



Intelligence Community Guidance Document

Roll-up Guidance for ISM

Version 2021-NOV

December 1, 2022

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Enterprise Need	1
1.4 - Conventions	2
1.4.1 - XML Namespaces	2
1.5 - Dependencies	3
1.5.1 - Specification Dependencies	3
1.5.2 - Inverse Dependencies	4
Chapter 2 - Development Guidance	5
2.1 - XSpec	5
2.2 - Understanding Roll-up	5
2.3 - Limitations of Roll-up	7
Chapter 3 - Constraints	8
3.1 - Data Validation Constraint Rules	8
Appendix A - Feature Summary	9
A.1 - ISM-Rollup Feature Summary	9
Appendix B - Change History	10
B.1 - V2021-NOV Initial Release Summary	10
Appendix C - Glossary	11
Appendix D - List of Abbreviations	12
Appendix E - Bibliography	13
Appendix F - Points of Contact	18

List of Figures

Figure 1 - Related Specifications	4
---	---

List of Tables

Table 1 - XML Namepaces	2
Table 2 - Dependencies	3
Table 3 - Feature Summary Legend	9
Table 4 - ISM-Rollup Feature comparison	9
Table 5 - Version Identifier History	10
Table 6 - Data Encoding Specification V2021-NOV Initial Release Summary	10

Chapter 1 - Introduction

1.1 - Purpose

This *Roll-up Guidance for ISM* (ISM-Rollup.XML) provides information on the Roll-up processes for *XML Data Encoding Specification for Information Security Markings* (ISM.XML^[23]) markings. This implementation uses Extensible Stylesheet Language (XSL) to determine what the roll-up security marking for documents marked with ISM.XML^[23] should be.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[11]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

This information guidance document addresses general concepts of using XSL to implement roll-up of security markings.

This specification is applicable to the IC and information produced by, stored, or shared within the IC. This document may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the Data Encoding Specification (DES) should be closely scrutinized and differences separately documented and assessed for applicability.

1.3 - Enterprise Need

The Intelligence Community Chief Information Officer (IC CIO) funds and oversees a number of critical enabling projects to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata including information security markings, enterprise data headers, and determination of an individual's need-to-know. A successful information sharing enterprise depends on the ability of the data creator and/or providers to accurately roll-up security markings via automated means.

This document provides general and prescriptive guidance on rolling-up ISM.XML^[23] markings on a given Extensible Markup Language (XML) document.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 200 Series:
 - Intelligence Community Directive (ICD) 208, *Write for Maximum Utility*^[12]
 - ICD 209, *Tearline Production and Dissemination*^[13]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*^[20]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer*^[14]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC*^[15]
 - Intelligence Community Program Guidance (ICPG) 500.2, *Attribute-based Authorization and Access Management*^[17]

- Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [\[21\]](#)
- ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* [\[22\]](#)
- 700 Series:
 - ICD 710, *Classification and Control Markings System* [\[16\]](#)
 - ICPG 710.1, *Application of Dissemination Controls: Originator Control* [\[18\]](#)
 - ICPG 710.2, *Application of Dissemination Controls: Foreign Disclosure and Release Markings* [\[19\]](#)
- Memorandums:
 - IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* [\[7\]](#)
- DoD Issuances:
 - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* [\[4\]](#)
- Executive Orders:
 - Executive Order 13526 *Classified National Security Information* [\[5\]](#)
 - Executive Order 13556 *Controlled Unclassified Information* [\[6\]](#)
- Implementing Directives:
 - 32 CFR Parts 2001 and 2003 *Classified National Security Information; Final Rule* [\[24\]](#)
 - 32 CFR Part 2002 *Controlled Unclassified; Final Rule* [\[25\]](#)
 - 32 CFR Parts 2003 *The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures* [\[26\]](#)
 - 32 CFR Parts 2004 *National Industrial Security Program Directive No. 1* [\[27\]](#)
 - ISOO Marking Booklet 2018 *Marking Classified National Security Information, Rev. 4 2018* [\[28\]](#)
 - CUI Category Registry *CUI Category Registry* [\[1\]](#)
 - CUI Limited Dissemination Controls Registry *CUI Limited Dissemination Controls Registry* [\[2\]](#)
 - CUI Marking Handbook *CUI Marking Handbook* [\[3\]](#)

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the “Specification Conventions” chapter in the IC-SF.XML [\[11\]](#).

