



# **Intelligence Community Technical Specification**

---

## **XML Data Encoding Specification for Information Security Markings**

**Version 2021-NOVr2022-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 .....	2
1.3 - Enterprise Need .....	2
1.3.1 - Policy Variances .....	4
1.4 - Conventions .....	6
1.4.1 - XML Namespaces .....	6
1.5 - Dependencies .....	6
1.5.1 - Specification Dependencies .....	6
1.5.2 - Inverse Dependencies .....	9
Chapter 2 - Development Guidance .....	11
2.1 - Understanding Access Control .....	11
2.2 - ISM.XML and Access Control .....	11
2.2.1 - Guidance for systems processing data containing NTK metadata .....	12
2.3 - Potential Unauthorized Disclosure Data Spill Procedures .....	13
2.4 - Additional Guidance .....	14
2.4.1 - Guidance for the ISM Segment .....	14
2.4.1.1 - Document Compliance and Exemptions .....	14
2.4.1.2 - Physical XML Attribute Groups .....	15
2.4.1.3 - Notices .....	16
2.4.1.3.1 - US-Person .....	17
2.4.1.3.2 - Point Of Contact Requirements .....	17
2.4.1.3.3 - pre13526ORCON .....	18
2.4.1.3.4 - CVEnumISMNoticeProse Value Numbering Convention .....	18
2.4.1.4 - Originator Controlled Assets .....	19
2.4.1.5 - Section and Portion Style Marking Limitations .....	19
2.4.1.6 - ISM Schema Types .....	20
2.4.1.7 - ISM Schema Attributes .....	20
2.4.1.8 - ISM Schema Attribute Groups .....	34
2.4.1.9 - Use of ISM for SAP Accesses .....	39
2.4.1.9.1 - Classification-based Read-ons for DoD SAPs .....	39
2.4.1.9.2 - Rendering SAPs in Classification Banners and Portion Marks ....	40
2.4.1.9.3 - Rendering Stylesheet for DOD .....	42
2.4.1.9.4 - Rules for SAP Values in ISM SARIdentifier .....	42
2.4.1.9.5 - Published and Unpublished SAPs .....	43
2.4.1.9.6 - WAIVED Dissemination Control for DoD SAPs .....	43
2.4.2 - NTK Guidance .....	43
2.4.2.1 - NTK Integration into a Schema .....	43
2.4.2.2 - NTK Basic Usage Model .....	44
2.4.3 - ARH Guidance .....	44
2.4.3.1 - ARH Security and ExternalSecurity .....	44
2.4.3.2 - ARH MIME type .....	44
Chapter 3 - Constraints .....	45
3.1 - "Living" Constraint Rules .....	45
3.2 - Data Validation Constraint Rules .....	45
3.2.1 - Value Enumeration Constraints .....	46

3.2.2 - Additional Constraints .....	46
3.2.2.1 - DES Constraints .....	46
3.2.3 - Constraint Rules .....	46
3.3 - Data Rendering Constraint Rules .....	46
3.3.1 - Purpose .....	46
3.3.2 - ISM.XML Rendering Constraint Rules .....	47
3.3.2.1 - [ISM-RENDER-00001] .....	47
3.3.2.2 - [ISM-RENDER-00002] .....	47
3.3.2.3 - [ISM-RENDER-00003] .....	47
3.3.2.4 - [ISM-RENDER-00004] .....	48
3.3.2.5 - [ISM-RENDER-00005] .....	49
3.3.2.6 - [ISM-RENDER-00006] .....	49
3.3.2.7 - [ISM-RENDER-00007] .....	49
3.3.2.8 - [ISM-RENDER-00008] .....	50
3.3.3 - NTK Rendering Constraint Rules .....	50
3.3.3.1 - [NTK-RENDER-00001] .....	50
3.3.3.2 - [NTK-RENDER-00002] .....	50
3.3.3.3 - [NTK-RENDER-00003] .....	51
3.3.3.4 - [NTK-RENDER-00004] .....	51
3.3.3.5 - [NTK-RENDER-00005] .....	51
Chapter 4 - NTK Access Profiles .....	53
4.1 - Access Profile Structures .....	53
4.1.1 - Agency Dissemination .....	53
4.1.2 - Data Sphere .....	53
4.1.3 - Group and Individual .....	53
4.2 - Profile DES .....	53
4.3 - Vocabulary Types .....	54
4.3.1 - Abstract Root Types .....	54
4.3.2 - Vocabulary Types .....	55
4.3.2.1 - Built-In Vocabulary Types .....	55
4.3.2.2 - Further Defining Built-In Vocabulary Types .....	56
4.4 - Pre-Defined Access Profiles .....	57
4.4.1 - Enterprise Role Permissive .....	57
4.4.2 - Enterprise Role Restrictive .....	58
4.4.3 - Exclusive Distribution (EXDIS) .....	58
4.4.4 - Group Permissive .....	58
4.4.5 - Group Restrictive .....	59
4.4.6 - Intelligence Community Only (ICO) .....	59
4.4.7 - License .....	59
4.4.8 - Mission Need Profile .....	59
4.4.9 - No Distribution (NODIS) .....	60
4.4.10 - Originator Controlled (ORCON) .....	60
4.4.11 - Proprietary Information (PROPIN) .....	61
4.4.12 - Restricted Authority Category (RAC) .....	61
Chapter 5 - Controlled Unclassified Information (CUI) .....	62
5.1 - Overview .....	62
5.2 - CUI and the IC Markings System Register and Manual .....	62
5.3 - Pure CUI and Commingled Documents .....	63
5.4 - CUI Banner .....	64

5.5 - CUI Block .....	67
5.6 - CUI Constraint Rules .....	68
5.6.1 - Dissemination Controls in CUI Documents .....	69
5.6.2 - Rules for Pure CUI Documents .....	69
5.6.3 - Rules for Commingled Documents .....	69
5.6.4 - NTK Rules for Documents Containing CUI .....	70
5.6.5 - Notice Rules for Documents Containing CUI .....	70
5.7 - CUI Rendering Stylesheets .....	70
Chapter 6 - Progressive Validation Using Phases .....	72
6.1 - Overview .....	72
Appendix A - Feature Summary .....	75
A.1 - ISM Feature Summary .....	75
A.1.1 - Features from V2019-MARr2019-SEP to V2021-NOVr2022-NOV .....	75
A.1.1.1 - Features Partial and N/A from V2019-MARr2019-SEP to V2021-NOVr2022-NOV .....	76
A.1.2 - Features from 2016-SEPr2018-NOV to V2019-MARr2019-SEP .....	76
A.1.2.1 - Features Partial and N/A from 2016-SEPr2018-NOV to V2019-MARr2019-SEP .....	77
A.1.3 - Features from V2016-SEPr2017-JUL to 2016-SEPr2018-NOV .....	78
A.1.3.1 - Features Partial and N/A from V2016-SEPr2017-JUL to 2016-SEPr2018-NOV .....	78
A.1.4 - Features from V2014-DEC to V2016-SEPr2017-JUL .....	79
A.1.4.1 - Features Partial and N/A from V2014-DEC to V2016-SEPr2017-JUL ...	80
A.1.5 - Features from V11 to V2014-DEC .....	80
A.1.5.1 - Features Partial and N/A from V11 to V2014-DEC .....	81
A.1.6 - Features from V8 to V11 .....	81
A.1.6.1 - Features Partial and N/A from V8 to V11 .....	83
A.1.7 - Features from V5 to V8 .....	84
A.1.7.1 - Features Partial and N/A from V5 to V8 .....	85
A.1.8 - Features from V2 to V5 .....	85
A.1.8.1 - Features Partial and N/A from V2 to V5 .....	87
A.1.9 - Features from V1 to V2 .....	87
A.1.9.1 - Features Partial and N/A from V1 to V2 .....	88
Appendix B - Change History .....	89
B.1 - V2021-NOVr2022-NOV Change Summary .....	90
B.2 - V2021-NOV Change Summary .....	92
B.3 - V2019-MARr2020-OCT Change Summary .....	99
B.4 - V2019-MARr2019-SEP Change Summary .....	102
B.5 - V2019-MARr2019-JUN Change Summary .....	103
B.6 - V2019-MAR Change Summary .....	103
B.7 - V2016-SEPr2018-NOV Change Summary .....	109
B.8 - V2016-SEPr2018-JUL Change Summary .....	109
B.9 - V2016-SEPr2018-APR Change Summary .....	110
B.10 - V2016-SEPr2017-JUL Change Summary .....	113
B.11 - V2016-SEP Change Summary .....	117
B.12 - V2015-AUG Change Summary .....	121
B.13 - V2014-DEC Change Summary .....	124
B.14 - V13 Change Summary .....	126
B.15 - V12 Change Summary .....	127

B.16 - V11 Change Summary .....	132
B.17 - V10 Change Summary .....	134
B.18 - V9 Change Summary .....	142
B.19 - V8 Change Summary .....	145
B.20 - V7 Change Summary .....	148
B.21 - V6 Change Summary .....	151
B.21.1 - V6 Change Errata .....	156
B.22 - V5 Change Summary .....	156
B.22.1 - V5 Change Errata .....	163
B.23 - V4 Change Summary .....	163
B.24 - V3 Change Summary .....	165
B.25 - V2 Change Summary .....	170
Appendix C - List of Abbreviations .....	174
Appendix D - Bibliography .....	177
Appendix E - Points of Contact .....	187
Appendix F - IC CIO Approval Memo .....	188

## List of Figures

Figure 1 - Related Specifications .....	9
Figure 2 - Inverse Dependency Specifications .....	10

## List of Tables

Table 1 - XML Namepaces .....	6
Table 2 - Direct Dependencies .....	7
Table 3 - CVEnumISMNoticeProse Value Numbering Convention .....	18
Table 4 - ISM Schema Simple Types .....	20
Table 5 - ISM Schema Complex Types .....	20
Table 6 - ISM Schema Attributes .....	21
Table 7 - ism:ISMNoticeBaseAttributeGroup .....	34
Table 8 - ism:ISMNoticeAttributeGroup .....	34
Table 9 - ism:ISMNoticeExternalAttributeGroup .....	35
Table 10 - ism:ISMResourceAttributeGroup .....	35
Table 11 - ism:ISMResourceAttributeOptionGroup .....	35
Table 12 - ism:ISMRootNodeAttributeGroup .....	35
Table 13 - ism:ISMRootNodeAttributeOptionGroup .....	35
Table 14 - ism:NoticeAttributesGroup .....	36
Table 15 - ism:NoticeAttributesOptionGroup .....	36
Table 16 - ism:NoticeExternalAttributesGroup .....	36
Table 17 - ism:NoticeExternalAttributesOptionGroup .....	36
Table 18 - ism:POCAttributeGroup .....	36
Table 19 - ism:ResourceNodeAttributeGroup .....	36
Table 20 - ism:ResourceNodeAttributeOptionGroup .....	36
Table 21 - ism:SecurityAttributesGroup .....	37
Table 22 - ism:SecurityAttributesOptionGroup .....	38
Table 23 - NTK Profile DES Values .....	54
Table 24 - CUI Limited Dissemination Controls .....	66
Table 25 - ISM Schematron Phases .....	72
Table 26 - Feature Summary Legend .....	75
Table 27 - ISM Feature Comparison V2019-MARr2019-SEP to V2021-NOVr2022-NOV .....	75
Table 28 - ISM Feature Comparison V2019-MARr2019-SEP to V2021-NOVr2022-NOV .....	76
Table 29 - ISM Feature Comparison 2016-SEPr2018-NOV to V2019-MARr2019-SEP .....	76
Table 30 - ISM Feature Comparison 2016-SEPr2018-NOV to V2019-MARr2019-SEP .....	77
Table 31 - ISM Feature Comparison V2016-SEPr2017-JUL to 2016-SEPr2018-NOV .....	78
Table 32 - ISM Feature Comparison V2016-SEPr2017-JUL to 2016-SEPr2018-NOV .....	78
Table 33 - ISM Feature Comparison V2014-DEC to V2016-SEPr2017-JUL .....	79
Table 34 - ISM Feature Comparison V2014-DEC to V2016-SEPr2017-JUL .....	80
Table 35 - ISM Feature Comparison V11 to V2014-DEC .....	80
Table 36 - ISM Feature Comparison V11 to V2014-DEC .....	81
Table 37 - ISM Feature Comparison V8 to V11 .....	81
Table 38 - ISM Feature Comparison V8 to V11 .....	83
Table 39 - ISM Feature Comparison V5 to V8 .....	84
Table 40 - ISM Feature Comparison V5 to V8 .....	85
Table 41 - ISM Feature Comparison V2 to V5 .....	85
Table 42 - ISM Feature Comparison V2 to V5 .....	87
Table 43 - ISM Feature Comparison V1 to V2 .....	87
Table 44 - ISM Feature Comparison V1 to V2 .....	88
Table 45 - DES Version Identifier History .....	89
Table 46 - Data Encoding Specification 2021-NOVr2022-NOV Change Summary .....	91



Table 47 - Data Encoding Specification 2021-NOV Change Summary .....	92
Table 48 - Data Encoding Specification V2019-MARr2020-OCT Change Summary .....	99
Table 49 - Data Encoding Specification 2019-MARr2019-SEP Change Summary .....	102
Table 50 - Data Encoding Specification 2019-MARr2019-JUN Change Summary .....	103
Table 51 - Data Encoding Specification 2019-MAR Change Summary .....	104
Table 52 - Data Encoding Specification 2016-SEPr2018-NOV Change Summary .....	109
Table 53 - Data Encoding Specification 2016-SEPr2018-JUL Change Summary .....	110
Table 54 - Data Encoding Specification 2016-SEPr2018-APR Change Summary .....	110
Table 55 - Data Encoding Specification 2016-SEPr2017-JUL Change Summary .....	114
Table 56 - Data Encoding Specification 2016-SEP Change Summary .....	118
Table 57 - Data Encoding Specification 2015-AUG Change Summary .....	121
Table 58 - Data Encoding Specification 2014-DEC Change Summary .....	124
Table 59 - Data Encoding Specification V13 Change Summary .....	127
Table 60 - Data Encoding Specification V12 Change Summary .....	128
Table 61 - Data Encoding Specification V11 Change Summary .....	133
Table 62 - Data Encoding Specification V10 Change Summary .....	135
Table 63 - Data Encoding Specification V9 Change Summary .....	142
Table 64 - Data Encoding Specification V8 Change Summary .....	145
Table 65 - Data Encoding Specification V7 Change Summary .....	149
Table 66 - Data Encoding Specification V6 Change Summary .....	152
Table 67 - Data Encoding Specification V6 Change Errata .....	156
Table 68 - Data Encoding Specification V5 Change Summary .....	157
Table 69 - Data Encoding Specification V5 Change Errata .....	163
Table 70 - Data Encoding Specification V4 Change Summary .....	164
Table 71 - Data Encoding Specification V3 Change Summary .....	165
Table 72 - Data Encoding Specification V2 Change Summary .....	171

## List of Examples

4.1 - Individual identified by IC PKI Distinguished Name .....	55
4.2 - Individual identified by CAD PKI Distinguished Name .....	55
4.3 - Group from the ICAM Service Provider Entitlement Management Service system .....	55
4.4 - Agencies from the USAgency.CES <sup>[71]</sup> specification .....	56
4.5 - Issues from the Mission Need <sup>[63]</sup> specification .....	56
4.6 - Regions from the Mission Need <sup>[63]</sup> specification .....	56
4.7 - Licenses from the License CES <sup>[62]</sup> specification .....	56
4.8 - Restricted Authority Categories from the AUTHCAT.CES <sup>[1]</sup> specification .....	56
4.9 - Declaring USAgency Version .....	57
4.10 - Agency Dissem Access Profile .....	57

## Chapter 1 - Introduction

### 1.1 - Purpose

This *XML Data Encoding Specification for Information Security Markings* (ISM.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode Information Security Markings (ISM.XML) data. This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing security markings and Need-To-Know Metadata (NTK) data concepts using XML, and for wrapping security markings and NTK attributes together in an Access Rights and Handling (ARH) XML container.

ISM.XML consists of three segments that meet different policy objectives and requirements for the protection of national security data:

- The Information Security Markings (ISM) segment of ISM.XML is used to represent how to add classification and control markings metadata in documents and electronic data, as detailed in Intelligence Community Directive (ICD) 710 *Classification and Control Marking System* [39]. The ISM segment of ISM.XML contains the security markings metadata that implements the classification banner, authority block, portion marking and warning notice requirements of Executive Order (E.O.) 13526, *Classified National Security Information* [24] and Information Security Oversight Office (ISOO) 32 CFR Parts 2001 and 2003 *Classified National Security Information; Final Rule* [51]. The ISM segment also implements requirements for warning notices for specific control markings prescribed in Intelligence Community (IC) Markings, *Intelligence Community Markings System Register and Manual* [28]. **In this document, the core security metadata for classification and control markings is referenced as ISM, while the entire specification that includes all three segments is referenced as ISM.XML.**
- The NTK segment of ISM.XML is used to represent the need-to-know properties assigned to an information resource that will be used, in conjunction with information about the user, and possibly other information, to determine the user's access to the data. Need-to-know is a determination that an entity requires access to classified information to perform or assist in authorized governmental functions (E.O. 13526[24]). The need-to-know determination is made based on the functions of an agency or the roles and responsibilities of the entity in the course of their official duties (ISOO 32 CFR Parts 2001 and 2003[51]). A single information resource may include multiple occurrences of NTK metadata in order to specify ISM.XML information according to multiple, different access policy systems. Each of the access policy systems will provide the specifics about the metadata to be captured.
- The *ARH* segment of ISM.XML combines NTK data concepts and ISM attributes into a single physical package. An *ARH* object always contains ISM attributes for classification and control markings. An *ARH* object may contain ISM warning notice metadata. An *ARH* object may contain NTK metadata.

ISM.XML supports the goal of “prescribing a uniform system for classifying, safeguarding, and declassifying national security information (ISOO 32 CFR Parts 2001 and 2003[51])” across national security disciplines, networks, services, and data. This goal is key to sharing information effectively while at the same time protecting national security information. Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata

(including enterprise data headers) to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of security metadata bound to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions being performed by human beings today.

## 1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML<sup>[34]</sup>) defines the basic conceptual structure and outlines the core philosophy of IC technical specifications. For convenience, a copy of this framework is included in every package.

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

## 1.3 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata including:

- information security markings
- enterprise data headers
- determination of an individual's need-to-know

Information assurance metadata supports interagency access control, automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of security marking metadata bound to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions being performed by human beings today. The enterprise will also increasingly rely on need-to-know metadata to allow users and systems to find and access a wide-range of data throughout the enterprise. A successful information sharing enterprise depends on the ability of the data creator and/or providers to specify the means by which need-to-know can be established in a manner to facilitate discovery and access via automated means.

Early in the intelligence life cycle, intelligence producers need:

- User interfaces that help reliably assign and manipulate information security markings.
- Automated formatting of IC classification and control markings as defined by E.O. 13526<sup>[24]</sup>, ICD 710<sup>[39]</sup>, and implemented by the IC Markings<sup>[28]</sup>. This includes portion marks, security banners, the classification authority block, and other security control markings.

- Cross-domain discovery, access, and dissemination capabilities.
- Standardization of various classification and control markings established for information sharing within the IC Markings<sup>[28]</sup> using the ISM.XML standard.
- IC Access Requirements and Handling that combines NTK data concepts and elements from ISM and extends them to access rights management and handling needs. The ISM.XML specification includes the markings representing access requirements and those for handling restrictions.
- Means to encode, in their data, the information an access system needs.
- Information encoded that varies by policy system and could include lists of individuals or groups permitted access, descriptions of subject matter in terms defined by the access policy, or other traits.

