

STANDARDS RELATED DOCUMENT

ADatP-4774.2

GUIDANCE ON THE DIGITAL LABELLING OF NATO INFORMATION

Edition A, Version 1

JUNE 2021



NORTH ATLANTIC TREATY ORGANIZATION

**Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN**

INTENTIONALLY BLANK

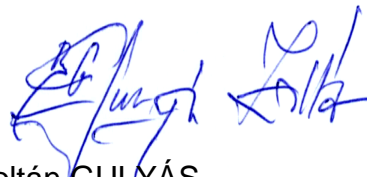
NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

1 June 2021

1. The enclosed Standards Related Document, ADatP-4774.2, Edition A, Version 1, GUIDANCE ON THE DIGITAL LABELLING OF NATO INFORMATION, which has been approved in conjunction with ADatP-4774.2 by the nations in the Consultation, Command and Control Board (C3B), is promulgated herewith.
2. ADatP-4774.2, Edition A, Version 1 is effective upon receipt/will come into effect on [NED].
3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.
4. This publication shall be handled in accordance with C-M(2002)60.



Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1	INTRODUCTION.....	1-1
CHAPTER 2	THE USE OF CONFIDENTIALITY METADATA LABELS FOR NATO INFORMATION	2-1
CHAPTER 3	ELEMENTS OF THE CONFIDENTIALITY METADATA LABEL	3-1
3.1.	The Governing Security Policy	3-1
3.2.	Classification	3-2
3.3.	Categories.....	3-2
3.4.	Context.....	3-4
3.5.	Releasable to	3-4
3.6.	Only	3-6
3.7.	Limited	3-7
3.8.	Special Category Designators	3-7
3.9.	Administrative.....	3-8
3.10.	Privacy Mark	3-9
CHAPTER 4	THE USE OF ALTERNATIVE CONFIDENTIALITY LABELS	4-1
CHAPTER 5	ENTITY VALUE DOMAINS	5-1
CHAPTER 6	EXAMPLES OF NATO CONFIDENTIALITY METADATA LABELS	6-1
CHAPTER 7	SECURITY POLICY INFORMATION FILE (SPIF).....	7-1
CHAPTER 8	REFERENCE MATERIALS	8-1
8.1	Terms and Definitions	8-1
8.2	References.....	8-3
8.3	Abbreviations	8-4
ANNEX A	NATO LABELLING STANAGs and RELATED DOCUMENTS.....	A-1

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1. The Primary Directive on CIS Security mandates the use of metadata to allow interagency access control, automated exchanges and appropriate protection of shared information among NATO Entities, Non-NATO Entities (NNEs), Communities of Interest (COIs), and non-governmental organizations (NGOs) when necessary. (Ref. A)
2. The Primary Directive on Information Management (PDIM) (Ref. B) mandates the use of metadata as a key enabler for effective and efficient information sharing across the Alliance. To support this mandate, a data object¹ must be labelled with metadata via the use of dedicated profiles, methods and standards.
3. Confidentiality Metadata Labelling (hereafter 'labelling') refers to a process that determines the appropriate Confidentiality Metadata Label (hereafter 'label') for a given data object, creating the metadata label and binding the metadata label to the data object. The labelling approach is facilitated through the following NATO standards:
4. **(Draft) ADatP-5636 NATO Core Metadata Specification (NCMS)** defines a core set of metadata elements in three layers (Security, Common, and Information Life Cycle) to support cross-domain information exchange. (Ref. C) The Security layer includes the confidentiality metadata elements.
5. **ADatP-4778 Metadata Binding Mechanism** defines how metadata is bound to a data object. (Ref. D)
6. **ADatP-4774 Confidentiality Metadata Label Syntax** defines confidentiality metadata elements and labelling syntax. (Ref. E)
7. This Standard-Related Document (SRD) defines the NATO value domains for the Metadata Labels as defined at the Security layer of ADatP-5636, and associates them with predefined business rules for labelling purpose.
8. The metadata labels, value domains and business rules listed in this SRD are captured as a Security Policy Information File (SPIF). The SPIF is a dynamic file, which is expected to be updated as the Alliance changes the business rules or value domains for the release or restriction of information.
9. An Extensible Markup Language (XML) representation of the SPIF is published in the NATO Metadata Registry & Repository (NMRR)², and supports the centralized configuration management of Communication and Information Systems (CIS).
10. The NATO Security Policy³ (Ref. F) is the authoritative Governing Security Policy for metadata labelling application in NATO.
11. The value domains and business rules listed in this SRD are primarily defined by the 'NATO Security Policy and 'The Management of Non-Classified NATO information' (Ref. G) to cover classified and non-classified information respectively.

¹ In this SRD, "information" and "data object" refers to object of finite size, such as a picture, a document, a message, a letter, a presentation, a map, a video, a database report, etc.

² <https://nmrr.ncia.nato.int/home.htm>

³ Security within the North Atlantic Treaty Organisation (Ref. F)

12. Ad-hoc requests influencing the metadata labels and value domains, e.g. new participation in NATO-led exercises, operations, etc., shall integrate with the SPIF once any requisite decisions are approved by the relevant authorities.
13. The value domains listed in this SRD shall also apply to the information received from non-NATO sources through Alternative Confidentiality Labelling – a component of Metadata labelling which is primarily designed to integrate the non-NATO information process in NATO CIS environments. (See Chapter 4)
14. The Communities of Interest (COIs) shall use the same value domains when and where they governed by the NATO Security Policy. (Ref. F)

CHAPTER 2 THE USE OF CONFIDENTIALITY METADATA LABELS FOR NATO INFORMATION

1. A Metadata Label includes a number of distinct metadata elements, each having a list of allowable value domains that control the selection when a label is applied to an information resource.
2. Each of these value domains and metadata labels have a specific purpose and an appropriate usage.
3. The correspondence between Marking and Labelling elements is presented in Table 2-1.

Marking Elements	Labelling Elements		Category
Ownership	The Governing Security Policy	Policy Identifier	
		Context	
Classification	Classification		
N/A	Privacy Mark ⁴		
Releasability Dissemination Limitation Markings	Releasable to		
	Only		
	Limited		
Administrative/Category Designators	Special Category Designators		
	Administrative		

Table 2-1 Correspondence between Marking and Labelling elements

4. Labelling and Marking are related concepts that need to be aligned. To ensure consistency, Label elements shall be rendered from the Marking automatically. In case of an inconsistency observed between Marking and Labelling, e.g. as a result of a declassification or downgrade process, the Label elements shall be recognised as the authoritative source.