1.4.1 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 1 - XML Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism
ntk	urn:us:gov:ic:ntk
arh	urn:us:gov:ic:arh

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML^[11].

1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g., Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the IC CIO specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[23])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[23] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[16] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[11])	This specification does not depend on a specific version of IC-SF.XML ^[11] ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.

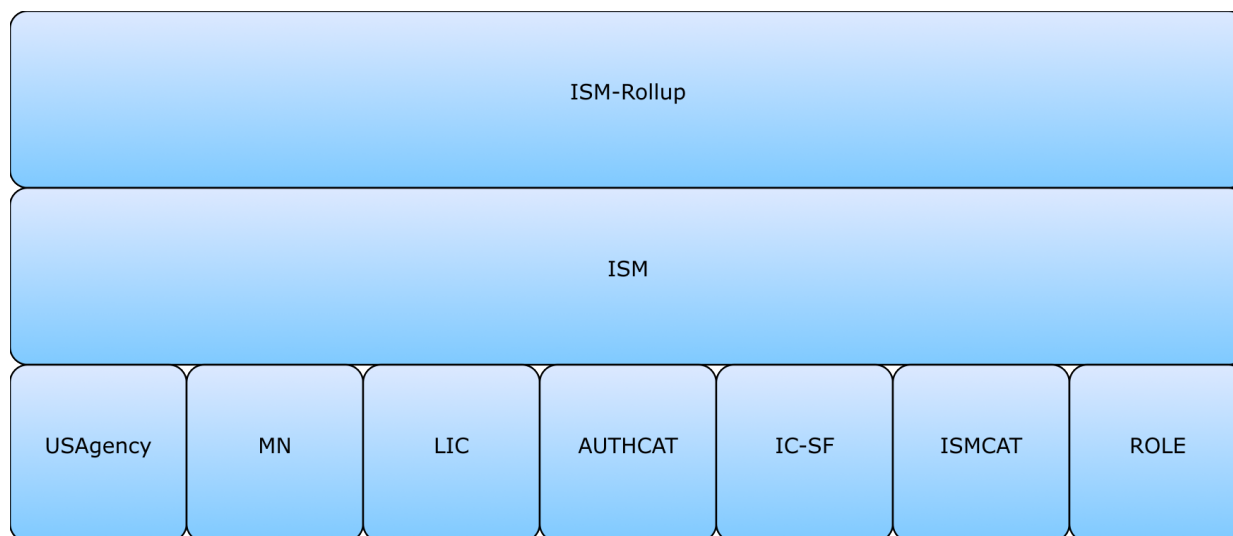


Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies (specifications that uses the given specification).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF^[11] framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this guidance document.

2.1 - XSpec

XSpec^[33] is a unit test and behaviour-driven development (BDD) framework for XSLT^[32], XQuery^[31], and Schematron^[30], consisting of a syntax for describing the behaviour of code, allowing the user to test code against those descriptions.

XSpec^[33] code is provided with this specification to allow the user the ability to test the functionality provided.

2.2 - Understanding Roll-up

Due to the complexity of things such as portion marking, decomposable Tetragraphs, and Foreign Disclosure & Release (FD&R) markings like REL TO, EYES, and DISPLAY ONLY, it can be difficult to determine what the overall classification for a document should be. ISM.XML^[23] provides information on what is wrong with a document; however, it does not help determine what the correct marking should be. The goal of ISM-Rollup.XML is to provide a tool that will help users make the proper classification markings. For SCI controls, for example, roll-up is just a union of all the values. The general solution must depend on ARH (See [Section 2.3 - Limitations of Roll-up](#)).