These capabilities will allow for security marking metadata to be captured and associated with intelligence structures in order to support attribute- and clearance-based information management practices, such as:

- Secure collaboration
- Content management
- Content and portion-level filtering of discovery results
- Cross-security domain content transfers
- Access granting
- Data protection
- Need-to-know access
- Evaluation of access an individual has to data

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

- 200 Series:
  - ICD 208, *Write for Maximum Utility*<sup>[35]</sup>
  - ICD 209, *Tearline Production and Dissemination*<sup>[36]</sup>
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*<sup>[43]</sup>
- 500 Series:
  - ICD 500, *Director Of National Intelligence Chief Information Officer*<sup>[37]</sup>
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC*<sup>[38]</sup>
  - Intelligence Community Program Guidance (ICPG) 500.2, *Attribute-based Authorization and Access Management*<sup>[40]</sup>
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance*<sup>[44]</sup>
  - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information*<sup>[45]</sup>

- 700 Series:
  - ICD 710, *Classification and Control Markings System* [\[39\]](#)
  - ICPG 710.1, *Application of Dissemination Controls: Originator Control* [\[41\]](#)
  - ICPG 710.2, *Application of Dissemination Controls: Foreign Disclosure and Release Markings* [\[42\]](#)
- Memorandums:
  - IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* [\[27\]](#)
- DoD Issuances:
  - Department of Defense Instruction Number 5200.48, *Controlled Unclassified Information (CUI)* [\[20\]](#)
  - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* [\[21\]](#)
  - Department of Defense Manual Number 5200.01, *DoD Information Security Program (Vol 1-3)* [\[19\]](#)
- Executive Orders:
  - Executive Order 13526 *Classified National Security Information* [\[24\]](#)
  - Executive Order 13556 *Controlled Unclassified Information* [\[25\]](#)
- Implementing Directives:
  - 32 CFR Parts 2001 and 2003 *Classified National Security Information; Final Rule* [\[51\]](#)
  - 32 CFR Part 2002 *Controlled Unclassified; Final Rule* [\[53\]](#)
  - 32 CFR Parts 2003 *The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures* [\[55\]](#)
  - 32 CFR Parts 2004 *National Industrial Security Program Directive No. 1* [\[56\]](#)
  - ISOO Marking Booklet 2018 *Marking Classified National Security Information, Rev. 4 2018* [\[57\]](#)
  - CUI Category Registry *CUI Category Registry* [\[13\]](#)
  - CUI Limited Dissemination Controls Registry *CUI Limited Dissemination Controls Registry* [\[14\]](#)
  - CUI Marking Handbook *CUI Marking Handbook* [\[15\]](#)
  - ISOO 32 CFR Part 2002 Clarification Memo *ISOO 32 CFR Part 2002 Clarification Memo, Date: June 4, 2019* [\[54\]](#)
- IC CIO Directives:
  - *Intelligence Community Markings System Register and Manual* [\[28\]](#)

### 1.3.1 - Policy Variances

There are a number of policy discrepancies in recent versions of the IC Markings [\[28\]](#) pertaining to how IC agencies and automated systems implement IC markings. The discrepancies conflict with established policy and differ from earlier versions of the Register, and/or are not machine implementable, thereby introducing enterprise risk into the safeguarding and sharing of data and information within the enterprise. This section documents these variances and how this release implements classification policy relating to the variances.

- **FD&R:** The Register gives conflicting guidance on the rollup of caveated unclassified information and explicit FD&R information. ISM.XML maintains adherence to the 2015 Register where mixing caveated unclassified information and explicit FD&R information rolls up to NOFORN.

- **Declassify On ISCAP exemptions:** Current wording in the Register could be interpreted to mean that documents marked with Interagency Security Classification Appeals Panel (ISCAP) exemptions do not require a declassification date in addition to the declassification exemption. Documents under E.O. 13526<sup>[24]</sup> require a declassification date or declassification event except when one of 25X1-EO-12951, 50X1-HUM, 50X2-WMD, AEA, NATO, or NATO-AEA is specified. In addition, documents with a declassification event also require a declassification date. For classified documents, ISM.XML requires either a declassification date or a declassification event with date, except when one of 25X1-EO-12951, 50X1-HUM, 50X2-WMD, AEA, NATO, or NATO-AEA is specified.
- **Declassify ON line:** There are two areas relating to the Declassify ON line:
  - The statements for the exemptions 50X1-50X9 and 25X1-25X9 could be interpreted as a mandate to list each and every unique exemption, choosing the longest declassification date/event from them. Prior interpretations had been to allow but not require multiple exemptions. ISM.XML allows but does not require that every possible exemption appear in a document.
  - The Registry content on the 75X1 exemption states that this exemption should appear with the appropriate automatic declassification exemption category number followed by the approved declassification date or event. Since declassification events require a declassification date, ISM.XML requires both a declassification date and event with the 75X1 exemption.
- **SCI Markings:** The Register sometimes states explicitly that an Sensitive Compartmented Information (SCI) compartment or subcompartment require its parent; e.g., HCS-P subcompartments explicitly require HCS-P. For other SCI compartments or subcompartments, however, the Register does not state that the marking requires its parent; e.g., the Register page for HCS-P does not say that it requires its parent, HCS. ISM.XML always requires the parent of any SCI compartment or subcompartment.
- **AEA RD and CNWDI:** The rule for access to Restricted Data (RD) conflicts with the access rule for Critical Nuclear Weapon Design Information (CNWDI). RD requires a Q clearance. Since CNWDI is a subset of RD, i.e., all CNWDI is RD, it could be assumed that all CNWDI requires a Q clearance since RD requires a Q clearance. Department of Energy (DOE) policy, however, does not require CNWDI to be restricted to people with a Q. This release of IC specifications requires a Q clearance for all RD data including CNWDI.
- **LIMDIS:** The Register lists two authorized portion mark options for LIMDIS: DS or LIMDIS. Allowing two different portion marks complicates automatic handling of classification metadata including automated access control decisions in Identity, Credential, and Access Management (ICAM) systems. ISM.XML only allows the "DS" portion mark.
- **RAWFISA:** In the Applicability paragraph for RAWFISA, the Register states that RAWFISA is available for Federal Bureau of Investigation (FBI) use only. In the Additional Markings Instruction, however, it states that the FBI is allowed to share raw FISA-acquired information in line with FISA, policies, and procedures. In addition, under Distribution statements and warnings, the Register states that RAWFISA-acquired information is shared internally within the FBI, as well as with certain IC elements for review, translation, analysis, and use in



accordance with standard minimization procedures. ISM.XML does not limit RAWFISA to FBI personnel, and the use of RAWFISA does not affect access control decisions.

## 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 [\[34\]](#).

### 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 [\[34\]](#).

### 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.

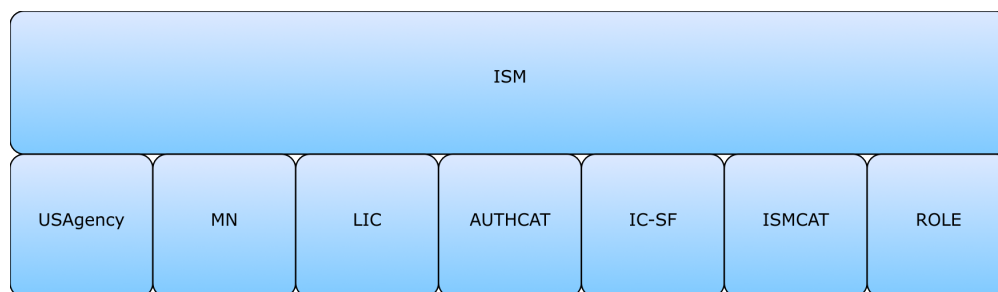
The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree 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 - Direct Dependencies**

Name	Dependency Description
<i>CVE Encoding Specification for ISM Country Codes and Tetragraphs</i> (ISM.CAT.CES.V2022-NOV+ <sup>[49]</sup> )	This specification depends on the LATEST technically sound, approved version of ISM.CAT.CES <sup>[49]</sup> . At the time of this release, the latest version of ISM.CAT.CES is 2022-NOV and MUST be used unless a later, technically sound, approved version of ISM.CAT.CES has been released. The requirement to use the latest technically sound, approved version is based on authoritative source compliance <sup>[65]</sup> .
<i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES.V2022-JUL+ <sup>[71]</sup> )	This specification does not depend on a specific version of USAgency.CES <sup>[71]</sup> ; versions later than version 2022-JUL MAY be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 22-2 was used for determining the version.
<i>CVE Encoding Specification for Mission Need</i> (MN.CES.V2021-NOV+ <sup>[63]</sup> )	This specification does not depend on a specific version of MN.CES <sup>[63]</sup> ; versions later than version 2021-NOV MAY be used. The minimum version was based on the earliest non-retired version; ESB 22-2 was used for determining the version.
<i>CVE Encoding Specification for License</i> (LIC.CES.V2015-AUG+ <sup>[62]</sup> )	This specification does not depend on a specific version of LIC.CES <sup>[62]</sup> ; versions later than version 2015-AUG MAY be used. The minimum version was based on the earliest non-retired version; ESB 22-2 was used for determining the version.
<i>CVE Encoding Specification for Authority Categories</i> (AUTHCAT.CES.V2018-APR+ <sup>[1]</sup> )	This specification does not depend on a specific version of AUTHCAT.CES <sup>[1]</sup> ; versions later than version 2018-APR MAY be used. The minimum version was based on the earliest non-retired version; ESB 22-2 was used for determining the version.
<i>CVE Encoding Specification for Role</i> (ROLE.CES.V2021-NOV+ <sup>[68]</sup> )	This specification does not depend on a specific version of ROLE.CES <sup>[68]</sup> ; versions later than version 2021-NOV MAY be used. The minimum version was based on the earliest non-retired version; ESB 22-2 was used for determining the version.

Name	Dependency Description
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ <sup>[34]</sup> )	<p>This specification does not depend on a specific version of IC-SF.XML<sup>[34]</sup>; 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.</p>
Schematron <sup>[69]</sup>	<p>Schematron — International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0<sup>[73]</sup> query binding.</p>
<p>XSLT 2.0<sup>[73]</sup> implementation of Schematron<sup>[69]</sup> by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): <a href="http://code.google.com/p/schematron/">http://code.google.com/p/schematron/</a>.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>

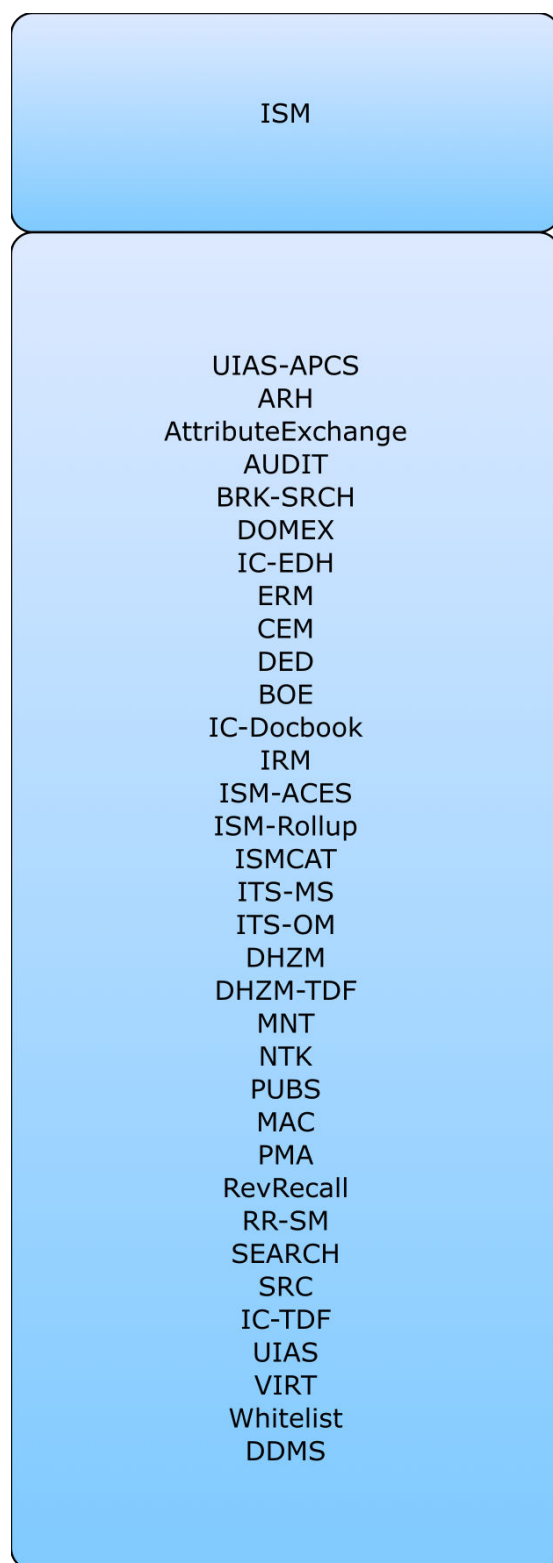


**Figure 1 : Related Specifications**

## 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).

Since this specification is one such specification that is used by other specifications released by the IC CIO, the [Figure 2](#) has been included to assist readers in understanding all of the inverse dependency relationships and how changes in this given specification may impact others specifications. This diagram is representative of direct and transitive inverse dependencies at the time of the release of this specification, but are subject to change over time and is presented in a list format that is different than [Figure 1](#).



**Figure 2 : Inverse Dependency Specifications**

## Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML<sup>[34]</sup> 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 specification.

### 2.1 - Understanding Access Control

This specification participates in the Data Attribute leg of the access control framework either as a primary specification or as a dependency of a primary specification. For more information, please see the “Components of Access Control Decisions” chapter in the IC-SF.XML<sup>[34]</sup> framework document.

### 2.2 - ISM.XML and Access Control

This section defines the relationship that ISM.XML has to Policy Encoding Documents for the purposes of automated access control. An ISM.XML access control system relies on 3 core elements:

1. Markings about the resource such as classification:

ISM.XML represents markings about the resource and implies a relationship to a set of access rules encoded in an Access Control Encoding Specification (ACES).

The ISM segment of ISM.XML represents the security markings describing the classification, dissemination, and caveats about the resource in accordance with the IC Markings<sup>[28]</sup>.

The NTK segment represents additional rules that may or may not require additional data. NTK represents metadata about a resource that impact an access control decision beyond its ISM classification markings. This metadata may supplement classification or control markings, as with agency dissemination NTK for Originator Controlled (ORCON) data, or provide other legal, administrative, and/or system-specific information for determining access to a given resource. To ensure data stability, NTK metadata should describe, categorize, label, and refine the resource itself instead of defining the mechanisms by which it is accessed.

Access control policies may evolve independently of the data and entity attributes used to enforce them.

2. Markings about the Person Entity (PE) or Non-Person Entity (NPE) desiring access:

*IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML<sup>[70]</sup>) is an example of a specification of markings about PEs and NPEs.

3. Rules for policy for granting access based on the markings:

The ACES associated with ISM.XML is the *Access Control Encoding Specification for Information Security Markings* (ISM.ACES<sup>[47]</sup>). ISM.ACES<sup>[47]</sup> prescribes access rules

triggered by ISM and NTK attributes on data. Each access rule in ISM.ACES<sup>[47]</sup> defines the conditions under which an entity with specific values of UIAS.XML<sup>[70]</sup> attributes may access data with specific values of ISM markings and, optionally, NTK markings.

NTK metadata references an access policy, often called an access policy system, along with any metadata needed to enforce the access policy. There are some access policies that require specific NTK metadata when a control marking is present in the ISM attributes. For example, if a document is marked with the ORCON dissemination control, then a type of NTK called ORCON-NTK is required. NTK metadata is expressed with one or more **ntk:AccessProfile** elements. Each **ntk:AccessProfile** MUST have an **ntk:AccessPolicy** element that contains the Uniform Resource Name (URN) of an access profile for that NTK statement. The **ntk:AccessPolicy** URN may be used to trigger Schematron rules, and it provides a pointer to a specific section of the ISM.ACES<sup>[47]</sup>. Each statement may also contain an **ntk:ProfileDes**, which contains a URN defined in this specification. The **ntk:ProfileDes** may conditionally be required depending on the specific access policy value. A **ntk:ProfileDes** defines structural constraints for an access profile, and the URN may be used to trigger additional Schematron rules. Each **ntk:AccessProfile** must be taken into account for access to a resource based on its location within either the **ntk:RequiresAllOf** element or the **ntk:RequiresAnyOf** element.

If a system receives a resource containing control markings in ISM attributes that the system does not know how to process and/or that the system does not have listed in its UIAS.XML<sup>[70]</sup> **handlingControls** attribute, then the resource MUST immediately be rejected, and the system MUST follow [Section 2.3 - Potential Unauthorized Disclosure Data Spill Procedures](#).

If a system receives a resource that is protected with any NTK metadata that is not supported by that system, the resource MUST immediately be rejected, and the system MUST follow [Section 2.3 - Potential Unauthorized Disclosure Data Spill Procedures](#) if:

- The unsupported **ntk:Access Profile** is a member of **ntk:RequiresAllOf** or
- The unsupported **ntk:Access Profile** is a member of an **ntk:RequiresAnyOf** and there are only unsupported **ntk:Access Profile** elements as members of the **ntk:RequiresAnyOf**.

An access control decision uses all three elements as inputs to a function or series of functions to determine access.

## 2.2.1 - Guidance for systems processing data containing NTK metadata

It is important to note that data may have multiple access system requirements expressed (e.g., system A profile, system B profile, etc.). Each access system requirement is considered separately. Logical structures are used to describe situations where more than one access requirement is needed ("AND"), or where any one of multiple access requirements ("OR") is sufficient for access:

- The element **ntk:RequiresAllOf** indicates that all of the access requirements specified must be satisfied according to the specific NTK-related section of the ISM.ACES<sup>[47]</sup> in order to have access to the resource.
- The element **ntk:RequiresAnyOf** is used to indicate that any one of the access requirements must be satisfied according to the specific NTK-related section of the ISM.ACES<sup>[47]</sup> in order to have access to the resource.

These logical structures are used within the NTK structure with the following restrictions:

- The **ntk:Access** and **ntk:ExternalAccess** elements must contain either a **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** element as the first child element.
- A **ntk:RequiresAllOf** element may optionally have one **ntk:RequiresAnyOf** child element.
- A **ntk:RequiresAnyOf** element may not include any **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** elements as child elements.
- **ntk:RequiresAllOf** and **ntk:RequiresAnyOf** elements require at least one **ntk:AccessProfile** element as a child element. There may be one or more access elements, each with its own access policy.

Systems handling data containing NTK metadata MUST assess and understand the NTK metadata in order to protect data appropriately. Receiving systems MUST be able to interpret and be authorized for all NTK access profiles necessary to make an access control decision. The following cases detail requirements based on the NTK logic structure:

1. When a logic structure exists indicating all of the access profiles are mandatory, the receiving system MUST be able to interpret access profiles listed within this structure and be able to process access decisions in accordance with associated ISM.ACES<sup>[47]</sup> rules. If any NTK metadata is not processable by the system, the system MUST follow [Section 2.3 - Potential Unauthorized Disclosure Data Spill Procedures](#).
2. When a logic structure exists indicating at least one access profile is required, then the receiving system MUST be able to interpret access profiles listed within this structure and be able to process access decisions in accordance with associated ISM.ACES<sup>[47]</sup> rules. If no processable NTK metadata exists, the system MUST follow [Section 2.3 - Potential Unauthorized Disclosure Data Spill Procedures](#).

## 2.3 - Potential Unauthorized Disclosure Data Spill Procedures

If a resource has any unknown metadata required to be understood based on its logic structure, then there is the potential of a data spill. The following steps outline the required actions a system MUST take:

1. The files MUST be segregated and protected via the most restrictive manner available.
2. The cognizant Information Systems Security Manager (ISSM) MUST be contacted.

3. The submitter **MUST** be contacted to facilitate assessment of the potential spill.

## 2.4 - Additional Guidance

This section provides guidance for encoding data in specific situations. In particular, this section provides guidance for situations that do not have a single, obvious encoding solution. The content of this section will evolve over time as the maintainers of the DES identify new situations that need clarification. Implementers are encouraged to contact the maintainers of this DES for further guidance when necessary.

### 2.4.1 - Guidance for the ISM Segment

This section details guidance for the ISM segment of ISM.XML.