⁴ The 'Privacy Mark' is in use for military messaging and carries only one value that is "CLEAR". The Privacy Mark does appear in Markings as "RECEIVED IN CLEAR, TREAT AS CONFIDENTIAL". See Chapter 3 for more details.

INTENTIONALLY BLANK

CHAPTER 3 ELEMENTS OF THE CONFIDENTIALITY METADATA LABEL

3.1. The Governing Security Policy

1. The Governing Security Policy refers to the security policy and specifications that are in effect and adhered to by the Originator in the Information Domain.
2. The Governing Security Policy is comprised of two elements: the “Policy Identifier” and the “Context”. The Policy Identifier refers to the Information Owner in association with the selected Context, and Context refers the domain where the information is born, e.g. EAPC.
3. In accordance with ADatP-4774, Policy Identifier is mandatory element and a single value “NATO” shall be present.

Policy Identifier	Definition
NATO	Information generated or received (including information received without a specific ownership value) in the context of NATO activities and subject to NATO Security Policy (Ref. F) and other information management policies. (Ref. B) (Ref. G)

Table 3-1: ‘NATO’ Policy Identifier value

4. The “Context” value domains listed in Table 3-2. Although this is not an exhaustive list, in the future more value domains may be added or removed as the Alliance changes the business rules or value domains for the release or restriction of information.

Context	Definition
NATO ⁵	Information generated within the Alliance context only without any other framework in this table.
EAPC	The overarching Framework for Political and Security Consultations (Euro-Atlantic Partnership Council) and for Enhanced Cooperation under the Partnership for Peace Programme (Ref. I)
GEORGIA	Information generated in the context of NATO-Georgia Commission (Ref. J)
KFOR	Information generated in the context of KFOR operations (Ref. K)
PFP	Information generated in the context of the Partnership for Peace Programme (Ref. L)
RESOLUTE SUPPORT	Resolute Support is a NATO-led mission provides training, advice and assistance for the Afghan security forces and institutions. (Ref. M)
RUSSIA	NATO information generated in the context of NATO-Russia Council (Ref. N)
UKRAINE	NATO information generated in the context of NATO-Ukraine Commission (Ref. O)

Table 3-2: Context values for the ‘NATO’ Policy Identifier

⁵ To prevent duplication (as NATO/NATO), the “NATO” value domain from “Context” will be omitted when it is rendered as marking.

3.2. Classification

5. The Directive on the Security of Information (Ref. P) defines this category as “the sensitivity of NATO information and is applied to alert recipients of the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure or loss”.

6. In accordance with ADatP-4774, Classification is a mandatory element.

7. All classified information created under the NATO Governing Security Policy shall bear one of the following value domains presented at Table 3-3.

Values	Definition
RESTRICTED	NATO Information whose unauthorized disclosure would be detrimental to the interests or effectiveness of NATO
CONFIDENTIAL	NATO Information whose unauthorized disclosure would be damaging to NATO
SECRET	NATO Information whose unauthorized disclosure would result in grave damage to NATO. The impact of improper disclosure of SECRET level documents is “High”
TOP SECRET ⁶	Unauthorized disclosure of this information would result in exceptionally grave damage to NATO

Table 3-3: Value Domains for NATO Security Classifications

8. The Policy on the Management of Non-Classified NATO Information (Ref. G) complements NATO Security Policy, which establishes the basic principles and standards to be applied for the protection and handling of non-classified NATO information. Within NATO, a single value domain exists and it is presented at Table 3-4.

Value	Definition
UNCLASSIFIED	NATO UNCLASSIFIED information shall only be used for official purposes and only individuals, bodies or organisations that require it for official NATO purposes may have access to it.

Table 3-4: Value Domain for NATO UNCLASSIFIED

9. Information intended to be shared with the public from its creation such as outreach activity, press release, e.g. shall be labelled as ‘Public’, and these kind of documents shall carry no markings of any sort.

3.3. Categories

10. Categories aim to restrict and/or expand dissemination within the scope of the classification of the information. Category types are interpreted from the perspective of the recipient of the information and his/her access privileges. Access privileges may be based, but not solely, on the clearance attributes of the recipient. Categories are designated as one of three types:

⁶ In cases of use of the “TOP SECRET” security classification, the ownership (Policy Identifier and Context) value shall be rendered as “COSMIC” (Ref. F)

11. **Restrictive Category Type** reduces the scope of information dissemination where a narrower distribution is required for Need-to-know assurance such as 'Special Category Designator' elements. In cases where the additional restrictive category values are attached to information, they further restrict the dissemination, as a recipient must have an authorization for all of the selected category values. For example, if a recipient has no authorisation to receive "ATOMAL" information, that recipient shall not have access to information that includes the "ATOMAL" category value. In cases where information belongs to multiple restrictive category types, a recipient shall have all of these authorisations.

12. **Permissive Category Type** provides explicit inclusion sets for the purpose of access control such as 'Releasable to' and 'Only'. In cases where the additional permissive category values ('Releasable to') are attached to information, they permit wider dissemination beyond than the selected context, or permit information dissemination to subset of selected context as a recipient requires authorization for one of the category values. Following example describes 'Only' category;

NATO/PFP RESTRICTED
NATO, FINLAND, AUSTRIA Only

13. If a recipient has an authorization for "NATO" in the "Only" permissive category, they are authorized to receive information that includes just the "Only" value "NATO". They can also receive information that has a label with the "Only" values "NATO", "FINLAND" and "AUSTRIA". In this case, the addition of the "FINLAND" and "AUSTRIA" value have permitted the further dissemination of the information (to those recipients with an authorization for either nation).⁷

14. **Informative Category Type** provides handling instructions for information in accordance with the content of the document. 'Administrative' can be an example of Informative Category. Informative Category has no impact on the automated access control decision functions (ACDF).

15. Table 3-5, provides the elements for each category used for a metadata label under the NATO Security Policy. Other national security policies may use a different set of Categories.

Categories	Definition
Context	A string representing the NATO membership or NAC-approved co-operative activity membership as shown in Table 3-2. (Column: Context)
Releasable to	A representation of a non-NATO nation(s) and/or entity as illustrated in Table 3-6.
Only	A representation of nation(s) that are a member of the Context as selected from Table 3-7.
Limited	Limited specifies a handling instruction provided by the originator.
Special Category Designators	A string representing a restriction of distribution as selected from Table 3-8.
Administrative	A string provided as an informative indication of an administrative nature as selected from Table 3-9.