ISM-Rollup.XML takes documents marked up with ISM.XML^[23] and determines what the roll-up should be. The roll-up is guaranteed to not be over classified but cannot guarantee that it will not be under classified, because automated roll-up code cannot determine that a document needs to be classified by compilation. Straight forward examples:

- $S + S = S$
- $S + TS = TS$
- $U + C + S = S$
- A document marked with only Secret portions will NEVER be rolled up by ISM-Rollup.XML to Top Secret. A human can decide that classification by compilation rolls up Secret portions to Top Secret, but the ISM-Rollup.XML automated logic cannot do that.

It becomes more complicated when Tetragraphs are present in FD&R markings like REL TO, EYES, and DISPLAY ONLY. In order to determine the overall classification, the intersection of all the countries and Tetragraphs needs to be determined. For example:

- $REL\ TO\ USA,\ CAN,\ AUS + REL\ TO\ USA,\ CAN,\ GBR = REL\ TO\ USA,\ CAN$

If a Tetragraph is not on all portions and is decomposable, it would need to be decomposed and rolled-up. For example if a portion is marked with FRME:

- REL TO USA, AUS, CAN, FRA, YEM + REL TO USA, FRME
- REL TO USA, FRME is decomposed to REL TO USA, AUS, BEL, CAN, DNK, FRA, DEU, ITA, NLD, NZL, NOR, ESP, GBR
- Making the roll-up: REL TO USA, AUS, CAN, FRA
- YEM does not roll up to the banner because YEM is not a member of FRME.

Two areas of complexity in the roll-up of countries and Tetragraphs are:

1. Tetragraphs that are not decomposable. A Tetragraph that is not decomposable cannot be expanded into its component countries for the purposes of roll-up; it can only be rolled up as the Tetragraph.
2. While most portions participate in the roll-up of countries and Tetragraphs, there is one type of portion that does not participate in the roll-up of countries and Tetragraphs. Unclassified Uncaveated portions do not contribute to the roll-up of countries and Tetragraphs. In contrast, Unclassified Caveated information will be treated as NOFORN for the purposes of roll-up for automated access control. *Intelligence Community Markings System Register and Manual* (DEC 2015)^[10]

If a Tetragraph is not on all portions and is not decomposable, it will usually result in the roll-up being marked NOFORN; however, it might not be rolled up to NOFORN if the document has any Uncaveated Unclassified portions, because Uncaveated Unclassified portions do not participate in REL TO roll-up. ISM.XML^[23] follows the 2015 *Intelligence Community Markings System Register and Manual* (DEC 2015)^[10] in its roll-up of Unclassified Uncaveated and Unclassified Caveated portions. For example, because the Tetragraph GFNX is not decomposable:

- If GFNX IS on every line: REL TO USA, AUS, CAN, GFNX + REL TO USA, GFNX = REL TO USA, GFNX
- If GFNX is NOT on every line:
 - U + S//REL TO USA, GFNX = S//REL TO USA, GFNX because the first portion is Unclassified Uncaveated
 - U//FOUO + S//REL TO USA, GFNX = NOFORN because the first portion is Unclassified Caveated
 - U//FOUO//REL TO USA, GFNX + S//REL TO USA, GFNX = S//REL TO USA, GFNX because all portions are REL TO USA, GFNX.

DISPLAY ONLY is similar to the rules for REL TO; only the REL TO countries MUST be considered also. For example:

- REL TO USA, CAN + DISPLAY ONLY CAN = DISPLAY ONLY CAN
- A portion that is REL TO CAN is certainly able to be Displayed to CAN, but a portion that is DISPLAY ONLY CAN is not releasable to CAN.