#### 2.4.1.1 - Document Compliance and Exemptions

Documents containing ISM attributes claim compliance with rule sets using the `@ism:compliesWith` attribute on the resource node of a document; `@ism:compliesWith` **MUST** be specified. This is a multi-valued attribute, and the acceptable values are U.S. Government ("**USGov**"), U.S. Intelligence Community ("**USIC**"), U.S. Department of Defense ("**USDOD**"), pure Controlled Unclassified Information (CUI) ("**USA-CUI-ONLY**"), U.S. CUI commingled with classified information ("**USA-CUI**"), and "**OtherAuthority**". These values are used to turn on rule sets for validation. Documents may assert compliance with multiple rule sets, and more rule sets may be added over time.

USGov	The minimum set of rules that United States of America (USA) produced documents must comply with. All documents that contain " <b>USA</b> " in the <code>@ism:ownerProducer</code> field of the resource node <b>MUST</b> contain " <b>USGov</b> " in <code>@ism:compliesWith</code> .
USIC	The rule set for documents that comply with United States (US) IC policies. Documents that assert " <b>USIC</b> " <b>MUST</b> assert " <b>USGov</b> ".
USDOD	The rule set for documents that comply with US Department of Defense (DOD) policies. Documents that assert " <b>USDOD</b> " <b>MUST</b> also assert " <b>USGov</b> ".
USA-CUI-ONLY	The rule set for documents that are Unclassified (U) and that comply with US policies for CUI. Documents that assert compliance with " <b>USA-CUI-ONLY</b> " <b>MUST NOT</b> assert any other value in <code>@ism:compliesWith</code> . This value of <code>@ism:compliesWith</code> is intended for environments that are exclusively CUI; i.e., the systems in the environment do not deal with any classified material or any classification markings, not even U. Documents that assert compliance with " <b>USA-CUI-ONLY</b> " <b>MUST NOT</b> include <code>@ism:classification</code> or <code>@ism:ownerProducer</code> .
USA-CUI	The rule set for documents that comply with US policies for CUI that are either commingled with Classified National Security Information (CNSI) data or that are CUI documents that contain " <b>(U)</b> " portion marks. CUI



documents that contain "(U)" portion marks will contain **@ism:classification** and therefore are not suited for **@ism:compliesWith = "USA-CUI-ONLY"**. Documents that assert compliance with **"USA-CUI"** MUST NOT assert **"USIC"** in **@ism:compliesWith**, because the IC has not implemented CUI at this time. Documents that assert compliance with **"USA-CUI"** MUST assert some other token in **@ism:compliesWith**.

**OtherAuthority** The rule set for documents that comply with policies not covered by **"USGov"**, **"USIC"**, or **"USDOD"**. Currently, there are no rules in the **"OtherAuthority"** category, but this may change over time. **"OtherAuthority"** provides a mechanism to turn off most ISM rules for documents that were produced by non-USA entities.

A USIC document may claim exemption from mandatory Foreign Disclosure & Release (FD&R) (ICD 710<sup>[39]</sup>), and a USDOD document may claim exemption from DOD Instruction 5230.24 *Distribution Statements on Technical Documents* <sup>[16]</sup> using **@ism:exemptFrom** on the resource node. The acceptable values are **"IC\_710\_MANDATORY\_FDR"** and **"DOD\_DISTRO\_STATEMENT"**.

## 2.4.1.2 - Physical XML Attribute Groups

The ISM schema in ISM.XML defines several attribute groups. These attribute groups are intended to be referenced by other DESs (e.g., *XML Data Encoding Specification for Information Resource Metadata* (IRM.XML<sup>[46]</sup>) or *XML Data Encoding Specification for Intelligence Publications* (PUBS.XML<sup>[66]</sup>) to incorporate the information security marking attributes as needed.

- **ism:SecurityAttributesOptionGroup** lists all of the attributes as optional. It is intended for use on elements such as "Sections" where marking of the classification of a section may be optional.
- **ism:SecurityAttributesGroup** lists the attributes **@ism:classification** and **@ism:ownerProducer** as required. It is the "normal" group to apply to a portion or resource mark element where classification is required.
- **ism:ResourceNodeAttributeGroup** is used on the resource node of an implementing schema and includes **ism:SecurityAttributesGroup**. The resource node is the element in an implementing schema that represents the security attributes for the entire resource, and is used to generate the "banner" mark for the resource. The resource node also specifies the rule sets the resource is claiming compliance with such as ICD 710<sup>[39]</sup>.
- **ism:ISMRootNodeAttributeGroup** is used on the root node of the implementing schema to ensure the DES version is specified.
- **ism:NoticeAttributesGroup** is used on an element designed to contain a warning or notice and which requires portion marking. It references the attributes necessary to record the portion mark as well as those necessary to record the details of the notice.
- **ism:NoticeAttributesOptionGroup** is used on an element designed to contain a warning or notice and which permit, but does not require portion marking. It references the attributes necessary to record the portion mark as well as those to record the details of the notice.

- **ism:POCAttributeGroup** is used on an element designed to contain a name and/or contact method for one of the various point-of-contact requirements in a document. It is used to indicate that the text or sub-elements of the parent element contain the contact information for the type of point-of-contact specified in the **@ism:pocType** attribute.

The attribute **@ism:excludeFromRollup** is not a part of any group, but should be added to any element in an implementing schema that may require the element's attributes to be excluded from roll-up logic that would otherwise impact the resource security element. A classic example of this would be a bibliographic source citation where the desire is to indicate that the classification of the referenced source is Top Secret (TS) even though the data extracted was U and the document with the source citation is U.

### 2.4.1.3 - Notices

The **ism:ISMNoticeAttributeGroup** can be used on an element to signify that it contains notice information concerning a "well-defined" security notice such as the notices related to IC markings RD, FRD, IMCON, and FISA. To include security markings on these notices, the **ism:NoticeAttributesGroup** and the **ism:NoticeAttributesOptionGroup** contain all of the attributes in the **ism:ISMNoticeAttributeGroup** as well as the security marking attributes defined in the **ism:SecurityAttributesGroup** and the **ism:SecurityAttributesOptionGroup**, respectively. The **ism:ISMNoticeAttributeGroup** is comprised of the following attributes:

- The attribute **@ism:noticeType** is an indicator that the element contains a security-related notice and is used to categorize which of the required notices is specified in the element. These categories include those described in the IC Markings<sup>[28]</sup> as well as additional well-defined and formally recognized security notice types described in other directives, such as **"US-Person"** and DoD Distribution values. The permissible values for this attribute are defined in the Controlled Vocabulary Enumeration (CVE) "CVEnumISMNotice" in ISM.XML.
- The attribute **@ism:noticeProseID** is an indicator that can be used to identify a security-related notice in an out-of-band fashion without actually having the notice text in the record but rather a notice text prose identifier. This prose identifier maps to the notice text which is stored in CVE "CVEnumISMNoticeProse" in ISM.XML. Note that not all notices can be supported out-of-band since some notices (i.e. DoD-Dist-B) require variable input (e.g., reason, date of determination, and controlling DoD office) or do not have standardized words.
- The attribute **@ism:noticeDate** specifies the date associated with the notice, such as the date it was issued.
- The attribute **@ism:noticeReason** specifies the reason a notice was issued.
- The attribute **@ism:unregisteredNoticeType** is used to represent notices that are not categorized according to the IC Markings<sup>[28]</sup> and/or notices with values that do not appear in the CVE "CVEnumISMNotice" in ISM.XML. This attribute can be used to designate specification-specific security notices that may not be sufficiently defined to be recognized by Security Markings Program (SMP).

ISM.XML provides constraint checking for the **@ism:noticeType** attribute, requiring that there be a match between notices used and portions requiring notices. For example, a **"FISA"** notice

without any FISA portions or vice versa will result in an error or warning, depending on the particular notice.

In addition to the notice attribute groups, the ISM schema in ISM.XML includes elements that can represent a set of notices. The element **ism:NoticeList** is comprised of one or more **ism:Notice** elements, which use the **ism:NoticeAttributesGroup** to provide additional information about each notice. The actual contents of a notice message is contained within the **ism:Notice** sub-element **ism:NoticeText**. The **ism:POCAttributeGroup** included on **ism:NoticeText** is used to specify the Point of Contact (POC) associated with the notice, such as the DoD Distribution POC. These elements have been provided for convenience, but an implementing schema could use any of the aforementioned attribute groups on an element defined outside of ISM.XML to benefit from the constraint checking that ISM.XML provides.

An implementing schema could use the same element to capture both the notices codified using this attribute as well as other notices, warnings, notes, etc. It is a best practice to limit the content of a single element, used for notice information, to a single type of notice. For example, if a document is to contain both a FISA notice and notice about languages used, two separate elements should be used, one with an **@ism:noticeType** attribute with a value of **"FISA"** and one with the **@ism:unregisteredNoticeType** attribute with some appropriate string value, such as **"Language"**.

Applying the **@ism:noticeType** attribute does not remove the obligation to put the appropriate required text in the **ism:Notice** element. For example, only placing the **@ism:noticeType** attribute with the value of **"RD"**, without including **"RD"** warning text in **ism:NoticeText**, would not constitute a valid RD notice.

DoD Distribution statements are slightly more complex; a single document may have multiple DoD Distribution statements embedded, but may have only one that applies to the whole document. Therefore the appropriate attributes **MUST** be applied to the Resource Security Element for the document.

### 2.4.1.3.1 - US-Person

The value **"US-Person"** in the **@ism:noticeType** supports the requirements of several agencies for notices associated with US-Person information. The inclusion of this value provides a standard implementation for all producing agencies.

### 2.4.1.3.2 - Point Of Contact Requirements

For documents containing certain types of data or claiming compliance with specific directives, a point-of-contact to whom questions about the document can be directed may be applied. The **ism:Notice** elements can be used to fulfill these requirements by using the **@ism:noticeType** value of **"POC"** to indicate that the contents of a **ism:Notice** are used to provide contact information. The **@ism:pocType** attribute indicates that the text of the **ism:NoticeText** element specifies the IC element point-of-contact and contact instructions to expedite decisions on information sharing, while specifying which type(s) of information that contact should handle.

### 2.4.1.3.3 - pre13526ORCON

E.O. 13526<sup>[24]</sup>, Section 4.1(i) provides guidance on the dissemination of classified information which the originating agency has determined requires prior authorization before further dissemination by a recipient organization (i.e., ORCON information). According to E.O. 13526<sup>[24]</sup>, classified ORCON documents created prior to the effective date of the order 25 June 2010 should be handled according to E.O. 12958, *Classified National Security Information, as Amended* <sup>[23]</sup>, and documents created after this date should be handled according to E.O. 13526<sup>[24]</sup>. However, derived products that include ORCON data produced prior to 25 June 2010 MUST include a statement that it should be handled according to the previous E.O. 12958<sup>[23]</sup>, as amended, and this statement MUST be marked with the `@ism:noticeType` attribute value **"pre13526ORCON"**. The attribute indicates that the document contains ORCON information that predates E.O. 13526<sup>[24]</sup>, and the text of the `ism:NoticeText` element should contain prose describing the correct handling of the data based on pre-13526 rules.

Example:

```
<Notice noticeType="pre13526ORCON" classification="U" ownerProducer="USA">
  <NoticeText classification="U" ownerProducer="USA">This document
    is derived from AgencyX asset HSJ-3472 and should be
    handled according to the rules outlined in E.O. 12958
    as amended. For questions, contact John Smith, AgencyX,
    888-555-5555, jsmith@agencyx.gov.</NoticeText>
</Notice>
```

### 2.4.1.3.4 - CVEnumISMNoticeProse Value Numbering Convention

The following is the numbering convention for the notice prose token values in CVE "CVEnumISMNoticeProse". If the notice prose changes for a notice (ie. ITAR-EAR\_00001), a new notice prose value (ie. ITAR-EAR\_00002) would be created to map to the new notice prose and the old notice value and prose would be retained and updated with a @deprecated date.

**Table 3 - CVEnumISMNoticeProse Value Numbering Convention**

Value Numbering Suffix	Classification Level
00001 to 09999	Reserved for Unclassified Notice Text
10001 to 19999	Reserved for Unclassified but For Official Use Only (FOUO) Notice Text
20001 to 20999	Reserved for Notice Text classified at the "Secret//REL USA, FVEY" level
21001 to 21999	Reserved for Notice Textclassified at the "Secret//NF" level
22001 to 29999	Reserved for Notice Text classified at the "Secret//TBD" level

Value Numbering Suffix	Classification Level
30001 and above	Reserved for Notice Text classified with other classifications

### 2.4.1.4 - Originator Controlled Assets

There are two dissemination control markings for use on Originator Controlled (OC) data. These markings are "OC" and "OC-USGOV". The "OC" marking does not have originator pre-approval for further dissemination, rather it requires a list of organizations approved for dissemination. Without the list of organizations, automated access control systems are unable to make access decisions. To prevent this issue, a list of approved organizations to which the data may be disseminated MUST be specified. This is accomplished through use of the OC NTK profile, which provides a defined structure for indicating the approved for dissemination agencies and organizations.

Data marked "OC-USGOV" may include in its OC NTK a list of approved organizations to which the data may be disseminated (not including pre-approvals), and, by definition, always has a pre-approval distribution list to Executive Branch departments and agencies. It also may include distribution of Disseminated Analytic Products to appropriate Congressional Oversight Committees as determined by the Office of Legislative Affairs (OLA) of each agency in possession of the data. This includes the OLA of the creating agency as well as the OLAs of agencies that receive the data.

### 2.4.1.5 - Section and Portion Style Marking Limitations

There are limitations to consider specific to the ISM segment of ISM.XML that are not necessarily policy driven in the automation of section and portion style markings. For clarification, the concepts are defined as such:

- **Section** - An optional, generic, and flexible subdivision of a document that when used requires a Section Banner and portion markings. Examples include: table, document chapter, or section.
- **Portion** - A piece of information that has a human-perceived, distinct, and separate existence from other pieces of information. Examples include: text paragraph, bulleted list item, or table cell.

ISM.XML Schematron cannot determine the difference between a **Section** and a **Portion** marked with ISM attributes, and as such cannot and does not enforce the roll up rules of all **Portions** in a **Section** to the markings of the **Section**. Proper enforcement of roll up in this case is left as an exercise for the user.

The ISM.XML schematron rules assume that the XML instance document under verification is a standalone document with respect to E.O. 13526<sup>[24]</sup>, ICD 710<sup>[39]</sup> and the IC Markings<sup>[28]</sup>. However, in some cases, the XML instance document under validation is really just a portion of a larger data set (e.g., a small block of metadata embedded within a National Imagery Transmission Format (NITF) file or an HDF5 file), where ISM.XML is used to provide the security markings for that portion while the rest of the data is portion marked with some other mechanism or falls under

an ISOO portion marking waiver. In those cases, the Schematron requirement that the embedded XML block contain portion marks may result in unnecessary portion marking.

In this case where the XML instance document is indeed a valid portion of the full document, data providers may use Phases (see [Chapter 6 - Progressive Validation Using Phases](#)) to tailor validation to this use case. Data providers will want to run ISM validation on documents that are only portions by running only the Phases PORTION, VALUECHECK, TYPECHECK, and STRUCTURECHECK. Data providers will not want to run the validation phases of BANNER, ROLLUP or ROLLDOWN on documents that are only portions.

While it may seem attractive to simply place security marking attributes on the first element within the root, thus satisfying the Schematron rule that the document contain at least one portion mark, this option is strongly discouraged; data consumers might view the document as ambiguously portion marked and then either reject the file or mishandle the unmarked elements.

### 2.4.1.6 - ISM Schema Types

The ISM schema defines various simple and complex types for use by other specifications as well as within ISM itself. The following tables separate the types by whether they are simple or complex types. The primary difference between simple and complex types is that simple types simply define the format constraints of a value field (i.e. cannot have attributes) while complex types can define entirely other containers or structures. For the ISM schema, the complex types are used primarily to add ISM attributes in addition to the basic value field simple type.

**Table 4 - ISM Schema Simple Types**

Name	Type
ism:LongStringType	xsd:string maxLength 32000
ism:ShortStringType	xsd:string maxLength 256

**Table 5 - ISM Schema Complex Types**

Name	Type	Attributes
ism:LongStringWithSecurityType	xsd:string maxLength 32000	<a href="#">SecurityAttributesGroup</a>
ism:ShortStringWithSecurityType	xsd:string maxLength 256	<a href="#">SecurityAttributesGroup</a>

### 2.4.1.7 - ISM Schema Attributes

The table in this section details the types and descriptions of attributes defined within the ISM schema.

**Table 6 - ISM Schema Attributes**

Attribute	Type	Description
<b>@ism:atomicEnergyMarkings</b>	xsd:token	Applicable atomic energy information markings for a document or portion.
<b>@ism:classification</b>	xsd:token	The highest level of classification applicable to the containing document or portion.
<b>@ism:classificationReason</b>	xsd:string maxLength 4096	One or more reason indicators or explanatory text describing the basis for an original classification decision (used primarily at the document level).  This attribute corresponds to the “reason” line of a document’s classification authority block, and it is only used, and only allowed, when classification is the result of an original classification decision.
<b>@ism:classifiedBy</b>	xsd:string maxLength 1024	The identity, by name or personal identifier and position title, of the original classification authority for a document (used primarily at the resource level).
<b>@ism:compilationReason</b>	xsd:string maxLength 1024	The reason that the classification of the document is more restrictive than the simple roll-up of the marked portions of the document.  This attribute is an indicator that there is not accidental over-classification of the document. Users must exercise special care beyond that indicated by the portion marks when using this information.
<b>@ism:compliesWith</b>	xsd:token	The ISM.XML rule sets a document complies with.



Attribute	Type	Description
<b>@ism:createDate</b>	xsd:date	<p>The date when ISM.XML metadata was added or updated.</p> <p>This date is used by some constraint rules to determine if ISM.XML markings are valid. For example, this date is used to check deprecation of some marks.</p>
<b>@ism:cuiBasic</b>	xsd:token	The set of CUI Basic Category markings for a document or portion.
<b>@ism:cuiControlledBy</b>	xsd:string	<p>The identity, by name or personal identifier and position title, of the CUI controlling authority for a document containing CUI information.</p> <p>This attribute corresponds to the 32 CFR Parts 2002 <i>Controlled Unclassified; Final Rule</i> <a href="#">[53]</a> paragraph 20(d) requirement that all documents containing CUI must carry an indicator of who designated the CUI within it.</p>
<b>@ism:cuiControlledByOffice</b>	xsd:string	<p>Office in an agency or department that is responsible for labeling and controlling information as CUI.</p> <p>This attribute corresponds to the <i>DoD Instruction 5200.48</i> <a href="#">[20]</a> paragraph 3.4(f)(2) requirement that all documents containing CUI must have a control block where the second line identifies the office making the CUI determination.</p>



Attribute	Type	Description
<b>@ism:cuiDecontrolDate</b>	xsd:date	<p>The specific date when a CUI resource is subject to automatic CUI decontrol procedures.</p> <p>This attribute corresponds to the 32 CFR Parts 2002<i>Controlled Unclassified; Final Rule</i> <a href="#">[53]</a> paragraph 20(e) requirement that, where feasible, designating agencies must include a specific decontrolling date or event with all CUI.</p>
<b>@ism:cuiDecontrolEvent</b>	xsd:string	<p>The specific event when a CUI resource is subject to automatic CUI decontrol procedures.</p> <p>This attribute corresponds to the 32 CFR Parts 2002<i>Controlled Unclassified; Final Rule</i> <a href="#">[53]</a> paragraph 20(e) requirement that, where feasible, designating agencies must include a specific decontrolling date or event with all CUI.</p>
<b>@ism:cuiPOC</b>	xsd:string	<p>Phone number or office mailbox for the originating DoD Component or authorized CUIholder.</p> <p>This attribute corresponds to the <i>DoD Instruction 5200.48</i> <a href="#">[20]</a> paragraph 3.4(f)(5) requirement that all documents containing CUI must have a control block where the fifth line identifies the CUI Point of Contact.</p>
<b>@ism:cuiSpecified</b>	xsd:token	The set of CUI Specified Category markings for a document or portion.