Table 3-5: Category Elements of a NATO Metadata Label

⁷ This example is valid as Finland and Austria are members of PFP.

16. In accordance with NATO Security Policy, multiple Category elements and their value domains may be present within a Metadata Label.

3.4. Context

17. The “Context” category is a permissive category and indicates that the dissemination of NATO information may be extended to more non-NATO nations or partners depending on the context in which the NATO information was created.

18. The “Context” category (Table 3-2) shall be used in conjunction with the Policy Identifier (Table 3-1), to indicate the ownership of the information.

19. A single value shall be present from Table 3-1 for “NATO” Policy Identifier.

3.5. Releasable to

20. The “Releasable to” category is a permissive category that supports the release of NATO information beyond the originating Information Domain. “Releasable to” category permits the release information to entities, if that entity is different from the selected context category that can be non-NATO nations and/or International Organizations, or NATO Groupings who meet the security standards by the accreditation authority.

21. Ownership together with originator determines the dissemination criteria when the information is ready for collaboration and/or publication. The “Releasable to” value(s) depends on the selected Ownership, sensitivity of information and established security agreements.

22. In accordance with ADatP-4774, “Releasable to” is an optional category.

23. Table 3-6 presents current and agreed value domains for the “Releasable to” category although this is not an exhaustive list, in the future more value domains may be added or removed as the Alliance changes the business rules or value domains for the release or restriction of information.

24. The “Releasable to” category value domains shall be applied by the originator during information creation.

25. Multiple values from Table 3-6 may be present in case of use this category.

Explanation	Values	Full Name
a) Individual entity(s) that is different from the information originator. ⁸	GEO	Georgia
	JAP	Japan
	(See Table 5-1 for a complete list of the anticipated nations)	
b) Organizations that have security agreements or arrangements with NATO (Ref. R, Ref. S)	EU Commission	European Commission
	EEAS	European External Action Service
	EUROCONTROL	The European Organisation for the Safety of Air Navigation
	Council of the EU	European Council
	OCCAR	Organisation for Joint Armament Cooperation
c) NATO Groupings ⁹	EAPC	Euro Atlantic Partnership Council
	CFE Signatories	Treaty on Conventional Armed Forces in Europe
	Global Coalition	Global Coalition
	ICI	Istanbul Cooperation Initiative
	IP	Interoperability Platform
	KFOR	Kosovo Force
	MD	Mediterranean Dialogue
	PFP	Partnership for Peace
	RESOLUTE SUPPORT	Resolute Support
	NMI	NATO Mission Iraq
	NATO Response Force	NATO Response Force

Table 3-6 Value Domains for “Releasable to” Category

26. The value domain for the "Releasable to" category includes only values that are not included in the specified Context, for instance if the Context value assigned is RESOLUTE SUPPORT then the "Releasable to" value cannot be a nation that is already a RESOLUTE SUPPORT member.

27. The following example illustrates proper Marking and Labelling for the “Releasable to” category.

⁸ To support Metadata Labelling, nation names are abbreviated into trigraph characters (e.g. JAP) and these values shall render in full name when displayed as a marking (e.g. JAPAN). See Table 5-1.

⁹ These groups are valid for the “Releasable to” category if they are different from the selected “Context” value.

NATO/RESOLUTE SUPPORT CONFIDENTIAL
Releasable to Jordan

Governing Security Policy (Policy Identifier): **NATO**
 Classification: **CONFIDENTIAL**
 Category Name: Context
 Category Type (Context): PERMISSIVE
 Category Value (Context): **RESOLUTE SUPPORT**
 Category Name: **Releasable to**
 Category Type (Releasable to): PERMISSIVE
 Category Value (Releasable to): **JOR**

28. In this example, information with this marking may release to current NATO members and RESOLUTE SUPPORT partners and to Jordan.

3.6. Only

29. The “Only” category is a permissive category used to limit dissemination of information to a subset of the entities identified by the “Context” and the “Releasable to” categories.¹⁰

Explanation	“Only” Values	Full Name
a) Individual nation(s) included in the selected “Context” membership applied to the information resource.	“BEL”	Belgium
	“CAN”	Canada
	“FRA”	France
	(See Chapter 5, Table 5-1 for a complete list)	
b) Partnership or activity that is included in the selected “Context” and/or “Releasable to” membership applied to the information resource.	- Any of the valid “Context” values from Table 3-2 (column: Context Value)	
	- Any of the valid “Releasable to” values from Table 3-6.	

Table 3-7 Value Domains for “Only” Category

30. In accordance with ADatP-4774, “Only” is an optional category.

31. Table 3-7 presents current and agreed value domains for the “Only” category although this is not an exhaustive list, in the future more value domains may be added or removed as the Alliance changes the business rules or value domains for the release or restriction of information.

32. The “Only” category value domains shall be applied by the originator during information creation.

33. Multiple values from Table 3-7 may be present in case of use this category.

¹⁰ The “Only” category limits dissemination and is a PERMISSIVE category type since the recipient must have one of the nation(s) in the list in their clearance attributes to permit receipt. Therefore, NATO staff (e.g. information managers and archivists) may access this information irrespective of their nationality.

34. The following example illustrates proper Marking and Labelling for the “Only” category.

<p>NATO RESTRICTED Canada, Germany, Spain, Netherlands, United States Only Releasable to Sweden</p>

<p>Governing Security Policy (Policy Identifier): NATO Classification: RESTRICTED Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO Category Name: Only Category Type (Only): PERMISSIVE Category Value (Only): CAN Category Value (Only): DEU Category Value (Only): ESP Category Value (Only): NLD Category Value (Only): USA Category Name: Releasable to Category Type: (Releasable to): PERMISSIVE Category Value (Releasable to): SWE</p>

3.7. Limited

35. “Limited” identifies handling instructions to indicate a specific onward dissemination and/or access limitation.

36. “Limited” values are free form instructions that are assigned by the information originator and as such, there is no fixed value domain within the NATO Security Policy. Therefore, as a best practice, “Limited” value domains shall be different from value domains defined in this SRD.

37. In accordance with ADatP-4774, “Limited” is an optional category.

3.8. Special Category Designators

38. The “Special Category Designators” category is a restrictive category that indicates the sensitivity of NATO information, which is not conveyed by the Ownership or Classification elements.