2.3 - Limitations of Roll-up

Roll-up procedures are limited when Need-To-Know Metadata (NTK) data concepts are present. When NTK data concepts are present, an Access Rights and Handling (ARH) container MUST be used. NTK has two main sub-structures; **ntk:RequiresAnyOf** and **ntk:RequiresAllOf**.

The ability to roll-up more than one **ntk:RequiresAnyOf** is not currently possible as there is no nesting logic capability.

When more than one **ntk:RequiresAllOf** is present, the originator and the order of the values MUST be taken into consideration. For example:

- If the originator is the same:
 - ORCON originator=CIA dissemto=NSA NRO would be a duplicate of originator=CIA dissemto=NRO NSA
- If the originator is different:
 - ORCON originator=CIA dissemto= NSA NRO is NOT considered a dupe of originator=NSA dissemto= CIA NSA

In theory, combining multiple Originator Controlled (ORCON) could result in a document that is impossible to read. For example, combining originator=CIA dissemto= NRO NSA with originator=DIA dissemto= NGA STATE would result in a spill.

This initial release of ISM-Rollup.XML does not handle roll-up of documents that have Controlled Unclassified Information (CUI) markings. Roll-up support of CUI markings will be implemented in a future release.

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

The ISM-Rollup.XML is a tool that uses portion marking metadata to generate valid classification metadata at the document level. Unlike standards such as PUBS.XML^[29], ISM-Rollup.XML is not used to hold shared documents or data files; instead, it is a tool that helps users roll-up portion markings. The ISM.XML^[23] resource node in a document contains the security metadata for the classification banner of the document. ISM.XML^[23] attributes in XML elements that are not the resource node contain metadata for portion marks. ISM-Rollup.XML can also be used to validate whether the ISM.XML^[23] classification metadata in portions of a document roll up correctly to the classification metadata in the resource node of the document. In that sense, ISM-Rollup.XML is itself a set of data validation constraint rules.

ISM-Rollup.XML does not contain XML schema, Controlled Vocabulary Enumeration (CVE)s, or Schematron^[30] files. Instead, ISM-Rollup.XML consists of the following artifacts:

- This DES.
- Transformations (XSLT) code that rolls up the portion marking metadata and creates the minimum classification banner metadata to properly protect the data. The main program file for this code is ISM-Rollup.xsl.
- A set of XSpec^[33] files and XSLT code that links the XSpec^[33] files to the ISM-Rollup.xsl code. The XSpec^[33] files in ISM-Rollup.XML provide executable validation constraints on ISM-Rollup.XML output. Users can add their own XSpec^[33] unit test cases to check whether a set of portion marks rolls up to expected classification banner metadata. These XSpec^[33] unit tests define:
 1. ISM.XML^[23] metadata for the portion marks of a document.
 2. Expectations of the result of ISM-Rollup.xsl executed against portion marking metadata. The results of ISM-Rollup.xsl are compared against the expected banner results. If the results of ISM-Rollup.xsl differ from the expected banner metadata, then an error message appears in the output of the XSpec^[33] test.

Appendix A Feature Summary

The following tables summarize major features by version for ISM-Rollup.XML. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g., The IC Markings^[9] has an implementation date of one year after issuance).

Table 3 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can’t comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. ISM-Rollup Feature Summary

Table 4 - ISM-Rollup Feature comparison

Required date	Feature	V2021-NOV
December 3, 2021	Defines the initial capabilities for implementing roll-up for ISM attributes and NTK access profiles.	F

Appendix B Change History

The following table summarizes the version identifier history for this document.

Table 5 - Version Identifier History

Version	Date	Purpose
2021-NOV	December 3, 2021	Initial Release. For details, see Section B.1 - V2021-NOV Initial Release Summary

B.1 - V2021-NOV Initial Release Summary

Significant drivers for Version V2021-NOV include:

- Creation of ISM-Roll-up specification.