Attribute	Type	Description
<b>@ism:declassDate</b>	xsd:date	The specific date when the resource is subject to automatic declassification procedures if not properly exempted from automatic declassification (used primarily at the document level).
<b>@ism:declassEvent</b>	xsd:string maxLength 1024	A description of an event upon which the information shall be subject to automatic declassification procedures if not properly exempted from automatic declassification (used primarily at the document level).
<b>@ism:declassException</b>	xsd:token	<p>The exemption from automatic declassification that is claimed for a document (used primarily at the document level).</p> <p>This element is used in conjunction with the Declassification Date or Declassification Event, and it corresponds to the “Declassify On” line of a resource’s classification authority block.</p>
<b>@ism:derivativelyClassifiedBy</b>	xsd:string maxLength 1024	<p>The identity, by name or personal identifier, of the derivative classification authority (used primarily at the document level).</p> <p>This attribute corresponds to the “Classified By” line of a resource’s classification authority block.</p>

Attribute	Type	Description
@ism:derivedFrom	xsd:string maxLength 1024	<p>A citation of the authoritative source or sources of the classification markings used in a derivative classification decision for a classified document.</p> <p>This attribute corresponds to the “Derived From” line of a document’s classification authority block. ISOO guidance is:</p> <p>Source of derivative classification. (1) The derivative classifier shall concisely identify the source document or the classification guide on the “Derived From” line, including the agency and, where available, the office of origin, and the date of the source or guide.</p>

Attribute	Type	Description
<b>@ism:DESVersion</b>	xsd:string conforming to regular expression:  [0-9]{6}(\.[0-9]{6})?(\-{1,23})?	<p>The version number of the specification. This attribute is intended for processing systems to determine the appropriate versions of Schema, Schematron, and CVE values for validation and interpretation of an instance document.</p> <p>If there are multiple of this attribute specified in an instance document, the first one in document order is the one that will apply to the entire document. Document order is defined in <a href="https://www.w3.org/TR/xpath-datamodel/#document-order">https://www.w3.org/TR/xpath-datamodel/#document-order</a>.</p>
<b>@ism:displayOnlyTo</b>	xsd:token	<p>The set of countries and/or international organizations associated with a “Display Only To” marking.</p> <p>The “Display Only To” marking indicates that a document is authorized for foreign viewing by appropriate affiliates of approved countries and/or international organizations <b>without</b> providing the foreign recipient with a copy for retention in any medium (physical or electronic).</p>
<b>@ism:disseminationControls</b>	xsd:token	Applicable dissemination control markings for a document or portion.

Attribute	Type	Description
<b>@ism:excludeFromRollup</b>	xsd:boolean	<p>An indicator that an element's ISM attributes do not contribute to the "rollup" classification of the document (used at the portion level).</p> <p><b>@ism:excludeFromRollup</b> is most often used when providing the security attributes of a referenced or linked-to resource. This attribute provides a mechanism to assert a more-restrictive classification of a resource pointed to by a link or reference without impacting the document's resource markings.</p>
<b>@ism:exemptFrom</b>	xsd:token	<p>Specific exemptions within a rule set that are claimed for a document.</p> <p>This attribute is used on the resource node of a document in conjunction with <b>@ism:compliesWith</b>.</p>
<b>@ism:externalNotice</b>	xsd:boolean	<p>An indicator that an element contains a security-related notice for information NOT contained in document.</p> <p>This flag allows for a notice to exist in a document without the data that would normally require the notice. For example, a document could contain a FISA notice without FISA data present. Source citations are a common use case for this attribute.</p>

Attribute	Type	Description
@ism:FGISourceOpen	xsd:token	<p>The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information is not concealed.</p> <p>FGI markings protect foreign-owned or foreign-produced information and are applied based on sharing agreements or arrangements with the source country or organization.</p>

Attribute	Type	Description
<b>@ism:FGISourceProtected</b>	xsd:token	<p>The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information must be concealed.</p> <p>This attribute has specific rules concerning its usage:</p> <p><b>PROTECTED SPACES —</b> Within protected internal organizational spaces, this attribute may be used to maintain a formal record of the foreign country or countries and/or registered international organization(s) that are the non-disclosable owner(s) and/or producer(s) of information which is categorized as foreign government information according to Security Markings Program guidelines. If the data element is employed in this manner, then additional measures must be taken prior to dissemination of the resource to shared spaces so that any indications of the non-disclosable owner(s) and/or producer(s) of information within the resource are eliminated. In all cases, the corresponding portion marking or banner marking should be compliant with Security Markings Program guidelines for FGI when the source must be concealed. In other words, even if the data element is being employed within protected internal organizational spaces to maintain a formal record of the non-disclosable owner(s)</p>

Attribute	Type	Description
		<p>and/or producer(s) within an XML resource, if the resource is rendered for display within the protected internal organizational spaces in any format by a stylesheet or as a result of any other transformation process, then the non-disclosable owner(s) and/or producer(s) should not be included in the corresponding portion marking or banner marking.</p> <p>SHARED SPACES — Within shared spaces, the data element serves only to indicate the presence of FGI; in this case, this element's value will always be "FGI". The data element may also be employed in this manner within protected internal organizational spaces.</p>
<b>@ism:hasApproximateMarkings</b>	xsd:boolean	When true, indicates the ISM markings specified are estimated (e.g., system high).
<b>@ism:handleViaChannels</b>	xsd:string	Handle VIA Channels that may appear in the second banner line.
<b>@ism:highWaterNATO</b>	xsd:string	This attribute is rendered in portion marks and banners. The permissible values for this attribute are defined in the ISM HighWater NATO CVE.
<b>@ism:ISMATCESVersion</b>	xsd:string conforming to regular expression: [0-9]{6}(\.[0-9]{6})?(\-{1,23})?	<p>The version number of the ISMCAT.CES<sup>[49]</sup> used in the document.</p> <p>If there are multiple <b>@ism:ISMATCESVersion</b> attributes specified in an instance document, the first one in document order is the one that will apply to the entire document.</p>



Attribute	Type	Description
<b>@ism:joint</b>	xsd:boolean	When true, an indicator that entities in the <b>@ism:ownerProducer</b> attribute are JOINT owners of the data.
<b>@ism:noAggregation</b>	xsd:boolean	When true, an indicator that there is no classification by compilation across any combination of portions extracted from the document.
<b>@ism:nonICMarkings</b>	xsd:token	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-intelligence components.  This attribute is rendered in portion marks and security banners.
<b>@ism:nonUSControls</b>	xsd:token	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-US components (foreign government or international organization).  This attribute is rendered in portion marks and security banners.
<b>@ism:noticeDate</b>	xsd:date	A date associated with a notice (for example, the DoD Distribution notice date).
<b>@ism:noticeProseID</b>	xsd:token	An indicator that can be used to identify a security-related notice in an out-of-band fashion without actually having the notice text in the record but rather a notice text prose identifier. This prose identifier maps to the notice text stored in CVE "CVEnum-ISMNoticeProse".

Attribute	Type	Description
<b>@ism:noticeReason</b>	xsd:string maxLength 2048	A reason associated with a notice (for example, the DoD Distribution reason).
<b>@ism:noticeType</b>	xsd:token	An indicator that the containing element contains a security-related notice. This attribute is used to categorize which of the required notices is specified in the element. These categories include those described in the IC Markings <sup>[28]</sup> , as well as additional well-defined and formally recognized security notice types described in other directives, such as US-Person and DoD Distribution.
<b>@ism:ownerProducer</b>	xsd:token	<p>The set of national governments and/or international organizations that have purview over the containing classification marking.</p> <p>This element is always used in conjunction with the <b>@ism:classification</b> attribute. Taken together, the two elements specify the classification category (TS, S, C, R, or U) and the type of classification (US, non-US, or Joint).</p> <p>The attribute value may be rendered in portion marks or security banners.</p>
<b>@ism:pocType</b>	xsd:token	<p>The type of a point of contact.</p> <p>This attribute is used to associate POC with the reason the POC is listed. For example, the POC for ICD 710<sup>[39]</sup> purposes would have the <b>@ism:pocType</b> value of "ICD-710".</p>

Attribute	Type	Description
<b>@ism:releasableTo</b>	xsd:token	<p>The set of countries and/or coalitions associated with a "Releasable To" marking.</p> <p>This is an explicit foreign disclosure and release marking to indicate the originator has determined that the information is releasable or has been released to the countries and/or international organizations indicated through established foreign disclosure procedures and channels. The document is not releasable to any foreign country or international organization not indicated in the REL TO marking.</p>
<b>@ism:resourceElement</b>	xsd:boolean	<p>Indicator that the associated ISM attributes represent the classification of the entire document.</p> <p>Every document must have at least one element with <b>@ism:resourceElement="true"</b>.</p> <p>It should be rare for a document to have more than one <b>@ism:resourceElement</b> attribute. This may occur in some aggregation schemas. In the case of aggregation, the first attribute in XML document order is the one used for all constraint rules. The first attribute in document order is the one that would satisfy the following XPath 2<sup>[72]</sup> path <code>// @ism:resourceElement[1]</code>.</p>
<b>@ism:SARIdentifier</b>	xsd:token	The set of applicable SAR identifiers for the containing document or portion.

Attribute	Type	Description
@ism:SCIcontrols	xsd:token	The set of applicable SCI controls for the containing document or portion.
@ism:secondBannerLine	xsd:token	Tokens that contain markings used to support administrative and legal processes for handling and protecting documents. When they appear in a document, these tokens form a second line that is placed below the banner.
@ism:unregisteredNoticeType	xsd:string maxLength 2048	A notice that is of a category not described in the IC Markings <sup>[28]</sup> and/or is not sufficiently defined to be represented in the CVE “CVCEnumISMNotice”.  This attribute can be used by specifications that import ISM.XML to represent a wider variety of security-related notices.

### 2.4.1.8 - ISM Schema Attribute Groups

There are several attribute groups that should be used when importing the ISM schema into other XML schemas to help reduce the effects of changes to the ISM schema (i.e. the addition of a new attribute), as these groups cover the main concepts of ISM and are updated as needed as attributes change.

**Table 7 - ism:ISMNoticeBaseAttributeGroup**

Attribute	Required
@ism:noticeType	Not Required
@ism:noticeProseID	Not Required
@ism:noticeReason	Not Required
@ism:noticeDate	Not Required
@ism:unregisteredNoticeType	Not Required

**Table 8 - ism:ISMNoticeAttributeGroup**

Attribute	Required
<a href="#">ism:ISMNoticeBaseAttributeGroup</a>	Not Required

Attribute	Required
@ism:externalNotice	Not Required

**Table 9 - ism:ISMNoticeExternalAttributeGroup**

Attribute	Required
<a href="#">ism:ISMNoticeBaseAttributeGroup</a>	Not Required
@ism:externalNotice	Required

**Table 10 - ism:ISMResourceAttributeGroup**

Attribute	Required
@ism:resourceElement	Required
@ism:compliesWith	Required
@ism:createDate	Required
@ism:exemptFrom	Not Required
@ism:noAggregation	Not Required

**Table 11 - ism:ISMResourceAttributeOptionGroup**

Attribute	Required
@ism:resourceElement	Not Required
@ism:compliesWith	Not Required
@ism:createDate	Not Required
@ism:exemptFrom	Not Required
@ism:noAggregation	Not Required

**Table 12 - ism:ISMRootNodeAttributeGroup**

Attribute	Required
@ism:DESVersion	Required
@ism:ISMCATCESVersion	Required

**Table 13 - ism:ISMRootNodeAttributeOptionGroup**

Attribute	Required
@ism:DESVersion	Not Required
@ism:ISMCATCESVersion	Not Required

**Table 14 - ism:NoticeAttributesGroup**

Attribute	Required
<a href="#">ism:ISMNoticeAttributeGroup</a>	Not Required
<a href="#">ism:SecurityAttributesGroup</a>	Not Required

**Table 15 - ism:NoticeAttributesOptionGroup**

Attribute	Required
<a href="#">ism:ISMNoticeAttributeGroup</a>	Not Required
<a href="#">ism:SecurityAttributesOptionGroup</a>	Not Required

**Table 16 - ism:NoticeExternalAttributesGroup**

Attribute	Required
<a href="#">ism:ISMNoticeExternalAttributeGroup</a>	Not Required
<a href="#">ism:SecurityAttributesGroup</a>	Not Required

**Table 17 - ism:NoticeExternalAttributesOptionGroup**

Attribute	Required
<a href="#">ism:ISMNoticeExternalAttributeGroup</a>	Not Required
<a href="#">ism:SecurityAttributesOptionGroup</a>	Not Required

**Table 18 - ism:POCAttributeGroup**

Attribute	Required
@ism:pocType	Not Required

**Table 19 - ism:ResourceNodeAttributeGroup**

Attribute	Required
<a href="#">ism:ISMResourceAttributeGroup</a>	Not Required
<a href="#">ism:SecurityAttributesGroup</a>	Not Required
<a href="#">ism:ISMNoticeAttributeGroup</a>	Not Required

**Table 20 - ism:ResourceNodeAttributeOptionGroup**

Attribute	Required
<a href="#">ism:ISMResourceAttributeOptionGroup</a>	Not Required
<a href="#">ism:SecurityAttributesOptionGroup</a>	Not Required
<a href="#">ism:ISMNoticeAttributeGroup</a>	Not Required

**Table 21 - ism:SecurityAttributesGroup**

<b>Attribute</b>	<b>Required</b>
@ism:classification	Required
@ism:ownerProducer	Required
@ism:joint	Not Required
@ism:SCIcontrols	Not Required
@ism:SARIdentifier	Not Required
@ism:atomicEnergyMarkings	Not Required
@ism:disseminationControls	Not Required
@ism:displayOnlyTo	Not Required
@ism:FGISourceOpen	Not Required
@ism:FGISourceProtected	Not Required
@ism:releasableTo	Not Required
@ism:nonICMarkings	Not Required
@ism:classifiedBy	Not Required
@ism:compilationReason	Not Required
@ism:derivativelyClassifiedBy	Not Required
@ism:classificationReason	Not Required
@ism:nonUSControls	Not Required
@ism:derivedFrom	Not Required
@ism:declassDate	Not Required
@ism:declassEvent	Not Required
@ism:declassException	Not Required
@ism:hasApproximateMarkings	Not Required
@ism:cuiBasic	Not Required
@ism:cuiControlledBy	Not Required
@ism:cuiControlledByOffice	Not Required
@ism:cuiDecontrolDate	Not Required
@ism:cuiDecontrolEvent	Not Required
@ism:cuiPOC	Not Required
@ism:cuiSpecified	Not Required
@ism:secondBannerLine	Not Required
@ism:handleViaChannels	Not Required
@ism:highWaterNATO	Not Required

**Table 22 - ism:SecurityAttributesOptionGroup**

<b>Attribute</b>	<b>Required</b>
@ism:classification	Not Required
@ism:ownerProducer	Not Required
@ism:joint	Not Required
@ism:SCIcontrols	Not Required
@ism:SARIdentifier	Not Required
@ism:atomicEnergyMarkings	Not Required
@ism:disseminationControls	Not Required
@ism:displayOnlyTo	Not Required
@ism:FGISourceOpen	Not Required
@ism:FGISourceProtected	Not Required
@ism:releasableTo	Not Required
@ism:nonICMarkings	Not Required
@ism:classifiedBy	Not Required
@ism:compilationReason	Not Required
@ism:derivativelyClassifiedBy	Not Required
@ism:classificationReason	Not Required
@ism:nonUSControls	Not Required
@ism:derivedFrom	Not Required
@ism:declassDate	Not Required
@ism:declassEvent	Not Required
@ism:declassException	Not Required
@ism:hasApproximateMarkings	Not Required
@ism:cuiBasic	Not Required
@ism:cuiControlledBy	Not Required
@ism:cuiControlledByOffice	Not Required
@ism:cuiDecontrolDate	Not Required
@ism:cuiDecontrolEvent	Not Required
@ism:cuiPOC	Not Required
@ism:cuiSpecified	Not Required
@ism:secondBannerLine	Not Required
@ism:handleViaChannels	Not Required
@ism:highWaterNATO	Not Required



## 2.4.1.9 - Use of ISM for SAP Accesses

This release of ISM incorporates DOD Special Access Program Control Office (SAPCO) guidance on how accesses to Special Access Program (SAP)s are handled (*Special Access Program (SAP) Security Manual: Marking (Vol 4)* [\[21\]](#)). This section documents SAPCO guidance and contrasts it with differing guidance in the IC Markings [\[28\]](#). Efforts are underway to reconcile differing guidance documents, but these efforts are not yet completed. This release of ISM adheres to multiple, differing guidance documents on SAPs in order to support multiple customers. This release of ISM adapts handling of SAPs based on the owner of a SAP and on whether data's ISM metadata indicates `@ism:compliesWith` contains "USIC", "USDOD", or both.

In the discussion below, hypothetical SAP markings are used for illustration. Following the IC Markings [\[28\]](#) section on SAPs, the hypothetical SAP BUTTER POPCORN and other hypothetical SAP markings are used for illustration.

### 2.4.1.9.1 - Classification-based Read-ons for DoD SAPs

The IC Markings [\[28\]](#), indicates that users are granted a single access level for each SAP. Information from DOD's SAPCO indicates that, for SAP's owned by DOD and possibly some SAPs owned by other agencies, SAP read-ons are granted at different classification levels. A user who is granted TS access to a SAP is authorized to see information classified at the TS level or below for that SAP. In contrast, a user who is granted SECRET access to a SAP is authorized to see information classified only at the SECRET or CONFIDENTIAL levels for that SAP.

The classification banner for a resource that contains SAP data does not explicitly identify the classification level read-on required to access the resource's SAP data. For example, if there is a hypothetical DOD SAP STORMY\_PETREL that requires different read-ons at different classification levels, then a document marked TOP SECRET//SAR-STORMY\_PETREL may contain STORMY\_PETREL data that is at the TS level, or alternatively it may contain STORMY\_PETREL data that only requires a SECRET or even CONFIDENTIAL read-on to STORMY\_PETREL. The banner in both cases is the same, and therefore does not provide sufficient information to determine whether a user needs a TOP SECRET read-on to STORMY\_PETREL, a SECRET read-on to STORMY\_PETREL, or just a CONFIDENTIAL read-on to STORMY\_PETREL.

EO 13526, *Executive Order 13526 – Classified National Security Information* [\[24\]](#), Section 4.3, states:

(a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program.

Since creation of SAPs is owned by several different agencies, there may not always be deconfliction of SAP markings across agencies. It is therefore important to retain metadata information about the owner of a SAP in data that is marked with one or more SAPs, especially to support automated access control.

To address these challenges, SAP values in the ISM controlled vocabulary for SAP markings in `@SARIdentifier` ("CVEnumISMSAR") identify, in the following order:

1. Initial characters of 'SAR-'
2. The agency that owns the SAP
3. (Optional) The required classification read-on level for the SAP data, for SAPs that have different read-ons for different classification levels
4. The SAP marking value.

The owning agency, any required classification read-on level, and marking value are separated by colons (:).

In addition, since some SAP markings contain spaces (e.g., a hypothetical Director of National Intelligence (DNI) SAP BUTTER POPCORN), the value in `@SARIdentifier` replaces a space with an underscore and becomes `"SAR-DNI:BUTTER_POPCORN"`. Finally, SAP markings may contain underscores; in these markings, the underscores will be duplicated in the ISM controlled vocabulary entry for `@SARIdentifier` (e.g., a `@SARIdentifier` attribute value containing `"SAR-DOD:S:STORMY__PETREL"` for a DOD SAP marking of STORMY\_PETREL). Here are some **hypothetical** tokens that may appear in `@SARIdentifier`:

- `"SAR-DNI:BUTTER_POPCORN"`
- `"SAR-DOD:TS:STORMY__PETREL"`
- `"SAR-DOD:S:STORMY__PETREL"`
- `"SAR-DOD:C:STORMY__PETREL"`
- `"SAR-DOD:TS:DEMOSAP1"`
- `"SAR-DOD:S:DEMOSAP1"`
- `"SAR-DOD:C:DEMOSAP1"`.

## 2.4.1.9.2 - Rendering SAPs in Classification Banners and Portion Marks

The owning agency and required classification read-on level in `@SARIdentifier` are to be used in metadata only, not in rendered classification banners or portion marks. Therefore, the ISM rendering stylesheets strip the owning agency and any classification level from the `@SARIdentifier` value before rendering. For example, for hypothetical `@SARIdentifier="SAR-DOD:S:DEMOSAP1"`, the rendered SAP portion of the classification banner would be SAR-DEMOSAP1.