39. In accordance with ADatP-4774, “Special Category Designators” is an optional category.

40. The Special Category Designators value domains shall be applied by originator during information creation.

41. Table 3-8 presents current and agreed value domains for “Special Category Designators”.

Value	Definition
ATOMAL	Information regarding nuclear issues to the agreement on the exchange of atomic information.
BOHEMIA	Information derived from or originated by Communications Intelligence (COMINT) and information regarding signals intelligence (SIGINT), related operations, sources and methods.
CRYPTO	Identifies information that is derived from or originated by COMSEC and is focused on protection of NATO cryptographic information.
SIOP	The term "SIOP" is a marking applied to special category information signifying that information shall be protected in accordance with Ref. F.

Table 3-8 "Special Category Designators" Category Elements

42. The information in this category is subject to additional stringent access and release control constraints. Each Special Category Designator element governs with a different (minimum) classification level to be applied in NATO. The classification boundaries are listed below:¹¹

43. "ATOMAL" shall bear at a minimum the "CONFIDENTIAL",

44. "BOHEMIA" shall bear at a minimum the "TOP SECRET",

45. "CRYPTO" shall bear at a minimum the "CONFIDENTIAL",

46. "SIOP" shall bear at a minimum the "CONFIDENTIAL".

47. Multiple values from Table 3-8 may be present, in case of use this category.

48. The following example illustrates proper Marking and Labelling for the "Special Category Designators" category.

NATO SECRET – ATOMAL

Governing Security Policy (Policy Identifier): **NATO**
 Classification: **SECRET**
 Category Name: Context
 Category Type (Context): PERMISSIVE
 Category Value (Context): NATO
 Category Name: Special Category Designators
 Category Type (Special Category Designators): RESTRICTIVE
 Category Value: **ATOMAL**

3.9. Administrative

49. The "Administrative" category is an informative category that provides handling instructions for the disposition of information.

50. The "Administrative" category value domains shall be applied by the originator during information creation.

¹¹ C-M(68)41,C-M(71)27-REV1, MC 101 and NATO Security Policy - Enclosure E (Ref. F)

51. The “Administrative” category shall not be applied together with “Releasable to” and “Only” categories.

Value	Definition
COMMERCIAL	Information containing commercial proprietary information, e.g. that received in procurement actions.
MANAGEMENT	Information concerning advice on policy and planning affecting the interests of NATO.
MEDICAL	Information concerning medical reports and related material on personnel and units.
PERSONAL	Information to be seen only by the individual to whom it is addressed.
STAFF	Information containing references to named or identifiable staff.

Table 3-9 “Administrative” Category Elements

52. In accordance with ADatP-4774, “Administrative” is an optional category.

53. Single values from Table 3-9 shall be present in case of use this category.

54. The following example illustrates proper Marking and Labelling for the “Administrative” category.

NATO CONFIDENTIAL – MANAGEMENT

Governing Security Policy (Policy Identifier): **NATO**
 Classification: **CONFIDENTIAL**
 Category Name: Context
 Category Type (Context): PERMISSIVE
 Category Value (Context): NATO
 Category Name: Administrative
 Category Type (Administrative): INFORMATIVE
 Category Value: **MANAGEMENT**

3.10. Privacy Mark

55. The Privacy Mark element conveys specific COI information such as operational instructions, warnings or notifications of significance to the owner, user or custodian of the information.¹²

56. The following example illustrates proper Marking and Labelling for the “Privacy Mark”¹³.

NATO CONFIDENTIAL- RECEIVED IN THE CLEAR, TREAT AS CONFIDENTIAL

¹² Also, see Ref. F, Enclosure F, paragraphs 11.6 - 11.7.

¹³ ACP 121, paragraphs 361- 363.

Governing Security Policy (Policy Identifier): **NATO**
Classification: **CONFIDENTIAL**
Category Name: Context
Category Type (Context): PERMISSIVE
Category Value (Context): NATO
Privacy Mark: CLEAR

57. STANAG 4406 Military Message Handling System (Ref. Q) provides broader instructions on Privacy Mark use cases and restrictions.

CHAPTER 4 THE USE OF ALTERNATIVE CONFIDENTIALITY LABELS

1. The Alternative Confidentiality Label is designed for information received to NATO CIS from a non-NATO source such as from a nation¹⁴, an international organisation (IO), or from a public source.
2. The Originator Confidentiality Label holds the originator label attributes which are mapped to an Alternative Confidentiality Label for NATO (policy) equivalency. For instance, if a confidential information is retrieved from EU COUNCIL, the Originator Confidentiality Label of “EU COUNCIL CONFIDENTIAL” shall map to “NATO CONFIDENTIAL” to processed in NATO CIS. (Ref. R, Ref. S)

