData phrase="NATO/KFOR">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="PFP" lacv="1006">
      <spif:markingData phrase="NATO/PFP">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="RUSSIA" lacv="1007">
      <spif:markingData phrase="NATO/RUSSIA">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="UKRAINE" lacv="1008">
      <spif:markingData phrase="NATO/UKRAINE">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="IP" lacv="1009">
      <spif:markingData phrase="NATO/IP">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="RESOLUTE SUPPORT" lacv="1010">
      <spif:markingData phrase="NATO/RESOLUTE SUPPORT">
        <spif:code>noNameDisplay</spif:code>
        <spif:code>replacePolicy</spif:code>
      </spif:markingData>
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
    <spif:tagCategory name="Releasable" lacv="10000">
      <spif:markingData>
        <spif:code>noNameDisplay</spif:code>
      </spif:markingData>
      <!-- Required when Releasable To category is used -->
      <spif:excludedClass>TOP SECRET</spif:excludedClass>
    </spif:tagCategory>
  </spif:securityCategoryTag>
</spif:securityCategoryTagSet>
```

```
  </spif:securityCategoryTagSets>
</spif:SPIF>
```

INTENTIONALLY BLANK

ANNEX C: PUBLIC Security Policy Confidentiality Labels

Introduction

The confidentiality label schema defined in Annex A of Appendix 1 specifies the syntax for confidentiality labels and provides the semantics for the values a confidentiality label may contain. In other words, the confidentiality label schema is a generic framework for storing any confidentiality label values that supports multiple different security policies.

However, the confidentiality label schema itself does not define the semantics of the values a confidentiality label can contain for a given specific security policy.

Ingest

NATO may ingest information from the public domain that does not contain a confidentiality label.

In order to support the information lifecycle within NATO, an originator confidentiality label SHOULD be bound with the information on ingest to order to record the original confidentiality label associated with the information[5].

In order to support the binding of an originator confidentiality label or information ingested from the public domain, a distinct security policy must be defined[6] which can be used with the confidentiality label syntax.

Release

In addition, NATO may release NATO information into the public domain and consequently relinquish ownership of that information.

During the lifecycle of that NATO information, it may be required to indicate that the information will be released into the public domain at a certain date (e.g. using the SuccessionHandling element to embargo a press release), or propose an alternative confidentiality label to be used as and when the NATO information enters the public domain.

In order for confidentiality labels to be used effectively and consistently within an enterprise environment, there must be a well-defined mapping of the security policy onto the appropriate confidentiality label elements in order to ensure that the appropriate semantics (according to the security policy) are observed and applied.

---

[5] In addition, on ingest, an alternative confidentiality label in the NATO security policy (see Appendix 2) should also be bound to the information to specify how the information should be handled within the NATO domain.

[6] Note, it is not acceptable to use the NATO security policy (for example NATO UNCLASSIFIED) in the originator confidentiality label as this infers NATO ownership of the information. The NATO security policy can however be used in the alternative confidentiality label.

This annex describes the *ConfidentialityInformation* and its child elements in order to support effective and consistent application of the PUBLIC security policy within the NATO environment in accordance with:

- Technical and Implementation Directive for Confidentiality Labelling of NATO Information (Reference 2)

Note that all confidentiality labels with the PUBLIC security policy have a corresponding blank/empty security marking.

ConfidentialityInformation

The following table specifies the Value Domain for each of the *ConfidentialityInformation* elements and the defined *Category* elements, in support of the PUBLIC security policy.

All values within the ConfidentialityInformation element are treated as case insensitive during processing.

For example, “Unmarked” and “UNMARKED” are equivalent.

All values used in the ConfidentialityInformation element use the English terms.

Each of the Value Domains for the ConfidentialityInformation elements are described in further detail below.

PolicyIdentifier

The *PolicyIdentifier* element indicates the security policy authority and the semantics of the values of the other *ConfidentialityInformation* elements.

A single policy is used across NATO and all NAC-approved activities for unlabelled information from the public domain, and has the value “PUBLIC”.

The corresponding attributes for Policy element are:

Table 19: Attributes for Policy Element

Attribute	Value
URI	“urn:oid:1.3.6.1.4.1.31778.12.2.1”

For example,

<PolicyIdentifier>**PUBLIC**</PolicyIdentifier>

Classification

The Classification element indicates the sensitivity of the content of the data object to which the confidentiality label is bound.

The Value Domain for Classification element within the PUBLIC security policy are:

Table 20: Value Domain for Classification Element

Value	Definition
“UNMARKED”	

For example,

<Classification>**UNMARKED**</Classification>

PrivacyMark

The privacy mark is not used within the PUBLIC security policy.

Categories

Introduction

The PUBLIC security policy defines a single security category:

Table 21: Security Categories for the PUBLIC Security Policy

Value	Definition
“In Confidence”	Informative guidance on how the information should be handled.

The “In Confidence” category is described in the following section.

In Confidence

The corresponding attributes for the “In Confidence” category element are:

Table 22: Attributes for the Context Category Element

Attribute	Value
tagName	“In Confidence”
type	“INFORMATIVE”
URI	“urn:oid:1.3.6.1.4.1.31778.13.2.1”

The Value Domain of the “In Confidence” Category within the PUBLIC security policy is defined in Reference 1.

For example,