For SAPs that have different read-ons for different classification levels, there may be different portions in a document that are marked with the SAP but at different classification levels. For example, a document could have two portions, one with a hypothetical DOD `"SAR-DOD:S:DEMOSAP1"` and a second paragraph with `"SAR-DOD:C:DEMOSAP1"`. The resource element would have `@SARIdentifier` with both `"SAR-DOD:S:DEMOSAP1"` and `"SAR-DOD:C:DEMOSAP1"`. ISM-Rollup.XML<sup>[48]</sup> Extensible Stylesheet Language (XSL) ensures that all

values of **@SARIdentifier** across all portion marks appear in the resource element. The ISM rendering stylesheets de-duplicate all **@SARIdentifier** tokens with the same SAP marking value. For example, for the hypothetical resource element that has **@SARIdentifier** with both **"SAR-DOD:S:DEMOSAP1"** and **"SAR-DOD:C:DEMOSAP1"**, and assuming no other SAP tokens, the rendered SAP portion of the classification banner would be SAR-DEMOSAP1.

As noted in [Section 2.4.1.9.1, "Classification-based Read-ons for DoD SAPs"](#), when a SAP marking contains spaces, e.g., BUTTER POPCORN, the metadata value in **@SARIdentifier** replaces the space with an underscore, e.g., **"BUTTER\_POPCORN"**. The ISM rendering stylesheets replace a single underscore with a space, rendering **"SAR-BUTTER\_POPCORN"** in the banner or portion mark as SAR-BUTTER POPCORN. When a SAP marking contains an underscore, e.g., SAR-STORMY\_PETREL, the metadata value in **@SARIdentifier** replaces the underscore with two underscores, e.g., **"SAR-STORMY\_\_PETREL"**. The ISM rendering stylesheets replace the double underscore with a single underscore, rendering **"SAR-STORMY\_\_PETREL"** in the banner or portion mark as SAR-STORMY\_PETREL.

Currently, there are some differences in the rendering of SAPs between the IC rules and DOD rules. The ISM rendering stylesheets display banners and portion marks differently depending on whether **@ism:compliesWith** contains **"USIC"** or **"USDOD"**, and in some cases on the owning agency of a SAP. Since rendering rules differ for IC and DOD documents, there are ISM Schematron constraint rules that disallow documents in some cases when **@ism:compliesWith** contains both **"USIC"** and **"USDOD"**. The different rendering rules in this version are:

1. Multiple tokens in **@SARIdentifier**. When **@SARIdentifier** contains multiple tokens:
  - The IC rule is to render the SAP value with 'SAR-' before the first SAP token, but not before subsequent tokens<sup>[28]</sup>.
  - The DOD rule is to render the SAP value with 'SAR-' before each and every SAP token<sup>[21]</sup>.
2. Three or more tokens in **@SARIdentifier**:
  - The IC rule is to render every token in **@SARIdentifier**, no matter how many tokens<sup>[28]</sup>.
  - The DOD rule requires that when there are three or more tokens in **@SARIdentifier**, the banner and portion mark should render as SAR-MULTIPLE PROGRAMS<sup>[21]</sup>.
3. Subcompartments in **@SARIdentifier**:
  - The IC rule for banners and portion marks is that dashes indicate SAP compartments, with subcompartments separated from their compartments by a space. The general pattern in a banner or portion mark is //SAR-[program identifier]-[compartment] [subcompartment]. In the ISM **@SARIdentifier** attribute, the space before a subcompartment is replaced by a dash (-) because individual values in **@SARIdentifier** must be tokens. For example, for a DNI SAP //SAR-BP-A12 125, the A12 is a compartment within BP, and 125 is a subcompartment of A12. The equivalent ISM **@SARIdentifier="SAR-BP-A12-125."** The rendering stylesheets treat a dash following a non-DOD SAP as indicating a compartment, and a dash

following a non-DOD SAP compartment as a subcompartment, and render the tokens back according to the IC rules. For example, according to the IC Markings<sup>[28]</sup>, a hypothetical DNI SAP portion of a banner //SAR-BP-121-A12 125 CDE indicates that the program identifier BP has two compartments: 121 and A12, and A12 has two subcompartments 125 and CDE. The @SARIdentifier value is "SAR-DNI:BP-121 SAR-DNI:BP-A12-125 SAR-DNI:BP-A12-CDE". For a non-DOD SAP, where the @SARIdentifier has a non-DOD owning agency, the rendering stylesheets handle the dashes in @SARIdentifier as indicating compartments and subcompartments, and render the @SARIdentifier value as indicated in the IC Markings<sup>[28]</sup>.

- DOD SAPCO guidance is that all DOD SAP markings are “peers” for the purposes of banner/portion markings. For a DOD SAP, where the @SARIdentifier has DOD as the owning agency, there are no special rendering rules for @SARIdentifier tokens that contain dashes. The rendering stylesheets treat all DOD @SARIdentifier tokens as single-level SAPs.

### 2.4.1.9.3 - Rendering Stylesheet for DOD

DOD agencies should use the “IC-ISM-DOD-Rendering.xml” rendering stylesheet, which sets parameters that cause the ISM.XML rendering stylesheets to conform to DOD policies for SAPs.

### 2.4.1.9.4 - Rules for SAP Values in ISM SARIdentifier

In order to ensure that SAP values in ISM follow the patterns documented in the previous section, the SAP values MUST follow the logical pattern, Augmented Backus-Naur Form (ABNF), and the Path Language (XPath) regular expression that follow: *Introducing Regular Expressions*<sup>[67]</sup>:

Logical pattern: SAR-[SAP Authority]:[Optional Classification Level]:[SAP Marking]

#### SAP ABNF Format

- [1] SAP ::= "SAR"-"SAP Authority ":" Optional Classification ":" SAP Marking
- [2] SAP Authority ::= 3\*255(ALPHA)
- [3] Optional ::= 0\*1("TS" / "S" / "C" )  
Classification
- [4] SAP Marking ::= 1\*255(ALPHA / DIGIT / "\_" / "." / "-" )

XPath regular expression: ^SAR-[A-Z]{3,}:(C|S|TS):{0,1}[A-Za-z0-9.\_-]{1,}\$

The [A-Z]{3,} portion of the above regular expression provides a general character constraint on the allowed SAP values. EO 13526, *Executive Order 13526 – Classified National Security Information*<sup>[24]</sup>, Section 4.3, lists the agencies that are authorized to establish special access programs. U.S. Department of State (DOS), DOD, DOE, Department of Homeland Security (DHS), Attorney General (AG), and DNI are the **only** agencies currently authorized to define SAPs. Therefore, the values of the [A-Z]{3,} portion of the SAP regular expression MUST be limited to these six agencies. This version of ISM contains an internal controlled vocabulary, “CVEnumISMSARAuthorities”, that lists the allowed values for the [A-Z]{3,} portion of the SAP regular expression. ISM Schematron constraint rule “ISM-ID-00530” validates a @SARIdentifier's owning agency against the allowed values in “CVEnumISMSARAuthorities”.

## 2.4.1.9.5 - Published and Unpublished SAPs

Currently, no SAP markings are published in the IC Markings<sup>[28]</sup>.

Developers of systems processing SAP from the unpublished Register will need to contact the POC listed in [Appendix E - Points of Contact](#) for guidance on how to add unpublished SAPs to “CVerenumISMSAR”.

All SAP values, published or unpublished, MUST conform to the regular expression defined in the preceding section.

## 2.4.1.9.6 - WAIVED Dissemination Control for DoD SAPs

*Special Access Program (SAP) Security Manual: Marking (Vol 4)* <sup>[21]</sup>, Section 2.d, states:

SAPs specifically exempted from normal congressional reporting requirements by the Secretary of Defense shall also be marked “WAIVED” in the banner line, at applicable portions, and prominently on media (e.g., TOP SECRET//SAR-DIGITAL AXIS//WAIVED). In such cases, “WAIVED” shall be placed last in the sequence and serves as a dissemination control marking.

This ISM.XML includes **"WAIVED"** as an allowed value in `@ism:disseminationControls`. **"WAIVED"** is only allowed when `@ism:compliesWith` contains **"USDOD"** (Schematron constraint rule “ISM-ID-00535”). **"WAIVED"** is rendered last in the sequence of `@ism:disseminationControls`.

## 2.4.2 - NTK Guidance

This section details guidance for the NTK segment of ISM.XML.

### 2.4.2.1 - NTK Integration into a Schema

The NTK schema is not designed nor intended to be used as a stand-alone schema. In order to use the capabilities, the XML schema must be incorporated into another XML schema. For purposes of this documentation, we will refer to this other schema as the “resource” schema. Additionally, the “resource” schema must include the ISM XML schema of ISM.XML. The basic process for incorporation is as follows:

- Import this schema into the “resource” schema
- Define a namespace prefix
- Allow for the `@ntk:DESVersion` attribute to be used in the “resource” schema
- Ensure ISM.XML metadata is incorporated into the “resource” schema
- Add the `ntk:Access` element to the “resource” schema model at an appropriate location

NTK elements are designed to record information for an entire resource. The resource includes the NTK element information itself. This means that those that have access to the resource will have access to all of the NTK information.

## 2.4.2.2 - NTK Basic Usage Model

This model should be used to help ensure this DES is effectively implemented in the enterprise.

- Systems that provide access control services to the enterprise must understand the NTK parameters defined in this specification. Access policy systems may also require custom NTK access profile structures including new parameters and syntax. Custom NTK structures are known as extensions. NTK extensions intended for exchange outside of a single agency should be coordinated with the IC CIO for publishing. Coordination with the IC CIO will help make information accessible and ensure uniform access control across the enterprise.
- To utilize a specific access policy system, resources must be marked in accordance with the requirements of that system, including any required NTK extensions. NTK may be specified in terms of more than one access requirement in separate access profiles.

## 2.4.3 - ARH Guidance

This section details guidance for the ARH segment of ISM.XML.

### 2.4.3.1 - ARH Security and ExternalSecurity

ARH defines two root elements, **arh:Security** and **arh:ExternalSecurity**, for expressing the access rights and handling information for a data object.

- The **arh:Security** element reflects ARH for a data object that is either present in the same instance document as **arh:Security** or is the instance document containing the **arh:Security** element.
- The **arh:ExternalSecurity** element reflects ARH for a data object external to the instance document containing the **arh:ExternalSecurity** element. Compared to **arh:Security**, **arh:ExternalSecurity** includes two additional ISM.XML elements to describe its external status, **@ism:externalNotice** and **@ism:excludeFromRollup**

### 2.4.3.2 - ARH MIME type

ARH has a Media Type (MIME) type as the container schema for ISM.XML. The MIME type for an ARH document is `application/dni-arh+xml`. This is a convention for our community. This type has NOT been registered with the Internet Assigned Numbers Authority (IANA). Should there be a conflict in the future it will be addressed at that time. Systems can use this MIME type to facilitate communications and address business needs within the community.



## Chapter 3 - Constraints

### 3.1 - “Living” Constraint Rules

These constraint rules are a “living” rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710<sup>[39]</sup> implemented in the IC Markings<sup>[28]</sup>, ISOO 32 Code of Federal Regulations (CFR) Parts 2001 and 2004 (as of September 22, 2003)<sup>[52]</sup>, E.O. 13526, as amended<sup>[24]</sup>, and E.O. 12829, as amended, *Executive Order 12829 – National Industrial Security Program, as Amended*<sup>[22]</sup>. These rules will be expanded and modified as the model matures, the IC Markings<sup>[28]</sup> Register is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

### 3.2 - Data Validation Constraint Rules

The ISM.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which XML instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML<sup>[34]</sup> framework document.



#### Note

The **arh:Security** and **arh:ExternalSecurity** elements are not intended to be the root node of a standalone XML instance document, and thus schematron validation of an instance document where one of those two elements is the root node will result in an error. However, when using ISM.XML to provide security marking metadata for non-XML files or data streams, an XML instance document containing just the security marking metadata for the file as a whole and not just the instance document MAY be embedded within the broader file or stream. In that case, use ISM.XML validation Phases by applying only those Phases that are applicable to **arh:Security** or **arh:ExternalSecurity** elements without document content. When validating **arh:Security** or **arh:ExternalSecurity** as physical or logical standalone elements, use the ISM.XML Phases of BANNER, TYPECHECK, VALUECHECK, and STRUCTURECHECK. Validating standalone **arh:Security** or **arh:ExternalSecurity** elements should not use ROLLUP or ROLLDOWN validation Phases, since the security metadata in standalone **arh:Security** or **arh:ExternalSecurity** elements will be referring to data that is not undergoing ISM.XML validation.

## 3.2.1 - Value Enumeration Constraints

Several elements and attributes of the ISM.XML model use CVEs to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

Some CVEs are not available on all networks. A subset CVE will be provided for use on networks not approved for the entire list. If the processing will occur on a network where the entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

Developers of systems processing SCI or SAP from the unpublished Register will need to contact the POC listed in [Appendix E - Points of Contact](#) for guidance as those values may have been omitted from the CVE.

As noted in the specific rules, a failure of validation against a CVE will generate an Error.

## 3.2.2 - Additional Constraints

### 3.2.2.1 - DES Constraints

The DES version is specified through attributes on the root element. The schema constrains the values of these attributes. The `@ism:DESVersion` attribute enables systems processing an instance document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

## 3.2.3 - Constraint Rules

The detailed constraint rules for the ISM.XML schema can be found in a separate document inside the Documents/ISM directory, in the "ISM\_Rules.pdf" file. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron. Obsolete rule numbers are listed in the "ISM\_Rules.pdf" file.

## 3.3 - Data Rendering Constraint Rules

### 3.3.1 - Purpose

Rendering rules define constraints on the rendering and display of ISM.XML documents. The intent is to inform the development of systems capable of rendering or displaying ISM.XML data for use by individuals not familiar with the details of the ISM.XML markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; instead, these rules should inform the evaluation of a system's capabilities and functionality.

ISM.XML includes XSL formatting stylesheets that render ISM attributes into a classification banner, portion marking, and classification authority block according to *Classified National Security Information; Final Rule* [\[51\]](#), *Marking Controlled Unclassified Information* [\[15\]](#) and



*Controlled Unclassified Information (CUI)* [\[20\]](#), as appropriate. The rendering stylesheets also render a second-line banner if there is a `@ism:secondBannerLine` attribute, and a Handle Via statement if there is a `@ism:handleViaChannels` attribute.

- Systems are not required to use the ISM rendering stylesheets to generate classification banners, portion markings and blocks. Systems MAY use other implementations that generate equivalent banners, portion marks and blocks.
- Systems MUST generate the same textual classification banners, second line banners, Handle Via lines, portion markings and blocks as the ISM rendering stylesheets, given the same ISM attribute values.

### 3.3.2 - ISM.XML Rendering Constraint Rules

The following sections contain the information for the ISM.XML data rendering constraint rules.

#### 3.3.2.1 - [ISM-RENDER-00001]

- **Rule Number:** ISM-RENDER-00001
- **Severity:** Error
- **Description:** Software that uses ISM attributes to generate classification banners MUST render classification banners that match the output of the “IC-ISM-SecurityBanner.xml” rendering stylesheet, given the same ISM attribute values.
- **Human Readable Description:** Systems MAY use software other than the ISM rendering stylesheets to generate classification banners, but the classification banners output by all systems MUST be identical to the output of the ISM rendering stylesheets.

#### 3.3.2.2 - [ISM-RENDER-00002]

- **Rule Number:** ISM-RENDER-00002
- **Severity:** Error
- **Description:** Software that uses ISM attributes to generate classification portion marks MUST render portion marks that match the output of the “IC-ISM-PortionMark.xml” rendering stylesheet, given the same ISM attribute values.
- **Human Readable Description:** Systems MAY use software other than the ISM rendering stylesheets to generate portion marks, but the portion marks output by all systems MUST be identical to the output of the “IC-ISM-PortionMark.xml” rendering stylesheet.

#### 3.3.2.3 - [ISM-RENDER-00003]

- **Rule Number:** ISM-RENDER-00003
- **Severity:** Error

- **Description:** When a document contains the ISM `@ism:secondBannerLine` attribute and/or the `@ism:handleViaChannels` attribute, the system must output a new line for the second banner line attributes `@ism:secondBannerLine` and/or `@ism:handleViaChannels`, as appropriate.
  - “IC-ISM-SecurityBanner.xml” outputs a pipe (‘|’) before the second banner line in the text output by “IC-ISM-SecurityBanner.xml”. Systems MAY use software other than the ISM rendering stylesheets to generate second banner lines, but the second banner line output by all systems MUST be identical to the second banner line output after the pipe (‘|’) of the “IC-ISM-SecurityBanner.xml” rendering stylesheet, given the same ISM attributes.
  - For the header of the document at the top of a page, the second banner line MUST be on a new line **below** the main classification banner. In the header of a page, the second banner line is rendered after the main classification banner.
  - For the footer of the document at the bottom of a page, the second banner line MUST be on a new line **above** the main classification banner. In the footer of a page, the second banner line is rendered before the main classification banner.
- **Human Readable Description:** Systems MUST render a second banner line when there is an `@ism:secondBannerLine` attribute and/or an `@ism:handleViaChannels` attribute.

The second banner line MUST be identical to the second banner line text output by “IC-ISM-SecurityBanner.xml”.

The second banner line MUST be rendered in a separate line **after** the main classification banner in the header of the document at the top of the page.

The second banner line MUST be rendered in a separate line **before** the main classification banner in the footer of the document at the bottom of the page.

### 3.3.2.4 - [ISM-RENDER-00004]

- **Rule Number:** ISM-RENDER-00004
- **Severity:** Error
- **Description:** When an asset has `@ism:noticeType` specified, then the rendering of the asset must display the appropriate notice:
  - When there is `@ism:noticeType` but **no** `@ism:noticeProseID`, then the system MUST render the value of `ism:NoticeText` for the notice.
  - When there is `@ism:noticeType` **and** `@ism:noticeProseID`, then the system MUST render the text found in “CVENumISMNoticeProse.xml” for the value of `@ism:noticeProseID`.
- **Human Readable Description:** Systems MUST render a notice or warning text when `@ism:noticeType` is specified. The notice/warning text MUST come from the “CVENumISMNoticeProse.xml” vocabulary when `@ism:noticeProseID` is present. The

notice/warning text MUST come from the `ism:NoticeText` attribute if there is no `@ism:noticeProseID` attribute.

### 3.3.2.5 - [ISM-RENDER-00005]

- **Rule Number:** ISM-RENDER-00005
- **Severity:** Error
- **Description:** Software that uses ISM attributes to generate classification authority blocks MUST render a classification authority block that matches the output of the “IC-ISM-ClassDeclass.xml” rendering stylesheet, given the same ISM attribute values.
- **Human Readable Description:** Systems MAY use software other than the ISM rendering stylesheets to generate classification authority blocks, but the classification authority blocks output by all systems MUST be identical to the output of the ISM rendering stylesheets.

### 3.3.2.6 - [ISM-RENDER-00006]

- **Rule Number:** ISM-RENDER-00006
- **Severity:** Error
- **Description:** Software that renders documents containing CUI markings MUST render CUI banners, portion marks and control/decontrol blocks that match the output of the ISM.XML XSL rendering stylesheets. When rendering DOD CUI documents, software MUST render a security banner, portion mark, and control/decontrol block that matches the output of the “IC-ISM-DOD-Rendering.xml” stylesheet. When rendering non-DOD CUI documents, software MUST render a security banner, portion mark, and control/decontrol block that matches the output of the “IC-ISM-ISOO-Rendering.xml” stylesheet.
- **Human Readable Description:** Systems MAY use software other than the ISM rendering stylesheets to generate CUI banners, portion marks and control/decontrol blocks, but the CUI marking output of all systems MUST be identical to the output of the ISM rendering stylesheets. DOD documents that have CUI markings MUST follow DoD policy when rendering a security banner, portion mark, and control/decontrol blocks. Non-DOD documents that have CUI markings MUST follow ISOO policy when rendering a security banner, portion mark, and control/decontrol blocks.