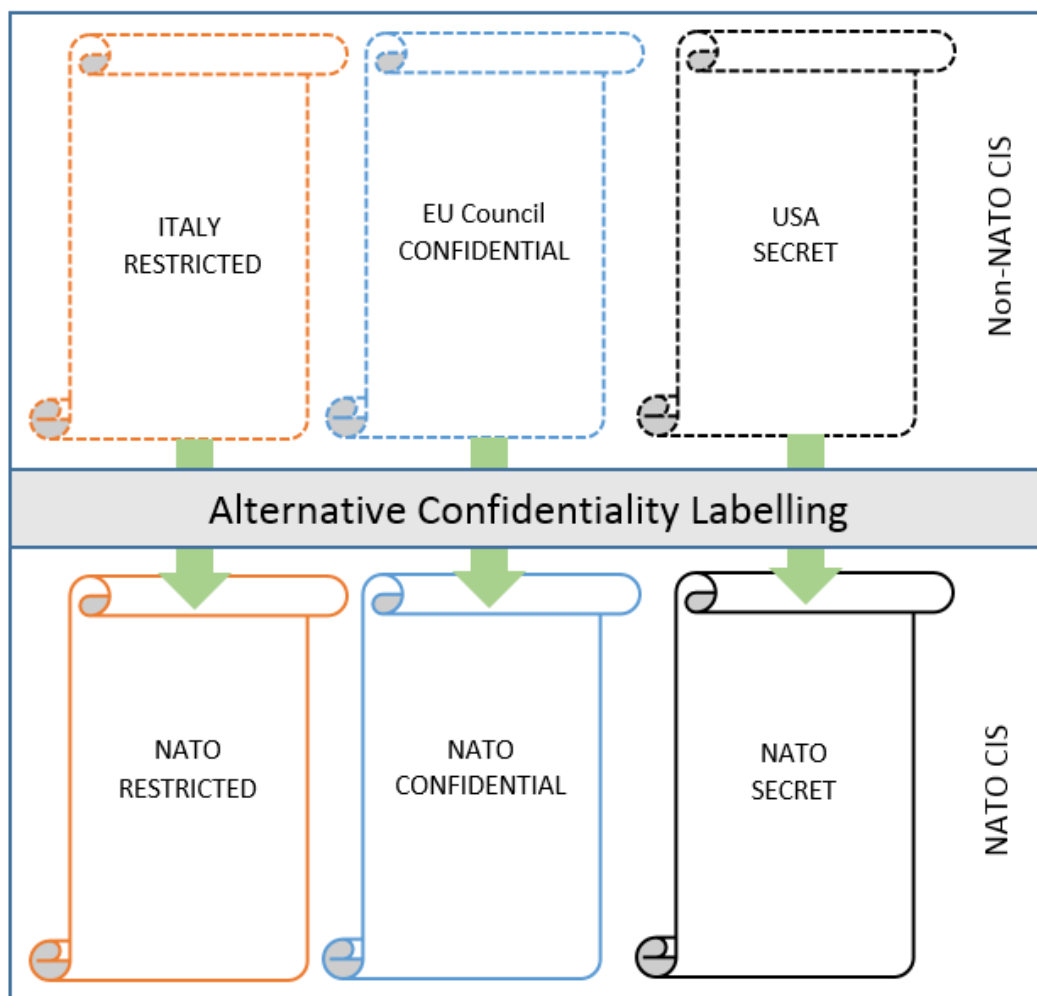


Figure 4-1 Business flow for “Alternative Confidentiality Label” Process

¹⁴ Alternative Confidentiality Labelling shall apply in instances where an information is ingested from a NATO nation using national labels.

3. The same procedure (paragraph 2) shall be applied in instances where non-NATO information ingested to NATO with unequal classification label¹⁵ respect to security agreement and arrangement listed at Ref. R. Result of this process the Originator Confidentially Label remained unchanged as the originator assigned.
4. Occasionally, information that published or broadcast for public consumption (e.g. a Wikipedia article, academic research, etc.) may be required to be transferred into the NATO CIS. In this case, a PUBLIC originator confidentiality label shall apply. Information originator (or custodian) may assigned a value domain from Table 3-3 or Table 3-4 where and when required.
5. As an outcome of Alternative Confidentiality Labelling process, NATO undertakes the Information Custodian role upon ingress of information and provides the agreed level of safe-keeping and availability of information as required by the originator.

¹⁵ Belgium, Canada, France and the United States do not use the security classification RESTRICTED in their national systems. Belgium, Canada, France and the United States handle and protect NATO RESTRICTED information in a manner no less stringent than the standards and procedures set forth in NATO Security Policy, its supporting directives, and the supporting document on the security protection of NATO RESTRICTED information.

CHAPTER 5 ENTITY VALUE DOMAINS

1. Information shall have a standard structure to enable consistent labelling across multiple domains. As such, the value domains are abbreviated into a standard form and presented at Table 5-1.
2. In NATO, metadata labelling values handled through an abbreviated form of the value domains (*Values* column), while the corresponding Marking shall render in full name as stated in the *Full Name* column.
3. Table 5-1 identifies the value domain for 'Context', 'Releasable to' and 'Only' categories (Table 2-1) and specifies Information Owner (members) as provided in Table 3-2. Although this is not an exhaustive list, in the future more value domains may be added or removed as the Alliance changes the business rules or value domains for the release or restriction of information.
4. The value domains listed at Table 5-1 are limited to individual nations, which are part of NATO groupings.
5. The value domains shall be merged with *NATO* (column) at Table 5-1 to constitute the Ownership as listed at Table 3-2.
6. The *Classification* (column) refers the highest information classification that a nation can access¹⁶.
7. In *Classification* column, the abbreviations U, S, and CTS refers to Unclassified, Secret and Cosmic Top Secret respectively.
8. Sharing of classified information with non-NATO groups shall be determined by NATO Security Policy (Ref. F) and individually signed security agreements/arrangements. (Ref. R) (Ref. S)
9. Sharing of Unclassified information with non-NATO groups shall be determined in accordance with The Management of Non-Classified NATO Information. (Ref. G)

Classification	Values	Full Name	NATO	EAPC	Georgia (NGC)	KFOR	PFP	Resolute Support	Russia (NRC)	UKRAINA (NUC)	Global Coalition	CFE Signatories	ICI	Interoperability Platform(IP)	MD	NMI	NATO Response Force
U	AFG	Afghanistan ¹⁷									✓						
CTS	ALB	Albania	✓														
S	ALG	Algeria													✓		
S	ARM	Armenia		✓		✓	✓	✓				✓		✓			

¹⁶ PDIM states, 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.

¹⁷ Allows sharing information up to NATO Secret, if that information is created in a Resolute Support Mission context.

Classification	Values	Full Name	NATO	EAPC	Georgia (NGC)	KFOR	PPF	Resolute Support	Russia (NRC)	UKRAINA (NUC)	Global Coalition	CFE Signatories	ICI	Interoperability Platform(IP)	MD	NMI	NATO Response Force
S	AUS	Australia						✓			✓			✓		✓	
S	AUT	Austria		✓		✓	✓	✓			✓			✓			
S	AZE	Azerbaijan		✓			✓	✓				✓		✓			
S	BAH	Bahrain									✓		✓	✓			
U	BLR	Belarus		✓			✓					✓					
CTS	BEL	Belgium	✓														
S	BIH	Bosnia and Herzegovina		✓			✓	✓			✓			✓			
CTS	BGR	Bulgaria	✓														
CTS	CAN	Canada	✓														
CTS	HRV	Croatia	✓														
CTS	CZE	Czech Republic	✓														
CTS	DNK	Denmark	✓														
S	EGY	Egypt									✓				✓		
CTS	EST	Estonia	✓														
S	FIN	Finland		✓		✓	✓	✓			✓			✓		✓	✓
CTS	FRA	France	✓														
S	GEO	Georgia		✓	✓		✓	✓			✓	✓		✓			✓
CTS	DEU	Germany	✓														
CTS	GRC	Greece	✓														
CTS	HUN	Hungary	✓														
CTS	ISL	Iceland	✓														
U	IRQ	Iraq									✓						
S	IRE	Ireland		✓		✓	✓							✓			
S	ISR	Israel													✓		
CTS	ITA	Italy	✓														
S	JAP	Japan												✓			
S	JOR	Jordan									✓			✓	✓		✓
S	KAZ	Kazakhstan		✓			✓					✓		✓			
U	SAU	Kingdom of Saudi Arabia									✓						
S	KUW	Kuwait									✓		✓				
S	KYR	Kyrgyz Republic of		✓			✓										
CTS	LVA	Latvia	✓														