The following table summarizes the initial release in V2021-NOV.

Table 6 - Data Encoding Specification V2021-NOV Initial Release Summary

#	Change	Artifacts changed	Compatibility Notes
	Creation of ISM-Roll-up specification.(CR-2018-065)	Documentation XSL	Initial Release.

Appendix C Glossary

This appendix lists terms, definitions and sources of the definitions for terms used in this document.

Caveated	<p>Caveated means a document bears no FD&R markings, but has one or more AEA markings, SAP markings, and/or dissemination control marking(s) (i.e., all IC and non-IC dissemination controls). SCI controls are intentionally not listed. If only an SCI marking is present, the information is considered Uncaveated.</p> <p>Source: IC Markings Register & Manual^[8]</p>
decomposable	<p>The term decomposable in the context of security markings refers to a decomposable Tetragraph. A decomposable Tetragraph is one that can be separated into its constituent countries for the purposes of rolling up portion markings into an overall classification banner for a document or data file. For example, FVEY is a decomposable Tetragraph. If a document has two portions, one that is REL TO USA, GBR, ZWE, and one that is REL to USA, FVEY, then the document's portions roll up to REL TO USA, GBR.</p> <p>If a Tetragraph is not decomposable, then all portions (except completely UNCLASSIFIED portions) must be REL TO the Tetragraph for the docu</p>
Tetragraph	<p>A Tetragraph is a group of countries represented by a four-character string, e.g., FVEY for the Five Eyes countries of USA plus AUS, CAN, GBR, and NZL. Tetragraphs are used in the context of security markings classification, e.g., RELEASABLE TO USA, FVEY.</p>
Uncaveated	<p>Uncaveated means the document bears no FD&R markings and no AEA markings, SAP markings, and/or dissemination control marking(s) (i.e., all IC and non-IC dissemination controls). SCI controls are intentionally not listed. If only an SCI marking is present, the information is considered uncaveated.</p> <p>Source: IC Markings Register & Manual^[8]</p>

Appendix D List of Abbreviations

This appendix lists all the acronyms and abbreviations referenced in this encoding specification.

AEA	Atomic Energy Act
ARH	Access Rights and Handling
CUI	Controlled Unclassified Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
FD&R	Foreign Disclosure & Release
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
ISOO	Information Security Oversight Office
NTK	Need-To-Know Metadata
ORCON	Originator Controlled
SAP	Special Access Program
SCI	Sensitive Compartmented Information
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix E Bibliography

- [1] CUI Category Registry
National Archives and Records Agency. *CUI Category Registry*.
Available online at: <https://www.archives.gov/cui/registry/category-list>
- [2] CUI Limited Dissemination Controls Registry
National Archives and Records Agency. *CUI Limited Dissemination Controls Registry*.
Available online at: <https://www.archives.gov/cui/registry/limited-dissemination>
- [3] CUI Marking Handbook
National Archives and Records Agency. *Marking Controlled Unclassified Information*.
Available online at: <https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf>
- [4] DoD Manual 5205.07
Under Secretary of Defense for Intelligence. *Special Access Program (SAP) Security Manual: Marking (Vol 4)*. 5205.07. October 10, 2013.
Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520507-V4p.pdf?ver=2020-09-09-110203-730>
- [5] E.O. 13526
The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.
Available online at: <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>
- [6] E.O. 13556
The White House. *Executive Order 13556 – Controlled Unclassified Information*. 4 November 2010.
Available online at: <https://www.archives.gov/files/isoo/policy-documents/eo-13556.pdf>
- [7] IC CIO Memo 2018-081
Intelligence Community Chief Information Officer. *IC CIO Memo 2018-081: Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness*. 26 November 2018.
- [8] IC Markings AUG 2019
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 30 Aug 2019.
Available online Intelink-TS at: <https://go.ic.gov/gbMr5fv> (case sensitive – golf bravo Mike romeo 5 foxtrot victor)
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>
- [9] IC Markings
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.
Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[10] IC Markings DEC 2015

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 24 Dec 2015.