### 3.3.2.7 - [ISM-RENDER-00007]

- **Rule Number:** ISM-RENDER-00007
- **Severity:** Error
- **Description:** Software that renders documents containing DOD SAP markings MUST render classification banners and portion marks that match the output of the “IC-ISM-DOD-Rendering.xml” stylesheet.
- **Human Readable Description:** Software that renders documents containing DOD SAP markings MUST follow DOD SAP policy for security banners and portion marks. Systems

MAY use software other than the ISM rendering stylesheets to generate classification banners and portion marks for documents containing DOD SAP markings , but the banners and portion marks MUST be identical to the output of the ISM rendering stylesheets.

### 3.3.2.8 - [ISM-RENDER-00008]

- **Rule Number:** ISM-RENDER-00008
- **Severity:** Error
- **Description:** When an asset has `@ism:nonUScontrols` specified with a value of "SSI" then the rendering of the asset must display an SSI warning at the bottom of every page.
- **Human Readable Description:** SSI Warnings must be rendered at the bottom of every page of an asset.

## 3.3.3 - NTK Rendering Constraint Rules

The following sections contain the information for the NTK data rendering constraint rules.

### 3.3.3.1 - [NTK-RENDER-00001]

- **Rule Number:** NTK-RENDER-00001
- **Severity:** Error
- **Description:** If a NTK assertion with a `ntk:AccessPolicy` value of "urn:us:gov:ic:aces:ntk:oc" exists, then
  - The value of `ntk:AccessProfileValue` with attribute `@ntk:qualifier="originator"` MUST be rendered as the originating agency.
  - The values of all `ntk:AccessProfileValue` elements with attribute `@ntk:qualifier="dissemto"` MUST be rendered as the list of agencies authorized for access.
- **Human Readable Description:** Systems used for rendering data containing ORCON MUST produce rendered documents that comply with ICPG 710.1, *Application of Dissemination Controls: Originator Control* <sup>[41]</sup>, and any guidelines described therein.

### 3.3.3.2 - [NTK-RENDER-00002]

- **Rule Number:** NTK-RENDER-00002
- **Severity:** Warning
- **Description:** If a NTK assertion with an `ntk:AccessPolicy` value of "urn:us:gov:ic:aces:ntk:nd" exists, then
  - The values of `ntk:AccessProfileValue` elements with `@ntk:vocabulary` attributes that start with 'group:' SHOULD be rendered as groups authorized for access.

- The values of **ntk:AccessProfileValue** elements with **@ntk:vocabulary** attributes that start with 'individual:' SHOULD be rendered as individuals authorized for access.
- **Human Readable Description:** Systems used for rendering data containing Data Encoding Specification for No Distribution Need-To-Know (NODIS) SHOULD produce rendered documents that display the groups and/or individuals authorized for access.

### 3.3.3.3 - [NTK-RENDER-00003]

- **Rule Number:** NTK-RENDER-00003
- **Severity:** Warning
- **Description:** If an ISM.XML assertion with an **ntk:AccessPolicy** value of "urn:us:gov:ic:aces:ntk:xd" exists, then
  - The value of **ntk:AccessProfileValue** with attribute **@ntk:qualifier="originator"** SHOULD be rendered as the originating agency.
  - The values of all **ntk:AccessProfileValue** elements with attribute **@ntk:qualifier="dissemto"** SHOULD be rendered as the list of agencies authorized for access.
- **Human Readable Description:** Systems used for rendering data containing Exclusive Distribution (EXDIS) SHOULD produce rendered documents that display the originator and agencies authorized for access.

### 3.3.3.4 - [NTK-RENDER-00004]

- **Rule Number:** NTK-RENDER-00004
- **Severity:** Warning
- **Description:** If an ISM.XML assertion with an **ntk:AccessPolicy** value that starts with "urn:us:gov:ic:aces:ntk:propin:" exists, then
  - The values of **ntk:AccessProfileValue** elements with **@ntk:vocabulary** attributes that start with "group:" SHOULD be rendered as groups authorized for access.
  - The values of **ntk:AccessProfileValue** elements with **@ntk:vocabulary** attributes that start with "individual:" SHOULD be rendered as individuals authorized for access.
- **Human Readable Description:** Systems used for rendering data containing Proprietary Information (PROPIN) SHOULD produce rendered documents that display the groups and/or individuals authorized for access.

### 3.3.3.5 - [NTK-RENDER-00005]

- **Rule Number:** NTK-RENDER-00005

- **Severity:** Warning
- **Description:** For ISM.XML assertions not defined above and in the absence of specific rendering guidance, render the **ntk:AccessPolicy** URN and **ntk:AccessProfileValues** grouped by **ntk:VocabularyType**.
- **Human Readable Description:** Systems used for rendering data containing ISM.XML assertions not defined above and in the absence of specific rendering guidance, SHOULD produce rendered documents that display the **ntk:AccessPolicy** URN and **ntk:AccessProfileValues** grouped by **ntk:VocabularyType**.

## Chapter 4 - NTK Access Profiles

### 4.1 - Access Profile Structures

NTK elements within ISM.XML provide a set of predefined access profile structures to help meet many enterprise requirements for need-to-know metadata. The predefined structures are Data Sphere, Group & Individual, and Agency Dissemination. Each structure is designated with a specific **ntk:ProfileDes** URN. For example, the use of the Agency Dissemination **ntk:ProfileDes** value — "urn:us:gov:ic:ntk:profile:agencydissem" — allows for the use of a list of authorized recipients by government agency.

While certain access profile structures are needed within the enterprise, caution should be exercised when applying these structures to data. Implementers should recognize that the use of Group and Individual access profile structures will carry a long-term maintenance tail that could result in loss of access to data over time.

#### 4.1.1 - Agency Dissemination

The Agency Dissemination structure is used for need-to-know metadata based on Government agencies and top-level organizations. It consists of a list that specified the originating agency and any other agencies to which the information may be disseminated. ORCON is an example of data that would need to use the Agency Dissemination structure.

#### 4.1.2 - Data Sphere

The Data Sphere structure is used for need-to-know metadata based on data attributes. These attributes are sometimes called "data sensitivities" and are considered to be an inherent part of the data. Data Sphere assertions are used to express access restrictions based on these inherent data attributes such as licensing, mission need, etc.

#### 4.1.3 - Group and Individual

The Group and Individual structure is used for need-to-know metadata based on groups and/or individuals, which may be used to represent many types of person-based labels or categories including roles, COIs, etc. For the purposes of the Group NTK structure, groups on data map to the concept of some person-based categorization provisioned in an authoritative attribute source. Individuals are commonly identified by fully-qualified Distinguished Name (DN). Some sources that might be used to find a DN are IC Public Key Infrastructure (PKI) and Cryptologic Agencies Domain (CAD) PKI. A vocabulary MAY be defined that uses any authoritative source that provides person or group-based labels or categorization. For example, ICAM Service Provider Entitlement Management Service is an authoritative attribute source for entitlements that may be used as a source for a Group structure.

### 4.2 - Profile DES

Access profile structures are indicated by the use of an appropriate **ntk:ProfileDES** value. The **ntk:ProfileDES** value unambiguously defines the allowable structures, and these rules are enforced by Schematron rules. New **ntk:ProfileDES** values must be defined in order to use

combinations of access profile structures not already defined (i.e. only one profile DES may be used at a time). ISM.XML has three pre-defined **ntk:ProfileDES** values.

**Table 23 - NTK Profile DES Values**

Profile DES	URN
Agency Dissem	"urn:us:gov:ic:ntk:profile:agencydissem"
Data Sphere	"urn:us:gov:ic:ntk:profile:datasphere"
Group & Individual	"urn:us:gov:ic:ntk:profile:grp-ind"

## 4.3 - Vocabulary Types

Vocabulary Types define a vocabulary's source, including version or other identifying information. The **@ntk:vocabulary** attribute provides the identifier for the Vocabulary Type of an **ntk:AccessProfileValue** value; it is a required attribute.

NTK assertions may use built-in Vocabulary Types or new Vocabulary Types defined according to agency or mission use cases. Vocabularies are declared with the **ntk:VocabularyType** element. The **ntk:VocabularyType** element has three attributes: **@ntk:name**, **@ntk:source**, and **@ntk:sourceVersion**.

<b>@ntk:name</b>	<p>The unique identifier of a Vocabulary (required)</p> <p>Vocabulary Type names MUST inherit from a vocabulary root type using the appropriate root type prefix.</p>
<b>@ntk:source</b>	<p>The source of a Vocabulary</p> <p>A vocabulary source may be a CVE, system, or other source. For an IC CIO defined CVE, the <b>@ntk:source</b> value should be the XML namespace defined for the CVE. This value is required for user-defined vocabularies and optional for predefined vocabularies. If a value is specified for a predefined vocabulary, the value must match the source definition in this specification.</p>
<b>@ntk:sourceVersion</b>	<p>The version or other identifying attribute of a Vocabulary (optional)</p> <p>For IC CIO defined CVEs, the <b>@ntk:sourceVersion</b> should be the value of the <b>@cve:CVEVersion</b> attribute defined in the CVE.</p>

### 4.3.1 - Abstract Root Types

There are four vocabulary root types, each with a corresponding prefix to be used in Vocabulary Type names. Root types provide built-in, abstract concepts that must be sub-classed for a



Vocabulary Type instance. Sub-classing enables typing for all `ntk:AccessProfileValue` values. Root types MUST be defined in this DES; custom root types are forbidden. The four root types are:

- Individual (prefix "`individual:`")
- Group (prefix "`group:`")
- Organization (prefix "`organization:`")
- Data Sphere (prefix "`datasphere:`")

Individual and Group are for vocabularies based on people. Data Sphere is for vocabularies based on data attributes such as content indicators or categorization information. Organization is for vocabularies based on agency affiliation. Organization can be considered to straddle the line between people and data attributes. In the world of attribute-based access control, it is generally considered preferable to utilize data attributes instead of directly using person or group based restrictions, so Data Sphere may be preferred from an Attribute Based Access Control (ABAC) perspective.

## 4.3.2 - Vocabulary Types

Vocabulary Types are derived from root types and provide the ability to define a concrete vocabulary type.

### 4.3.2.1 - Built-In Vocabulary Types

To facilitate ease of use and reduce common repetitive information in instances of NTK elements within ISM.XML, there are several built-in subclasses defined in this DES.

## Built-In Individual Vocabulary Types

### Example 4.1. Individual identified by IC PKI Distinguished Name

```
<ntk:VocabularyType ntk:name="individual:icpki" ntk:source="IC-PKI:DN"/>
```

### Example 4.2. Individual identified by CAD PKI Distinguished Name

```
<ntk:VocabularyType ntk:name="individual:cadpki" ntk:source="CAD-PKI:DN"/>
```

## Built-In Group Vocabulary Types

### Example 4.3. Group from the ICAM Service Provider Entitlement Management Service system

```
<ntk:VocabularyType ntk:name="group:icamems" ntk:source="JWICS:ICAMEMS"/>
```

## Built-In Organization Vocabulary Types

### Example 4.4. Agencies from the USAgency.CES<sup>[71]</sup> specification

```
<ntk:VocabularyType ntk:name="organization:usa-agency"
  ntk:source="urn:us:gov:ic:cvenum:usagency:agencyacronym"/>
```

## Built-In DataSphere Vocabulary Types

### Example 4.5. Issues from the Mission Need<sup>[63]</sup> specification

```
<ntk:VocabularyType ntk:name="datasphere:mn:issue"
  ntk:source="urn:us:gov:ic:cvenum:mn:issue"/>
```

### Example 4.6. Regions from the Mission Need<sup>[63]</sup> specification

```
<ntk:VocabularyType ntk:name="datasphere:mn:region"
  ntk:source="urn:us:gov:ic:cvenum:mn:region"/>
```

### Example 4.7. Licenses from the License CES<sup>[62]</sup> specification

```
<ntk:VocabularyType ntk:name="datasphere:license"
  ntk:source="urn:us:gov:ic:cvenum:lic:license"/>
```

### Example 4.8. Restricted Authority Categories from the AUTHCAT.CES<sup>[1]</sup> specification

```
<ntk:VocabularyType ntk:name="datasphere:rac"
  ntk:source="urn:us:gov:ic:cvenum:authcat:authcattype"/>
```

## 4.3.2.2 - Further Defining Built-In Vocabulary Types

For built-in vocabulary types based on CVEs, it is necessary to specify the source version using the `@ntk:sourceVersion` attribute of an `ntk:VocabularyType` element. The `@ntk:name` attribute of the `ntk:VocabularyType` element must be identical to the built-in type. If specified, the `@ntk:source` attribute must be identical to the built-in source. Once a source or a version is specified, it is not possible to override those values. It is not necessary to specify a source version for other types of vocabularies (e.g., "`group:icamems`" does not require a source version since it is not based on a CVE). Currently, the source version must be specified for "`organization:usa-agency`", "`datasphere:mn:issue`", "`datasphere:mn:region`", and "`datasphere:license`" built-in vocabulary types.

For example, when using the built-in "`organization:usa-agency`" vocabulary, it is necessary to specify the *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES<sup>[71]</sup>) Controlled Vocabulary Enumeration Encoding Specification (CES) version. The instance document must declare the version with an `ntk:VocabularyType`. If the instance document used the 2015-FEB version of USAgency.CES<sup>[71]</sup>, it would declare the version in the following way:

## Example 4.9. Declaring USAgency Version

```
<ntk:VocabularyType ntk:name="organization:usa-agency"
ntk:sourceVersion="201502"/>
```

The full instance might look something like:

## Example 4.10. Agency Dissem Access Profile

```
<ntk:Access ism:classification="U" ism:ownerProducer="USA">
  <ntk:RequiresAnyOf>
    <ntk:AccessProfileList>
      <ntk:AccessProfile ism:classification="U" ism:ownerProducer="USA">
        <ntk:AccessPolicy>urn:us:gov:ic:aces:ntk:oc</ntk:AccessPolicy>
        <ntk:ProfileDes
          >urn:us:gov:ic:ntk:profile:agencydissem</ntk:ProfileDes>
        <ntk:VocabularyType ntk:name="organization:usa-agency"
          ntk:sourceVersion="201502"/>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="originator">CIA</ntk:AccessProfileValue>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="dissemto">DNI</ntk:AccessProfileValue>
        <ntk:AccessProfileValue ntk:vocabulary="organization:usa-agency"
          qualifier="dissemto">NSA</ntk:AccessProfileValue>
        </ntk:AccessProfile>
      </ntk:AccessProfileList>
    </ntk:RequiresAnyOf>
  </ntk:Access>
```

## 4.4 - Pre-Defined Access Profiles

ISM.XML provides a number of pre-defined Access Profiles, which are indicated by an **ntk:AccessPolicy** value. An access policy may provide additional restrictions on structure and vocabulary defined by the **ntk:ProfileDes**. For example, the Restrictive profile requires the Group & Individual **ntk:ProfileDes**, but it forbids the use of individuals in an assertion. Access Profiles may define new Schematron rules, which trigger on a specific **ntk:AccessPolicy** value. These new rules are in addition to any rules defined for the associated **ntk:ProfileDes**.

Access control decisions must conform to the logic defined in an ACES, and specific access control logic for these profiles is defined in ISM.ACES<sup>[47]</sup>. Implementers are free to develop an ACES and define new access profiles for use in local exchanges, but systems MUST reject information marked with a profile that is not defined for that system. The following sections provide the **ntk:AccessPolicy** URN, the associated **ntk:ProfileDes**, and any restrictions for use of profile structures and vocabularies. The following sections are for descriptive purposes and are not intended as a substitute for the ISM.ACES<sup>[47]</sup>.

### 4.4.1 - Enterprise Role Permissive

Access Policy: "urn:us:gov:ic:aces:ntk:enterprise:role:permissive"

Profile DES: "urn:us:gov:ic:ntk:profile:role"

The Enterprise Role Permissive profile provides an association mechanism for roles. The Enterprise Role Permissive profile is used to mark information that must be protected in accordance with the Enterprise Role Permissive access policies defined in the ISM.ACES<sup>[47]</sup>. Enterprise Role Permissive MUST be used with the Role **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited in use to the "**role:enterpriseRole**" vocabulary.

## 4.4.2 - Enterprise Role Restrictive

Access Policy: "**urn:us:gov:ic:aces:ntk:enterprise:role:restrictive**"

Profile DES: "**urn:us:gov:ic:ntk:profile:role**"

The Enterprise Role Restrictive profile provides an association mechanism for roles. The Enterprise Role Restrictive profile is used to mark information that must be protected in accordance with the Enterprise Role Restrictive access policies defined in the ISM.ACES<sup>[47]</sup>. Enterprise Role Restrictive MUST be used with the Role **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited in use to the "**role:enterpriseRole**" vocabulary.

## 4.4.3 - Exclusive Distribution (EXDIS)

Access Policy: "**urn:us:gov:ic:aces:ntk:xd**"

Profile DES: "**urn:us:gov:ic:ntk:profile:agencydissem**"

EXDIS is a Department of State marking that restricts a resource from being shared outside of the originating agency without prior approval of the originating agency. The XD-NTK access profile is used to mark information that must be protected in accordance with the EXDIS policies defined in the ISM.ACES<sup>[47]</sup>. XD-NTK requires the Agency Dissemination Profile **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited in use to the "**organization:usa-agency**" vocabulary.

## 4.4.4 - Group Permissive

Access Policy: "**urn:us:gov:ic:aces:ntk:permissive**"

Profile DES: "**urn:us:gov:ic:ntk:profile:grp-ind**"

The Group Permissive profile provides an association mechanism for groups or individuals. The Group Permissive profile is used to mark information that must be protected in accordance with the Group Permissive policies defined in the ISM.ACES<sup>[47]</sup>. Group Permissive MUST be used with the Group & Individual **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited to use with vocabularies that start with **"group:"** or **"individual:"** for the access profile values.

## 4.4.5 - Group Restrictive

Access Policy: **"urn:us:gov:ic:aces:ntk:restrictive"**

Profile DES: **"urn:us:gov:ic:ntk:profile:grp-ind"**

The Group Restrictive profile provides an association mechanism for groups. The Group Restrictive profile is used to mark information that must be protected in accordance with the Group Restrictive policies defined in the ISM.ACES<sup>[47]</sup>. Group Restrictive **MUST** be used with the Group & Individual **ntk:ProfileDes**, but Group Restrictive may only be used with groups. That is, the use of individuals with Group Restrictive is forbidden.

This access profile is solely restricted to use with vocabularies that start with **"group:"** for access profile values.

## 4.4.6 - Intelligence Community Only (ICO)

Access Policy: **"urn:us:gov:ic:aces:ntk:ico"**

Profile DES: N/A

The Intelligence Community Only (ICO) profile is used to mark information that must be protected in accordance with the ICO policies defined in the ISM.ACES<sup>[47]</sup>. ICO is used without a **ntk:ProfileDes** value since no additional structure is required.

## 4.4.7 - License

Access Policy: **"urn:us:gov:ic:aces:ntk:license"**

Profile DES: **"urn:us:gov:ic:ntk:profile:datasphere"**

The License profile is used to mark information that must be protected in accordance with a licensing agreement as defined in an ACES. License is used with the Data Sphere **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited to use of vocabularies **"datasphere:license"** for the access profile values.

## 4.4.8 - Mission Need Profile

Access Policy: **"urn:us:gov:ic:aces:ntk:mn"**

Profile DES: **"urn:us:gov:ic:ntk:profile:datasphere"**

Mission Need is used to express issues and regions that affect access control in accordance with the mission need policies defined in the ISM.ACES<sup>[47]</sup>. *XML CVE Encoding Specification for Mission-Need* (MN.CES<sup>[63]</sup>) Profile is used with the Data Sphere **ntk:ProfileDes**. MN.CES<sup>[63]</sup> Profile assertions are restricted to "**datasphere:mn:issue**" and "**datasphere:mn:region**" vocabularies.

This access profile is limited to use of vocabularies "**datasphere:mn:issue**" and "**datasphere:mn:region**" for the access profile values.