Classification	Values	Full Name	NATO	EAPC	Georgia (NGC)	KFOR	PPF	Resolute Support	Russia (NRC)	UKRAINA (NUC)	Global Coalition	CFE Signatories	ICI	Interoperability Platform(IP)	MD	NMI	NATO Response Force
U	LBY	Libya ¹⁸									✓						
CTS	LTU	Lithuania	✓														
CTS	LUX	Luxembourg	✓														
S	MAL	Malta ¹⁸		✓			✓										
S	MAU	Mauritania													✓		
S	MOL	Moldova, Republic of ¹⁸		✓		✓	✓					✓		✓			
S	MNG	Mongolia						✓						✓			
CTS	MNE	Montenegro	✓														
S	MOR	Morocco									✓			✓	✓		
CTS	NLD	Netherlands	✓														
S	NZL	New Zealand						✓			✓			✓			
S	NOM	North Macedonia	✓														
CTS	NOR	Norway	✓														
CTS	POL	Poland	✓														
CTS	PRT	Portugal	✓														
S	QAT	Qatar ¹⁹									✓		✓				
CTS	ROU	Romania	✓														
S	ROK	Korea, Republic of												✓			
S	RUS	Russian Federation		✓			✓		✓								
S	SER	Serbia ¹⁸		✓			✓							✓			
CTS	SVK	Slovakia	✓														
CTS	SVN	Slovenia	✓														
CTS	ESP	Spain	✓														
CTS	SWE	Sweden		✓		✓	✓	✓			✓			✓		✓	✓
S	CHE	Switzerland		✓		✓	✓							✓			
S	TAJ	Tajikistan ¹⁸		✓			✓										
S	TUN	Tunisia									✓			✓	✓		
CTS	TUR	Turkey	✓														
S	TUM	Turkmenistan ¹⁸		✓			✓										
S	UKR	Ukraine		✓		✓	✓	✓		✓	✓	✓		✓			✓

¹⁸ Paper copy only.

¹⁹ Up to NATO Secret information if that information is created in Resolute Support Mission and Operation Unified Protector (OUP) contexts.

Classification	Values	Full Name	NATO	EAPC	Georgia (NGC)	KFOR	PPF	Resolute Support	Russia (NRC)	UKRAINA (NUC)	Global Coalition	CFE Signatories	ICI	Interoperability Platform(IP)	MD	NMI	NATO Response Force
S	UAE	United Arab Emirates									✓		✓	✓			
CTS	GBR	United Kingdom ²⁰	✓														
CTS	USA	United States of America	✓														
S	UZB	Uzbekistan ¹⁸		✓			✓										

Table 5-1: Entity Value Domains

10. The value domains listed at Table 5-2 may be used for 'Releasable to' category (Table 3-6) with an emphasis on the 'responsibility-to-share' balanced by the security principle of 'need-to-know'.

Classification	Values	Full Name
S	EU Commission	European Commission
S	EEAS	European External Action Service
S	EUROCONTROL	The European Organisation for the Safety of Air Navigation
S	Council of the EU	European Council
S	OCCAR	Organisation for Joint Armament Cooperation

Table 5-2: Organizations with Established Security Agreements

²⁰ The United Kingdom of Great Britain and Northern Ireland.

CHAPTER 6 EXAMPLES OF NATO CONFIDENTIALITY METADATA LABELS

The following examples illustrate NATO Markings and their equivalent representation in Labelling elements.

Marking Elements	Labelling Elements
NATO RESTRICTED	Governing Security Policy (Policy Identifier): NATO Classification: RESTRICTED Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO
NATO CONFIDENTIAL-STAFF	Governing Security Policy (Policy Identifier): NATO Classification: CONFIDENTIAL Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO Category Name: Administrative Category Type (Administrative): INFORMATIVE Category Value: STAFF
NATO RESTRICTED Releasable to Japan, Australia, PFP	Governing Security Policy (Policy Identifier): NATO Classification: RESTRICTED Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO Category Name: Releasable to Category Type (Releasable to): PERMISSIVE Category Value (Releasable to): JAP Category Value (Releasable to): AUS Category Value (Releasable to): PFP
NATO/KFOR CONFIDENTIAL NATO, Ireland, Ukraine Only	Governing Security Policy (Policy Identifier): NATO Classification: CONFIDENTIAL Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): KFOR Category Name: Only Category Type (Only): PERMISSIVE Category Value (Only): NATO Category Value (Only): IRL Category Value (Only): UKR

Marking Elements	Labelling Elements
<p style="text-align: center;">NATO SECRET Norway, United States Only Releasable to Sweden</p>	<p>Governing Security Policy (Policy Identifier): NATO Classification: SECRET Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO Category Name: Only Category Type: PERMISSIVE Category Value (Only): NOR Category Value (Only): USA Category Name: Releasable to Category Type: PERMISSIVE Category Value (Releasable to): SWE</p>
<p style="text-align: center;">NATO/EAPC CONFIDENTIAL Releasable to RESOLUTE SUPPORT</p>	<p>Governing Security Policy (Policy Identifier): NATO Classification: CONFIDENTIAL Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): EAPC Category Name: Releasable to Category Type (Releasable to): Permissive Category Value (Releasable to): RESOLUTE SUPPORT</p>
<p style="text-align: center;">NATO RESTRICTED Releasable to European Commission, EEAS, INTEROPERABILITY PLATFORM</p>	<p>Governing Security Policy (Policy Identifier): NATO Classification: RESTRICTED Category Name: Context Category Type (Context): PERMISSIVE Category Value (Context): NATO Category Name: Releasable to Category Type (Releasable to): PERMISSIVE Category Value (Releasable to): EU Commission Category Value (Releasable to): EEAS Category Value (Releasable to): IP</p>

CHAPTER 7 SECURITY POLICY INFORMATION FILE (SPIF)

1. Security Policy Information File (SPIF) is a dynamic policy file that provides electronic representation of agreed Markings and Labelling. The NATO SPIF stored in NMRR² enhances interoperability among NATO Bodies, national and non-governmental organization (NGO) systems by being accessible via a website.
2. The Information Processing Section, Archives & Information Management Division, is the authority to provide appropriate coordination among NATO Bodies, updating the SPIF and apply decisions when and where necessary.