```
<ConfidentialityInformation>
   <PolicyIdentifier>PUBLIC</PolicyIdentifier>
   <Classification>UNMARKED</Classification>
   <Category tagName=”In Confidence” type=”PERMISSIVE”>
      <GenericValue>LEGAL</GenericValue>
</ConfidentialityInformation>
```

Examples

The following table shows some example confidentiality labels in the PUBLIC security policy.

Table 23: Example - Confidentiality Labels

Confidentiality Label
<ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> </ConfidentialityInformation>
<ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> <Category tagName="In Confidence" type="INFORMATIVE"> <GenericValue>MEDICAL</GenericValue> </Category> </ConfidentialityInformation>
<ConfidentialityInformation> <PolicyIdentifier>PUBLIC</PolicyIdentifier> <Classification>UNMARKED</Classification> <Category tagName="In Confidence" type="INFORMATIVE"> <GenericValue>COMMERCIAL</GenericValue> <GenericValue>LEGAL</GenericValue> </ConfidentialityInformation>

ANNEX D: PUBLIC Security Policy Information File

Introduction

A Security Policy Information File (SPIF) describes all of the allowable values within a security policy and the relationships between them.

The SPIF can also include information that defines how the allowable values should be rendered as a security marking.

The SPIF can include information for rendering in different languages.

An XML schema for representing a SPIF is defined at www.xmlspif.org.

The following SPIF uses this XMLSPIF schema to encapsulate the PUBLIC security policy described in Appendix 2 Annex C.

Public SPIF

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  $Id: PUBLIC Security Policy.xml 58 2014-09-16 09:14:24Z g.lunt $ -->
<spif:SPIF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xmlns:spif="http://www.xmlspif.org/spif"
          xsi:schemaLocation="http://www.xmlspif.org/spif ../Schemas/spif.xsd"
          schemaVersion="1.0" version="1" creationDate="20140916090512Z"
          originatorDN="CN=Graeme Lunt,O=SMHS Ltd,C=GB"
          keyIdentifier="6AA4BA9F66BFCD44" privilegeId="2.16.840.1.101.2.1.8.3"
          rbacId="2.16.840.1.101.2.1.8.3">
  <spif:securityPolicyId name="PUBLIC" id="1.3.6.1.4.1.31778.12.2.1"/>
  <spif:securityClassifications>
    <spif:securityClassification name="UNMARKED" lacv="0" hierarchy="0">
      <spif:markingData>
        <spif:code>noMarkingDisplay</spif:code>
      </spif:markingData>
    </spif:securityClassification>
  </spif:securityClassifications>
  <spif:securityCategoryTagSets>
    <spif:securityCategoryTagSet name="In Confidence"
      id="1.3.6.1.4.1.31778.13.2.1">
      <spif:securityCategoryTag name="In Confidence" tagType="tagType7"
        tag7Encoding="bitSetAttributes" singleSelection="false">
        <spif:tagCategory name="COMMERCIAL" lacv="1">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
        <spif:tagCategory name="INTELLECTUAL PROPERTY" lacv="2">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
        <spif:tagCategory name="JUSTICE" lacv="3">
          <spif:markingData>
            <spif:code>noMarkingDisplay</spif:code>
          </spif:markingData>
        </spif:tagCategory>
```

```
      <spif:tagCategory name="LEGAL" lacv="4">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
      <spif:tagCategory name="MANAGEMENT" lacv="5">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
      <spif:tagCategory name="MEDICAL" lacv="6">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
      <spif:tagCategory name="PERSONAL" lacv="7">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
      <spif:tagCategory name="SECURITY" lacv="8">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
      <spif:tagCategory name="STAFF" lacv="9">
        <spif:markingData>
          <spif:code>noMarkingDisplay</spif:code>
        </spif:markingData>
      </spif:tagCategory>
    </spif:securityCategoryTag>
  </spif:securityCategoryTagSet>
 </spif:securityCategoryTagSets>
</spif:SPIF>
```

INTENTIONALLY BLANK

ADatP-4774(A)(1)