#### 4.4.9 - No Distribution (NODIS)

Access Policy: "**urn:us:gov:ic:aces:ntk:nd**"

Profile DES: "**urn:us:gov:ic:ntk:profile:grp-ind**"

NODIS is a DOS marking that restricts the distribution of a resource to named individuals. The ND-NTK access profile is used to mark information that must be protected in accordance with the NODIS policies defined in the ISM.ACES<sup>[47]</sup>. NODIS is used with the Group & Individual **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited to use with vocabularies that start with "**group:**" or "**individual:**" for the access profile values.

#### 4.4.10 - Originator Controlled (ORCON)

Access Policy: "**urn:us:gov:ic:aces:ntk:oc**"

Profile DES: "**urn:us:gov:ic:ntk:profile:agencydissem**"

ORCON restricts a resource from being shared outside of the originating agency without prior approval of the originating agency. The IC Markings<sup>[28]</sup> states this marking allows originators to maintain knowledge, supervision, and control of the distribution of the ORCON information beyond its original dissemination, and further dissemination of ORCON information requires advance permission from the originator. The ORCON access profile is used to mark information that must be protected in accordance with the ORCON policies defined in the ISM.ACES<sup>[47]</sup>. ORCON must be used with the Agency Dissem **ntk:ProfileDes**. There are no additional restrictions.

This access profile is limited in use to the "**organization:usa-agency**" vocabulary.

## 4.4.11 - Proprietary Information (PROPIN)

Access Policies:

"urn:us:gov:ic:aces:ntk:propin:1"

"urn:us:gov:ic:aces:ntk:propin:2"

Any that start with "urn:us:gov:ic:aces:ntk:propin:"

Profile DES: "urn:us:gov:ic:ntk:profile:grp-ind" (NOTE: Profile DES required for profile 2. Profile DES required for profile 1 only if groups or individuals are used.)

PROPIN is a marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value, as defined by the IC Markings<sup>[28]</sup>. The PROPIN profile is used to mark data that must be protected in accordance with the PROPIN policies defined in the ISM.ACES<sup>[47]</sup>. PROPIN is used with the Group & Individual **ntk:ProfileDes**. Multiple access policies are defined in the ISM.ACES<sup>[47]</sup>, and each access policy may define additional restrictions on the use groups and individuals. The second access policy of PROPIN ("urn:us:gov:ic:aces:ntk:propin:2") requires at least one group or individual.

Both of the profiles defined here are limited to use with vocabularies starting with "group:" or "individual:" for access profile values.

## 4.4.12 - Restricted Authority Category (RAC)

Access Policy: "urn:us:gov:ic:aces:ntk:rac"

Profile DES: "urn:us:gov:ic:ntk:profile:datasphere"

RAC specifies the authority under which the entity (person or non-person) is authorized to access and/or discover protected resources with policies defined in the ISM.ACES<sup>[47]</sup>. RAC is used with the Data Sphere **ntk:ProfileDes**.

This access profile is limited to use of vocabularies "datasphere:rac" for the access profile values.



## Chapter 5 - Controlled Unclassified Information (CUI)

### 5.1 - Overview

CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information. (*Controlled Unclassified; Final Rule* [\[53\]](#))

Implementation of CUI in ISM.XML follows requirements documented in the following Federal regulations and authorities:

- Executive Order 13556 *Controlled Unclassified Information* [\[25\]](#)
- 32 CFR Part 2002 *Controlled Unclassified; Final Rule* [\[53\]](#)
- CUI Category Registry *CUI Category Registry* [\[13\]](#)
- CUI Limited Dissemination Controls Registry *CUI Limited Dissemination Controls Registry* [\[14\]](#)
- *CUI Marking Handbook* [\[15\]](#)
- DoD Instruction 5200.48, *Controlled Unclassified Information (CUI)* [\[20\]](#).

CUI data is organized into Categories. Each CUI Category is based on at least one (and sometimes many) Federal laws, regulations, or government-wide policies that require a certain type of information to be protected or restricted in dissemination. There are two types of CUI Categories: Basic and Specified.

- CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in the CUI Final Rule and Registry. (*Controlled Unclassified; Final Rule* [\[53\]](#))
- CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. A CUI marking may be a Basic Category, a Specified category, or either type depending on the law that is being applied to a document or data. For example, the CUI General Law Enforcement Category ("**LEI**") category is always Basic. The CUI Foreign Intelligence Surveillance Act ("**FISA**") category is always Specified. The CUI General Proprietary Business Information ("**PROPIN**") category could be either Basic or Specified depending on the law(s) that led to the document being labeled as ("**PROPIN**"). CUI Specified markings can be identified because they are preceded by 'SP-', e.g., 'PROPIN' in a CUI banner means Basic ("**PROPIN**"), while 'SP-PROPIN' means Specified ("**PROPIN**").

### 5.2 - CUI and the IC Markings System Register and Manual

The latest version of the IC Markings [\[28\]](#), 30 April 2019, indicates that CUI for the IC is planned for implementation but detailed requirements have not yet been specified. Consequently, ISM.XML focuses on general CUI requirements from ISOO rather than requirements specific to the IC,



except for information in the latest IC Markings<sup>[28]</sup> that relates to future implementation of CUI. In addition, ISM.XML implements requirements from *DoD Instruction 5200.48* <sup>[20]</sup>, including DoD rules for the CUI control block.

The latest IC Markings<sup>[28]</sup> identifies several IC markings that are planned to be reflected in CUI markings and that will be evaluated for continued IC registration as CUI is implemented in the IC. These IC markings are:

- Dissemination Control Markings
  - **"FOUO"** maps to multiple, unspecified CUI categories.
  - **"DSEN"** maps to multiple, unspecified CUI categories.
- Non-IC Markings
  - **"DS"** maps to multiple, unspecified CUI categories.
  - **"SBU"** maps to multiple, unspecified CUI categories.
  - **"SBU-NF"** maps to multiple, unspecified CUI categories.
  - **"LES"** maps to the CUI **"LEI"** category.
  - **"LES-NF"** maps to the CUI **"LEI"** category combined with the **"NF"** dissemination control.
  - **"SSI"** maps to the CUI **"SSI"** category.

In addition to the above markings, two dissemination controls map to CUI categories even though they are not identified in the IC Markings<sup>[28]</sup> as markings that may be replaced by CUI markings. These are:

- **"FISA"** maps to the CUI **"FISA"** category.
- **"PR"** maps to the CUI **"PROPIN"** category..

Since **"DSEN"**, **"FISA"** and **"PR"** are allowed with both unclassified and classified data, ISM.XML implements these markings as ones that can appear as analogous CUI Categories in pure CUI documents and as dissemination controls or CUI Categories in commingled documents (see "Pure CUI and Commingled Documents" below).

Implementation of CUI in ISM.XML includes changes to CVEs and constraint rules that recognize the migration or replication of the above IC markings to CUI categories.

## 5.3 - Pure CUI and Commingled Documents

The *CUI Marking Handbook* <sup>[15]</sup> identifies two different types of documents that contain CUI information:

- Pure CUI. This type of document contains only CUI information and no classified information. These documents are always UNCLASSIFIED. They are subject to Federal rules for CUI but

are not subject to Federal rules for CNSI. In ISM.XML, a pure CUI document is identified by `@ism:compliesWith="USA-CUI-ONLY"`.

- Commingled documents. These documents contain CUI but also contain any type of classified information. In ISM.XML, a commingled document is identified by `@ism:compliesWith="USA-CUI"`.

## 5.4 - CUI Banner

The *CUI Marking Handbook* [\[15\]](#) defines rules for the banner in pure CUI and commingled documents.

In a pure CUI document, the banner includes:

- The CUI Control Marking. According to CUI policy, this marking may be either "Controlled" or "CUI," but ISM.XML always generates "CUI." The CUI Control Marking is just a text string in the banner in order to highlight the existence of CUI information in the document. CUI Categories follow the CUI Control Marking in the banner.
- CUI Category marking(s). Any CUI Specified Category Markings appear before any CUI Basic Category Markings. The *CUI Marking Handbook* [\[15\]](#) states that CUI Specified Category markings are required to appear in the CUI banner, while CUI Basic Category markings optionally appear in the CUI banner. Since a key objective of ISM.XML is to incorporate access control metadata needed for automated access control of a document, the ISM.XML implementation requires metadata for all CUI Basic and Specified Categories in the document. This allows the banner to display all CUI Category marking(s) that apply to the document, and supports ICAM systems in controlling access to CUI data.
- Any applicable dissemination controls from the *CUI Limited Dissemination Controls Registry* [\[14\]](#).
- The major parts of the CUI banner (CUI Control Marking, Specified Category Markings, Basic Category Markings, and Dissemination Controls) are separated by '//'. Within each part, multiple markings are separated by '/'.
- *DoD Instruction 5200.48* [\[20\]](#) states that CUI Categories and Limited Dissemination Controls do not have to appear in the banner, but must be included in the CUI control block. ISM.XML always includes CUI Categories and Limited Dissemination Controls in the banner, but provides rendering software for DoD systems that will also render the CUI Categories and Limited Dissemination Controls in the control block.

An example of a pure CUI banner is "**CUI//SP-FISA//LEI//NF**", where:

- 'CUI' is the CUI Control Marking
- 'SP-FISA' is the category marking for the Foreign Intelligence Surveillance Act CUI Specified Category
- 'LEI' is the category marking for the General Law Enforcement CUI Basic Category
- 'NF' is the marking for the NOFORN CUI Limited Dissemination Control.

In a commingled document, the CUI Category markings are integrated into the classified banner (*CUI Marking Handbook* [\[15\]](#)). The CUI Control Marking and Category Marking(s) appear in a classified banner after any **@ism:FGI** markings and before any **@ism:dissemination controls**.

An example of a commingled banner is "**SECRET//SI/TK//FGI GBR//CUI//SP-FSEC/INTEL/LEI//REL TO USA, GBR**", where:

- 'SECRET' is the overall classification of the commingled document
- 'SI' and 'TK' are the two SCIs for the document
- 'FGI GBR' indicates the document contains Foreign Government Information (FGI) from Great Britain ('GBR')
- 'CUI' is the CUI Control Marking
- 'SP-FSEC' is a CUI Specified Category Marking
- 'INTEL' and 'LEI' are two CUI Basic Category Markings
- 'REL TO USA, GBR' is a dissemination control that indicates the document is releasable to USA and GBR.

The *CUI Marking Handbook* [\[15\]](#) does not clarify where classified dissemination controls and non-IC markings appear in a commingled banner.

- The ISM.XML implementation of CUI integrates classified dissemination controls with CUI-specific dissemination controls in the same section of a commingled document banner. In ISM.XML, the classified dissemination controls precede the CUI-specific dissemination controls.
- Since "**FOUO**" is planned for replacement with one or more CUI markings, and is only allowed with unclassified information, ISM.XML does not allow "**FOUO**" in a commingled document; CUI markings that replace "**FOUO**" should be used instead of "**FOUO**".

- Most non-IC markings in the IC can only be used with unclassified information and therefore are expected to be replaced by CUI markings, including in commingled documents. The exceptions are "**XD**" and "**ND**", which can appear with either classified or unclassified data. Since the *CUI Marking Handbook* <sup>[15]</sup> does not specify where non-IC markings appear in a commingled banner, ISM.XML does not allow non-IC markings in commingled documents until banner requirements are clarified.

The CUI Limited Dissemination Controls overlap with the dissemination controls in the IC Markings<sup>[28]</sup>. The following table lists the CUI Limited Dissemination Controls from the *CUI Limited Dissemination Controls Registry* <sup>[14]</sup>, and notes where the list overlaps with dissemination controls in the IC Markings<sup>[28]</sup>.

**Table 24 - CUI Limited Dissemination Controls**

Dissemination Control	Portion Marking	Description	Notes
No foreign dissemination	NF	Cannot be disseminated to foreign governments, foreign nationals, foreign or international organizations, or non-US citizens.	Same as " <b>NF</b> " for classified data
Federal Employees Only	FED ONLY	Disseminate only to (1) employees of US Government Executive branch departments and agencies, or (2) armed forces personnel of the US or Active Guard and Reserve.	Used only for documents with CUI information
Federal Employees and Contractors Only	FEDCON	Disseminate only to (1) persons meeting the definition for FED ONLY, or (2) individuals or employers who enter into a contract with the US government.	Used only for documents with CUI information
No dissemination to Contractors	NOCON	No dissemination authorized to individuals or employers who enter into a contract with the US Government.	Used only for documents with CUI information
Dissemination List Controlled	DL ONLY	Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list.	Used only for documents with CUI information
Authorized for release to certain nationals only	REL TO [USA, LIST]	Information has been predetermined by the designating agency to be releasable or has been released only to the foreign country(ies)/international organization(s) indicated.	Same as " <b>REL TO</b> " for classified data

Dissemination Control	Portion Marking	Description	Notes
DISPLAY ONLY	DISPLAY ONLY	Information is authorized for disclosure to a foreign recipient, but without providing the foreign recipient with a physical copy for retention.	Same as " <b>DISPLAY ONLY</b> " for classified data
Attorney-Client	AC	Dissemination of information protected by the attorney client privilege beyond the attorney, the attorney's agents, or the client can result in the loss of the privilege and is prohibited by this marking, unless the agency's executive decision makers decide to disclose the information outside the bounds of its protection.	Note the Legal Privilege Category marking "PRIVILEGE" must be applied in order to use this limited dissemination control marking.
Attorney-WP	AWP	Dissemination of information protected by the Attorney Work Product Privilege beyond the attorney, the attorney's agents, or the client can result in the loss of the privilege and is prohibited by this marking, unless specifically permitted by the overseeing attorney who originated the work product or their successor.	Note the Legal Privilege Category marking "PRIVILEGE" must be applied in order to use this limited dissemination control marking.
Deliberative	DELIB	Dissemination of information protected by the deliberative process privilege beyond the department, agency, or U.S. Government decision maker who is part of the policy deliberation can result in the loss of the privilege and is prohibited by this marking, unless the executive decision makers at the agency decide to disclose the information outside the bounds of its protection.	Note the Legal Privilege Category marking "PRIVILEGE" must be applied in order to use this limited dissemination control marking.

## 5.5 - CUI Block

The *Controlled Unclassified; Final Rule* [\[53\]](#) defines a CUI designation indicator and decontrolling indicators that are analogous to lines in the classification authority block in a classified document.

- The CUI designation indicator is implemented in a new **@ism:cuiControlledBy** attribute. The **@ism:cuiControlledBy** attribute is required whenever there is CUI data in a

document, as indicated by `@ism:compliesWith="[USA-CUI]"` or `@ism:compliesWith="[USA-CUI-ONLY]"` (Executive Order 13556 *Controlled Unclassified Information* <sup>[25]</sup>). The `@ism:cuiControlledBy` attribute is equivalent to the `@ism:classifiedBy` and `@ism:derivativelyClassifiedBy` attributes for classified data. A commingled document must include the `@ism:cuiControlledBy` attribute and one of the `@ism:classifiedBy` or `@ism:derivativelyClassifiedBy` attributes.

- There are two decontrolling indicators for CUI. These are the decontrol date and decontrol event. They are implemented in ISM.XML by `@ism:cuiDecontrolDate` and `@ism:cuiDecontrolEvent`. These attributes are equivalent to `@ism:declassDate` and `@ism:declassEvent` for classified documents. Executive Order 13556 *Controlled Unclassified Information* <sup>[25]</sup> identifies these indicators as optional, so ISM.XML does not require them in CUI documents. A commingled document must include one of `@ism:declassDate`, `@ism:declassEvent` or `@ism:declassException`, but is not required to include either `@ism:cuiDecontrolDate` or `@ism:cuiDecontrolEvent`.

ISM.XML only allows a document to have `@ism:cuiControlledBy`, `@ism:cuiDecontrolDate`, and/or `@ism:cuiDecontrolEvent` if the document contains CUI data; i.e., the document is either a pure CUI document or a commingled document.

- *DoD Instruction 5200.48* <sup>[20]</sup> requires additional information in the control block of a document marked CUI. The DoD CUI control block has five lines:
  - Controlled by: [Name of DoD Component]. *DoD Instruction 5200.48* <sup>[20]</sup> states this line is only required if the component is not listed in the letterhead. ISM.XML requires this line so that the information is contained in metadata and not just in text in a letterhead. The value in this line comes from the `@ism:cuiControlledBy` attribute.
  - Controlled by: [Name of Office]. The value in this line comes from the new `@ism:cuiControlledByOffice` attribute.
  - CUI Category: This line lists `@ism:cuiBasic` markings followed by `@ism:cuiSpecified` markings.
  - Distribution/Dissemination Control: This line lists the `@ism:disseminationControls` that are CUI Limited Dissemination Controls identified in the CUI Registry.
  - POC: [Phone or email address] . The value in this line comes from the new `@ism:cuiPOC` attribute.
  - *DoD Instruction 5200.48* <sup>[20]</sup> does not list decontrol instructions as information that should appear in the CUI control block. ISM.XML will render `@ism:cuiDecontrolDate` and/or `@ism:cuiDecontrolEvent` if either or both of these attributes are available in the document.

## 5.6 - CUI Constraint Rules

This Section provides a high-level overview of key constraint rules for CUI data in ISM.XML.

## 5.6.1 - Dissemination Controls in CUI Documents

As described above, the list of CUI dissemination controls overlaps with dissemination controls for classified information, but there are also CUI-specific dissemination controls. The list of allowable dissemination controls for a document that contains CUI information depends on whether the document is pure CUI or commingled.

ISM.XML uses the value of `@ism:compliesWith` for a CUI document to determine the appropriate list of dissemination controls allowed in the document.

- For a pure CUI document, i.e., `@ism:compliesWith="[USA-CUI-ONLY]"`, then the ISM.XML executable constraint rules use the list of dissemination controls from the *CUI Limited Dissemination Controls Registry* [\[14\]](#). This list is found in the controlled vocabulary called `CVEnumISMDissemCui.xml`.
- For a commingled document, i.e., `@ism:compliesWith="[USA-CUI]"`, then the ISM.XML executable constraint rules use the list of dissemination controls from the *CUI Limited Dissemination Controls Registry* [\[14\]](#), **plus** the IC Markings [\[28\]](#) dissemination controls, removing the "FOUO" marking and collapsing duplicates such as "NF" and "REL". This list is found in the controlled vocabulary called `CVEnumISMDissemCommingled.xml`.
- For a document that contains no CUI, i.e., is exclusively CNSI, the ISM.XML executable constraint rules use the list of dissemination controls from the IC Markings [\[28\]](#). This list is found in the controlled vocabulary called "CVEnumISMDissemIcrm".

## 5.6.2 - Rules for Pure CUI Documents

ISM.XML implements the following abstract rules for pure CUI documents:

- A pure CUI document **MUST** have `@ism:compliesWith="[USA-CUI-ONLY]"`.
- `"[USA-CUI-ONLY]"` **MUST** be the only token in `@ism:compliesWith`.
- A pure CUI document **MUST NOT** include `@ism:classification` or `@ism:ownerProducer`. The concept of a classification marking is **NOT** part of CUI, so `@ism:classification` and `@ism:ownerProducer` **MUST NOT** appear in a pure CUI document. In contrast, a commingled document **MUST** include `@ism:classification` or `@ism:ownerProducer` in the banner and on any portion with ISM.XML attributes other than `@ism:DESVersion`, `@ism:ISMCATCESVersion`, `@ism:unregisteredNoticeType`, or `@ism:pocType`.
- A pure CUI document **MUST NOT** include any `@ism:SCIcontrols`, `@ism:SARIdentifier`, `@ism:atomicEnergyMarkings`, `@ism:FGISourceOpen`, `@ism:FGISourceProtected`, or `@ism:nonICcontrols` attributes.

## 5.6.3 - Rules for Commingled Documents

ISM.XML implements the following abstract rules for commingled documents:



- A commingled document, i.e., one that contains both CUI and CNSI data, **MUST** have `@ism:compliesWith` that contains "USA-CUI", plus some other token in `@ism:compliesWith`, e.g., "USGov" or "USDOD".
- A commingled document **MUST NOT** include any `@ism:nonICcontrols` attributes, pending resolution of where `@ism:nonICcontrols` should appear in a commingled banner.

## 5.6.4 - NTK Rules for Documents Containing CUI

ISM.XML implements two NTK rules for documents that contain CUI.