SPIF	http://www.xmlspif.org/						
Policy Name	NATO						
Policy Id	1.3.26.1.3.1						
Version	83						
CreationDate	20181122100000						
Originator	cn=Graeme Lunt, o=SMHS Ltd, c=GB						
Reference	AC/322-N(2017)0125						
Source							
							
Classifications							
Name	LACV	Hierarchy	documentStart:en	documentStart:fr	portionMarking	Obsolete	Notes
UNCLASSIFIED	1	1	UNCLASSIFIED	SANS CLASSIFICATION	NU	FALSE	C-M(2002)
RESTRICTED	2	2	RESTRICTED	DIFFUSION RESTREINTE	NR	FALSE	C-M(2002)
CONFIDENTIAL	3	3	CONFIDENTIAL	CONFIDENTIEL	NC	FALSE	C-M(2002)
SECRET	4	4	SECRET	SECRET	NS	FALSE	C-M(2002)
TOP SECRET	5	5	TOP SECRET	TRES SECRET	CTS	FALSE	C-M(2002)
Categories							
Name	Id	TagType	Values	Values	Values	Values	Values
Special Category Designators	1.3.26.1.4.1	restrictive	SpecialCategoryDesignators				
Releasable To	1.3.26.1.4.2	permissive	NATONations	EAPCNations	PartnerNations	Groupings	Organizations
Administrative	1.3.26.1.4.3	tagType7	AdministrativeValues				
Context	1.3.26.1.4.4	permissive	ContextValues	ReleasableContext			
Only	1.3.26.1.4.5	permissive	NATONations	EAPCNations	PartnerNations	Groupings	Organizations
Limited	1.3.26.1.4.6	tagType7	LimitedValue				
SpecialCategoryDesignators							
Name	LACV	MinClass	MaxClass	documentStart:en	documentStart:fr	UserInput	Obsolete
ATOMAL	1	CONFIDENTIAL					FALSE
CRYPTO	2	RESTRICTED					FALSE
SIOP	3						FALSE
BOHEMIA	9	CONFIDENTIAL					FALSE
ContextValues							
				Context	Context		

Figure 7-1: Example (partial) view of NATO SPIF

INTENTIONALLY BLANK

CHAPTER 8 REFERENCE MATERIALS

8.1 Terms and Definitions

Binding: In the context of this SRD, it is the relationship between information and its metadata that provides an appropriate level of assurance of the integrity of the association between the information and its metadata. (Ref. D)

Business Rule: A business rule is a statement that defines or constrains some aspect of the business. It is intended to assert business structure or to control or influence the behaviour of the business.

Consistency of Labelling and Marking: The Metadata Label and its corresponding NATO marking must be coherent. In case of an inconsistency captured, the labelling attributes should take into account.

Community of Interest (COI): 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. (Ref. B)

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities or processes. (Ref. B)

Confidentiality Metadata Label (Metadata Label): A Metadata Label is a set of metadata elements and attributes that indicate the sensitivity of the information in an agreed structure and a controlled value domain. (Ref. E)

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. (Ref. B)

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. (Ref. F)

Information Custodian: The nation or organization that receives information, makes it visible, is responsible to the Information Owner for the agreed level of safe-keeping and availability of information. (Ref. B)

Information Domain: The domain where information born, transformed and shared. (Ref. B)

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

Information Owner: The nation or organisation that 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. (Ref. B)

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, optimize information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations. (Ref. B)

Labelling: The process of determining the appropriate metadata for given information, creating the Metadata Label and binding the Metadata Label to the information. (Ref. E)

Metadata: Structured information that describes, explains, locates and otherwise makes it easier to retrieve and use an information resource. The structure consists of 'elements', each of which contains 'values'. (Ref. C)

Marking: The term "marking" refers to the human-readable textual representation found on information resources that identifies the ownership of its content, its sensitivity, its Releasability and limitations on dissemination as well as administrative caveats. (Ref. F)

Need-to-know: The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services. (Ref. B)

NATO Information: NATO information embraces all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources. (Ref. F)

NATO Metadata Registry and Repository (NMRR): The NMRR refers to an interim database created for storing and cataloguing XML artefacts.

NNEs: NNEs include International Organizations, Governmental Organizations of non-NATO nations, Non-Governmental Organizations (NGO), Non-NATO Multinational forces, Host Nations (when the host nation is not a NATO nation), Contractors on operations, exercises and transformational activities, and Non-NATO countries that do not meet the "partners" criteria, which can be defined as "partners" refers to Partnership for Peace (PFP), Mediterranean Dialogue (MD), Istanbul Cooperation Initiative (ICI) countries, as well as those partners accredited as part of any partnership programme with NATO. (Ref. T)

Originator: The nation or international organisation under whose authority the information has been produced or introduced into NATO. (Ref. B)

Outreach activities: NATO information, which from its inception, is intended to be communicated to the public as part of NATO's public diplomacy and outreach activities, e.g. a press release. (Ref. H)

Security Classification: Security classifications indicate the sensitivity of NATO information and are applied to alert recipients of the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure. (Ref. F)

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

Standard-Related Document (SRD): A SRD is a NATO standardization document that facilitates understanding and implementation of one or more Allied standards. It may provide additional data and information to support the management and implementation of Allied standards. (Ref. U)