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[11] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf)

Available online Intelink-U at: <https://w3id.org/ic/standards/IC-SF>

Available online at: <https://w3id.org/ic/standards/public>

[12] ICD 208

Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.

Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[13] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.

Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>

[14] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[15] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <https://go.ic.gov/fTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[16] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

Available online Intelink-TS at: <https://go.ic.gov/oSj9K7O> (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[17] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online Intelink-TS at: <https://go.ic.gov/NUAEWk1> (case sensitive – November Uniform Alpha Echo Whiskey kilo 1)

Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[18] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <https://go.ic.gov/fdyoylS> (case sensitive – foxtrot delta yankee oscar yankee India Sierra)

Available online at: <http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf>

[19] ICPG 710.2

Director of National Intelligence. *Application of Dissemination Controls: Foreign Disclosure and Release Markings*. Intelligence Community Policy Guidance 710.2. 20 March 2014.

Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710-2_403-5.pdf

[20] ICPM 2007-200-2

Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2. 11 December 2007.

Available online at: <http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf>

[21] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[22] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <https://go.ic.gov/0Agmenr> (case sensitive – 0 Alpha golf mike echo november romeo)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[23] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)

Available online Intelink-U at: <https://w3id.org/ic/standards/ISM>

Available online at: <https://w3id.org/ic/standards/public>

[24] ISOO 32 CFR Parts 2001 and 2003

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information; Final Rule*. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. 28 June 2010.

Available online at: <http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf>

[25] ISOO 32 CFR Part 2002

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Controlled Unclassified; Final Rule*. 32 CFR Parts 2002. Federal Register, Vol. 81, No. 178. 14 September 2016.

Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2002.pdf>

[26] ISOO 32 CFR Parts 2003

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures*. 32 CFR Parts 2003. Federal Register, Vol. 77, No. 131. 9 July 2012.

Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2003.pdf>

[27] ISOO 32 CFR Parts 2004 Amendment

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *National Industrial Security Program Directive No. 1*. 32 CFR Parts 2004. Federal Register, Vol. 75, No. 65. 6 April 2010.

Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2004-amendment.pdf>

[28] ISOO Marking Booklet 2018

Information Security Oversight Office. *Marking Classified National Security Information 2018*. Rev. 4, January 2018.

Available online at: <https://www.archives.gov/files/isoo/training/marketing-booklet-revision.pdf>

[29] PUBS.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Intelligence Publications (PUBS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/u6bb18P> (case sensitive – uniform 6 bravo bravo 1 8 Papa)

Available online Intelink-U at: <https://w3id.org/ic/standards/PUBS>

Available online at: <https://w3id.org/ic/standards/public>

[30] Schematron

International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.

ISO Spec Available online at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

StyleSheets for compiling Available online at: <http://code.google.com/p/schematron/>

[31] XQuery

World Wide Web Consortium (W3C). *XQuery 3.0: An XML Query Language*. W3C Candidate Recommendation 08 January 2013.
Available online at: <http://www.w3.org/TR/xquery-3/>

[32] XSLT2

World Wide Web Consortium (W3C). *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.
Available online at: <http://www.w3.org/TR/xslt20/>

[33] XSpec

XSLT Unit Test (XSpec). *XSpec*.
Available online at: <https://github.com/xspec/xspec/wiki>

Appendix F Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at the following Director of National Intelligence (DNI)-sponsored web sites.

Public Website: <https://w3id.org/ic/standards/public>

Intelshare: <https://w3id.org/ic/standards/data-specs>

Direct all inquiries about this IC technical specification, IC technical specification collaboration and coordination forums, or IC element representatives involved in those forums, to the IC CIO.

E-mail: ic-standards-support@odni.gov.