8.2 References

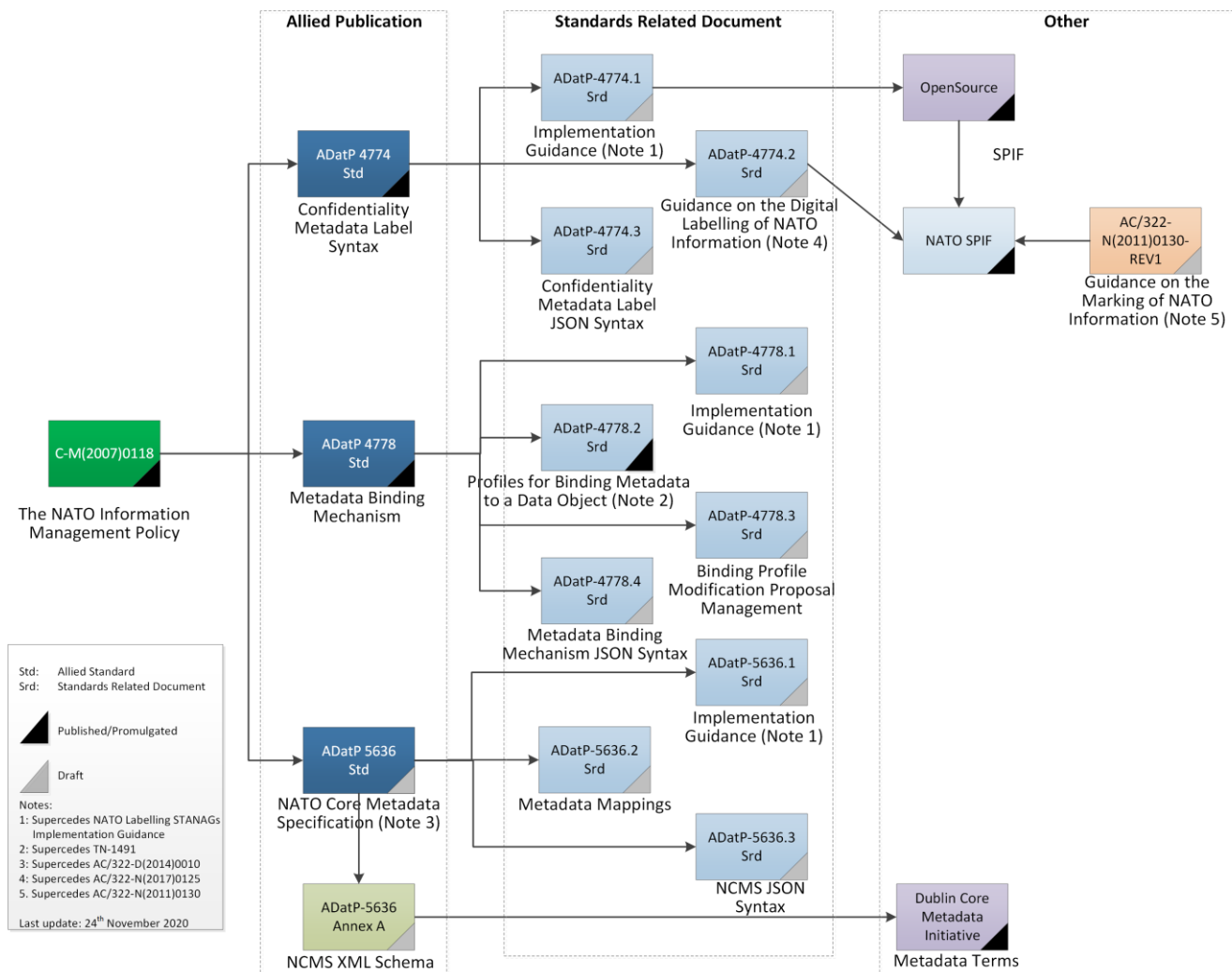
- A. AC/35-D/2004-REV3 Primary Directive on CIS Security, 15 November 2013
- B. C-M(2008)0113, The Primary Directive on Information Management (PDIM), 18 December 2008
- C. AC/322-N(2020)0090-Rev-AS1, Draft ADatP-5636 – NATO Core Metadata Specification (NCMS), 23 October 2020
- D. STANAG 4778 Metadata Binding Mechanism, Edition A Version 1, 26 October 2018
- E. STANAG 4774 Confidentiality Metadata Label Syntax, Edition A Version 1, 20 December 2017
- F. C-M(2002)49-REV1 Security Within The North Atlantic Treaty Organization (NATO) 20 November 2020
- G. C-M(2002)60 The Management of Non-Classified NATO Information, 11 July 2002
- H. AC/322-N(2011)0130 Guidance on the Marking Of NATO Information, 16 June 2011
- I. M-NACC-EAPC-1 (97)66 Basic Document of the Euro-Atlantic Partnership Council, 30 May 1997
- J. PO(2008)0122 NATO Georgia Framework Document, 15 September 2008
- K. C-R(98)30 Summary Record of A Meeting Of The Council, 25 May 1998
- L. DPA(2000)660 PFP Framework Document, 11 January 1994
- M. AC/324-N(2014)0022-AS1 Ownership Marking for Resolute Support, 1 December 2014
- N. DPA(98)1260 NATO Russia Founding Act, 12 October 1998
- O. DPA (97)758 NATO UKRAINE Charter, 28 May 1997
- P. AC/35-D/2002-REV5, Directive On The Security Of Information, 25 November 2020
- Q. STANAG 4406 Military Message Handling System, 26 October 2006
- R. AC/35-D/1002-REV8, NATO Security Classifications with Their National Equivalents, 27 March 2020
- S. AC/35-N(2013)0011-REV2-COR1 Security Agreements - Dates Of Signatures, 22 June 2020
- T. MC 458/3 NATO Education, Training, Exercise and Evaluation (ETEE) Policy, 03 September 2014
- U. AAP-03, Directive for the Production, Maintenance and Management of NATO Standardization, 28 February 2018

8.3 Abbreviations

ACDF	Access Control Decision Function
ADatP	Allied Data Processing Publication
CIS	Communication and Information Systems
COIs	Communities of Interest
EAPC	Euro-Atlantic Partnership Council
IP	Interoperability Platform
KFOR	Kosovo Force
MD	Mediterranean Dialogue
n/a	Not applicable
NCMS	NATO Core Metadata Specification
NGC	The NATO-Georgia Commission
NATO C3B	NATO C3 Board
NGO	Non-Governmental Organizations
NIMA	NATO Information Management Authority
NIMP	NATO Information Management Policy
NMRR	NATO Metadata Registry and Repository
NNEC	NATO Network Enabled Capability
NNEs	Non-NATO Entities
NRC	The NATO-Russia Council
NUC	The NATO-Ukraine Commission
PFP	Partnership for Peace
SPIF	Security Policy Information File
SRD	Standards Related Document
XML	Extensible Markup Language

ANNEX A NATO LABELLING STANAGs and RELATED DOCUMENTS

NATO Labelling STANAGs



ADatP-4774.2(A)(1)