- If a document is marked with the "PROPIN" CUI Category, then the document **MUST** contain NTK metadata matching the "PROPIN" NTK profile.
- If a document is marked with the "DL\_ONLY" CUI `@ism:disseminationControls` token, then the document **MUST** contain NTK metadata matching the Group and Individual NTK profile.

## 5.6.5 - Notice Rules for Documents Containing CUI

ISM.XML implements two CUI rules that require `@ism:Notice` elements. These `@ism:Notice` requirements are defined in the IC Markings<sup>[28]</sup> and ISM.XML carries them over to the equivalent CUI categories:

- Documents marked with the "LEI" CUI category **MUST** include an "LES" non-external `@ism:Notice`. Note: The `@ism:nonICmarkings` Law Enforcement token is "LES", while the analogous CUI Category is "LEI", but both require `@ism:noticeType="LES"` for consistency.
- Documents marked with the "FISA" CUI category **MUST** include a "FISA" non-external `@ism:Notice`.

## 5.7 - CUI Rendering Stylesheets

ISM.XML provides two rendering stylesheets that support different approaches to formatting CUI markings. These two stylesheets can be called by customer software in agencies that want to select one of the two different ways to render banners, blocks and portion marks for documents marked CUI. These two stylesheets call the ISM stylesheets for the banner, block and portion marks, passing along a parameter that indicates how to render CUI markings. Agencies can call these two stylesheets for all types of documents and data, not just for data marked CUI.

- The "IC-ISM-ISOO-Rendering.xml" stylesheet is used when the customer wants CUI markings rendered according to the ISOO rules documented in the *Marking Controlled Unclassified Information*<sup>[15]</sup>.
  - The *CUI Marking Handbook*<sup>[15]</sup> does not establish a strict format for a CUI block. In fact, the only CUI block information required by CUI policy is the Controlled By line. The *Controlled Unclassified; Final Rule*<sup>[53]</sup> states that a decontrol date or event should be provided, if feasible, but agencies "may do so in any manner that makes the decontrolling schedule readily apparent to an authorized holder."



- ISM.XML rendering of a CUI block using ISOO rules will render lines with information from `@ism:cuiControlledByOffice` and `@ism:cuiPOC` if these attributes exist. Agencies following ISOO rules for CUI do not need to provide these attributes, but the ISM.XML stylesheets will render these attributes if they exist.
- If the “IC-ISM-ISOO-Rendering.xml” stylesheet is used, ISM.XML will **not** render CUI Category markings or dissemination controls in the block.
- The “IC-ISM-DOD-Rendering.xml” stylesheet is used when the customer wants CUI markings rendered according to the DoD rules documented in *DoD Instruction 5200.48* [\[20\]](#).
  - ISM.XML will render the DoD five-lined version of a CUI block. ISM.XML does not require data for all five line; only the `@ism:cuiControlledBy` attribute is required and will be put into the Controlled By line.
  - ISM.XML will always render `@ism:cuiDecontrolDate` and/or `@ism:cuiDecontrolEvent` in the block if either or both of these attributes are available in the document.
  - ISM.XML will render CUI markings in the banner, even if the “IC-ISM-DOD-Rendering.xml” stylesheet is called.
  - ISM.XML will use the unclassified marking “(U)” as a portion marking for unclassified information within CUI documents or materials as required by *DoD Instruction 5200.48* [\[20\]](#), paragraph 3.4b.

Agency software can call one of the two CUI stylesheets, or they can continue to call the existing stylesheets for the banner, block and portion marks. In either case, the calling software passes the value of `@mode` to tell a stylesheet whether to render a banner, block or portion mark. If the agency software calls the banner, block or portion mark stylesheet directly, then any CUI markings will be rendered according to the ISOO rules.

## Chapter 6 - Progressive Validation Using Phases

### 6.1 - Overview

Progressive validation is the validation of constraints in stages rather than validating everything all at once. It is accomplished through the use of phases in Schematron<sup>[69]</sup> and enables workflow by allowing one to run the phases in any order selected. Each Schematron<sup>[69]</sup> rule can have one or more phases associated with it. The phases that currently exist for ISM Schematron<sup>[69]</sup> rules are in the table below.

**Table 25 - ISM Schematron Phases**

Phase	Description
#ALL	The ISM_XML.xsl file will run ALL of the rules.
BANNER	Schematron <sup>[69]</sup> rules that handle constraints on the banner and/or the classification authority block. For example, if the banner is classified, then there must be either <b>@ism:classifiedBy</b> or <b>@ism:derivativelyClassifiedBy</b> on the resource element. A use case for validating with the BANNER phase only is when an ARH is separated from the rest of the document.
PORTION	Schematron <sup>[69]</sup> rules that handle constraints on the portions. For example, if a portion has <b>@ism:disseminationControls="REL"</b> , then the portion must include the attribute <b>@ism:releasableTo</b> .
ROLLUP	Schematron <sup>[69]</sup> rules that handle rollup constraints on the banner. These rules validate that the markings in the banner correctly roll up all the portion marks in the document. For example, if there is any portion with <b>@ism:SCIcontrols="SI"</b> , then the banner must have <b>@ism:SCIcontrols="SI"</b> .
ROLLDOWN	Schematron <sup>[69]</sup> rules that handle rolldown constraints on the portions. These rules validate the existence of markings in portions that are necessary for the banner to be correct. For example, if the banner is <b>"UNCLASSIFIED"</b> , then there cannot be any portions that are <b>"C"</b> , <b>"S"</b> , or <b>"TS"</b> .

Phase	Description
VALUECHECK	Schematron <sup>[69]</sup> rules that handle value checking for elements and/or attributes. The required values may be conditionally dependent on the value of other elements or attributes. For example, if <b>@ism:ownerProducer="USA"</b> , then the value of <b>@ism:classification</b> must be in the CVE "CVerenum-ISMClassificationUS".
TYPECHECK	Schematron <sup>[69]</sup> rules that handle type checking. For example, <b>@ism:createDate</b> must have the schema type date without any timezone.
STRUCTURECHECK	Schematron <sup>[69]</sup> rules that handle XML structure checking such as the existence of an element or attribute. For example, if <b>@ism:atomicEnergyMarkings</b> has "RD" or "FRD", then attributes <b>@ism:declassDate</b> and <b>@ism:declassEvent</b> are not allowed.
INFRASTRUCTURE	Schematron <sup>[69]</sup> rules that handle constraints specific to the validation infrastructure. For example, there are infrastructure rules that identify the version of each CES used by ISM, to ensure that regardless of the CES versions identified in a document, the environment will validate against the latest CES versions, in order to comply with the latest policy.
NON_INFRASTRUCTURE	Schematron <sup>[69]</sup> rules that handle constraints not related to the validation infrastructure. Essentially, every Schematron <sup>[69]</sup> rule is either an INFRASTRUCTURE rule or a NON_INFRASTRUCTURE rule.

Because the rules can have one or more associated Phase(s), it is possible to only run a single phase and still be sure the data or system is valid. The following are couple of examples of possible use cases where you would only run a single phase:

Banner	Sometimes a document is received that does not have portion marks. It may only have classification markings in a banner. In order to check the documents validity, the user would only need to run the BANNER portion. As long as the banner's markings are correct, then the user would be confident that the document is classified appropriately.
Infrastructure	Infrastructure does not change very often. In order to check that the infrastructure is valid, the user would only need to run the INFRASTRUCTURE phase once. Unless changes are made to the infrastructure, the phase would not need to be run again, thus saving time. This is why every ISM.XML Schematron <sup>[69]</sup> rule is either an

INFRASTRUCTURE rule or a NON\_INFRASTRUCTURE rule.  
INFRASTRUCTURE rules only need to be run when the environment changes, whereas NON\_INFRASTRUCTURE rules are the ones that are used to validate individual documents.

Each ISM.XML Schematron<sup>[69]</sup> rule identifies the phases where it is used, in an XML processing instruction. For example, rule “ISM-ID-00012” contains the following XML processing instruction: **<?schematron-phases phaseids="PORTION STRUCTURECHECK"?>**. This processing instruction identifies PORTION and STRUCTURECHECK as the ISM.XML validation phases that invoke rule “ISM-ID-00012”.

The ISM.XML convenience packages contain an “ISM\_Rules.pdf” file. This PDF contains Chapters that list all the ISM.XML Schematron<sup>[69]</sup> rules for each validation phase.

Appendix A Feature Summary

The following tables summarize major features by version for ISM.XML. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, 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<sup>[28]</sup> has an implementation date of one year after issuance).

Table 26 - 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 Feature Summary

A.1.1. Features from V2019-MARr2019-SEP to V2021-NOVr2022-NOV

Table 27 - ISM Feature Comparison V2019-MARr2019-SEP to V2021-NOVr2022-NOV

Driver	Feature	V2019-MARr2019-SEP	V2019-MARr2020-OCT	V2021-NOV	V2021-NOVr2022-NOV
Required Date					
2019-MARr2020-OCT	Add ITAR/EAR warning notice type	N	F	F	F
	Modify ISM, ISM-ACES for August 2019 version of the IC Markings Register and Manual	N	F	F	F
	Controlled Unclassified Information (CUI)	N	N	F	F
	Enterprise Role access profile	N	N	F	F
	Deprecated DoD-Dist-X	N	N	F	F
	Require resourceNode on all arh:Security elements	N	N	F	F
	Add support for a second line classification banner	N	N	F	F
	Add Phases to ISM Schematron	N	N	F	F
2021-NOV	Enabled Out-of-Band Notice in ISM	N	N	F	F
	Change NATO access levels from one to four levels of read-on. Add new highWaterNATO attribute.	N	N	F	F
	Allow attribute values to be unsorted.	N	N	F	F
	Incorporate DOD SAPCO guidance on SAPs	N	N	F	F
	Add Exempt From ICD 501 Discovery dissemination control	N	N	F	F
2022-NOV	Modify SAP values in CVEnumISMSAR.xml to have a "SAR-" prefix	N	N	N	F

A.1.1.1. Features Partial and N/A from V2019-MARr2019-SEP to V2021-NOVr2022-NOV

Table 28 - ISM Feature Comparison V2019-MARr2019-SEP to V2021-NOVr2022-NOV

Driver	Feature	V2019-MARr2019-SEP	V2019-MARr2020-OCT	V2021-NOV	V2021-NOVr2022-NOV
Required Date					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	KDK	N/A	N/A	N/A	N/A
December 10, 2010					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
September 11, 2009					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	P	P	P	P
December 10, 2010					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N/A	N/A	N/A	N/A
March 11, 2011					

A.1.2. Features from 2016-SEPr2018-NOV to V2019-MARr2019-SEP

Table 29 - ISM Feature Comparison 2016-SEPr2018-NOV to V2019-MARr2019-SEP

Driver	Feature	2016-SEPr2018-NOV	V2019-MAR	V2019-MARr2019-JUN	V2019-MARr2019-SEP
Required Date					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	F	P	P	P
December 10, 2010					
March 2019	Merge NTK into ISM	N	F	F	F
	Agency Dissem Profile	N	F	F	F
	Data Sphere Profile	N	F	F	F
	Group & Individual Profile	N	F	F	F
	EXDIS access profile	N	F	F	F
	ICO access profile	N	F	F	F
	License access profile	N	F	F	F
	Mission Need Profile (MN) access profile	N	F	F	F
	NODIS access profile	N	F	F	F
	ORCON access profile	N	F	F	F
	Permissive access profile	N	F	F	F
	PROPIN access profile	N	F	F	F
	Restrictive access profile	N	F	F	F

Driver	Feature	2016-SEPr2018-NOV	V2019-MAR	V2019-MARr2019-JUN	V2019-MARr2019-SEP
Required Date					
	Ability to define custom vocabulary types	N	F	F	F
	Built-in Vocabulary Types	N	F	F	F
	Restricted Authority Category access profile	N	F	F	F
March 2019	Merge ARH into ISM	N	F	F	F
	Support for NATO notice	N	F	F	F
	Support for RC_Dissemination_Control_Required notice	N	F	F	F
September 2019	Support for HCS-X	N	N	N	F

A.1.2.1. Features Partial and N/A from 2016-SEPr2018-NOV to V2019-MARr2019-SEP

Table 30 - ISM Feature Comparison 2016-SEPr2018-NOV to V2019-MARr2019-SEP

Driver	Feature	2016-SEPr2018-NOV	V2019-MAR	V2019-MARr2019-JUN	V2019-MARr2019-SEP
Required Date					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	KDK	N/A	N/A	N/A	N/A
December 10, 2010					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
September 11, 2009					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	F	P	P	P
December 10, 2010					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N/A	N/A	N/A	N/A
March 11, 2011					

A.1.3. Features from V2016-SEPr2017-JUL to 2016-SEPr2018-NOV

Table 31 - ISM Feature Comparison V2016-SEPr2017-JUL to 2016-SEPr2018-NOV

Driver	Feature	V2016-SEPr2017-JUL	V2016-SEPr2018-APR	V2016-SEPr2018-JUL	2016-SEPr2018-NOV
Required Date					
Authorized Classification and Control Markings Register v4.1 <sup>[6]</sup>	HCS subcompartments	P	P	P	F
December 10, 2010					
	Validation of rules for @ism:joint	N	F	F	F
	Support for IMCON_RSEN notice when IMCON and RSEN are used in combination	N	F	F	F
	Support for GEOCAP warning statement requirement with TK compartments/subcompartments	N	F	F	F
	Enforce the IC/DOD Classification Marking Implementation Working Group (CMIWG) policies which require a @ism:declassDate to accompany @ism:declassEvent	N	F	F	F
	Support for KLM	N	N	F	F
	Support for RAW-FISA	N	N	N	F
	Support for KLM-R	N	N	N	F

A.1.3.1. Features Partial and N/A from V2016-SEPr2017-JUL to 2016-SEPr2018-NOV

Table 32 - ISM Feature Comparison V2016-SEPr2017-JUL to 2016-SEPr2018-NOV

Driver	Feature	V2016-SEPr2017-JUL	V2016-SEPr2018-APR	V2016-SEPr2018-JUL	2016-SEPr2018-NOV
Required Date					
Authorized Classification and Control Markings Register v4.1 <sup>[6]</sup>	KDK	N/A	N/A	N/A	N/A
December 10, 2010					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
September 11, 2009					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N/A	N/A	N/A	N/A
March 11, 2011					



A.1.4. Features from V2014-DEC to V2016-SEPr2017-JUL

Table 33 - ISM Feature Comparison V2014-DEC to V2016-SEPr2017-JUL

Driver	Feature	V2014-DEC	V2015-AUG	V2016-SEP	V2016-SEPr2017-JUL
Required Date					
<i>Authorized Classification and Control Markings Register v4.1</i> <sup>[6]</sup>	KDK	F	F	N/A	N/A
December 10, 2010					
<i>Authorized Classification and Control Markings Register v4.1</i> <sup>[6]</sup>	HCS subcompartments	F	F	P	P
December 10, 2010					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	N/A	F	F	F
June 28, 2010					
ICD 710 <sup>[39]</sup>	710 POC	N/A	F	F	F
September 11, 2009					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0, “CAPCO Manual Appendix B NATO Protective Markings Appendix B”</i> <sup>[11]</sup> , Section 4	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	P	F	F	F
Feb 2014					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	50X2, 50X3, 50X4, 50X5, 50X7, 50X8, and 50X9	N	F	F	F
December 2010					
	Use Tetragraph taxonomy to validate tetragraph classification does not violate document classification	N	N	F	F
	Support for approximate markings	N	N	F	F
	Support indicator of absence of aggregation	N	N	F	F
<i>Intelligence Community Markings System Register and Manual 24 December 2015</i> <sup>[31]</sup>	Remove support for HCS-O subcomparments	N	N	F	F
Dec 2016					
<i>Intelligence Community Markings System Register and Manual</i> <sup>[28]</sup> 30 June 2016 <sup>[29]</sup>	Alignment with June 2016 <i>Intelligence Community Markings System Register and Manual</i> <sup>[29]</sup>	N	N	F	F
June 2017					
	Use of fully decomposed tetragraph taxonomy	N	N	N	F

A.1.4.1. Features Partial and N/A from V2014-DEC to V2016-SEPr2017-JUL

Table 34 - ISM Feature Comparison V2014-DEC to V2016-SEPr2017-JUL

Driver	Feature	V2014-DEC	V2015-AUG	V2016-SEP	V2016-SEPr2017-JUL
Required Date					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	KDK	F	F	N/A	N/A
December 10, 2010					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
September 11, 2009					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	F	F	P	P
December 10, 2010					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N/A	N/A	N/A	N/A
March 11, 2011					

A.1.5. Features from V11 to V2014-DEC

Table 35 - ISM Feature Comparison V11 to V2014-DEC

Driver	Feature	V11	V12	V13	V2014-DEC
Required Date					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	F	F	N/A	N/A
September 11, 2009					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N	F	F
June 23, 2013					
ICD 710 <sup>[39]</sup>	710 POC	F	F	N/A	N/A
September 11, 2009					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v6.0 <sup>[3]</sup>	ORCON and ORCON-USGOV may not be used with RELIDO	N	F	F	F
Feb 2014					
<i>Intelligence Community Markings System Register and Manual</i> 31 December 2013 <sup>[33]</sup>	Required compliesWith to support ICD 710 <sup>[39]</sup> Foreign Disclosure and Release changes	N	N	F	F
Feb 2014					
<i>Intelligence Community Markings System Register and Manual</i> 31 December 2013 <sup>[33]</sup>	Support for NATO NACs	N	N	N	F
Feb 2014					

A.1.5.1. Features Partial and N/A from V11 to V2014-DEC

Table 36 - ISM Feature Comparison V11 to V2014-DEC

Driver	Feature	V11	V12	V13	V2014-DEC
Required Date					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	F	F	N/A	N/A
September 11, 2009					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	N/A	N/A	N/A	N/A
June 28, 2010					
ICD 710 <sup>[39]</sup>	710 POC	F	F	N/A	N/A
September 11, 2009					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N/A	N/A	N/A	N/A
March 11, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v6.0, “CAPCO Manual Appendix B NATO Protective Markings Appendix B” <sup>[11]</sup> , Section 4	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	P	P	P	P
Feb 2014					

A.1.6. Features from V8 to V11

Table 37 - ISM Feature Comparison V8 to V11

Driver	Feature	V8	V9	V10	V11
Required Date					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	F	N	N	F
December 10, 2010					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	F	F	N/A	N/A
June 28, 2010					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	F	F	N/A	N/A
March 11, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <sup>[4]</sup>	Allow use of KDK compartments and subcompartments	N	F	F	F
December 30, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <sup>[4]</sup>	Allow use of SI compartments and subcompartments	N	F	F	F

Driver	Feature	V8	V9	V10	V11
Required Date					
December 30, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 “CAPCO Manual Appendix A Non-US Protective Markings Annex A” <a href="#">[12]</a>	Allow use of OSTY Open Skies	N	F	F	F
December 30, 2011					
IC CIO enhance data quality	External Notice	N	F	F	F
DoD Manual 5200.01-R <a href="#">[19]</a>	COMSEC Notice	N	F	F	F
February 2012					
DoD Manual 5200.01-R <a href="#">[19]</a>	Support for NNPI	N	F	F	F
February 2012					
Decouple ISM.XML from the Schema	Informative Schema	N	N	F	F
January 2013					
Decouple ISM.XML from the Schema	Normative Schematron rules and CVEs	N	N	F	F
January 2013					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <a href="#">[4]</a>	Add ENDSEAL system with compartments ECRU and NONBOOK	N	N	F	F
December 2012					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <a href="#">[4]</a>	Limit KDK system compartments to BLUEFISH, IDITAROD and KANDIK	N	P	F	F
December 2013					
ISOO Notice 2013-01 <a href="#">[61]</a> .	Support NATO exemptions to declass date	N	N	F	F
November 2012					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <a href="#">[4]</a>	Support multiple non JOINT countries prior to the Classification	N	N	N	F
December 2013					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v6.0 <a href="#">[3]</a>	Support ORCON-USGOV	N	N	N	F
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v6.0 <a href="#">[3]</a>	Support RD precedence over FRD	N	N	N	F
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v6.0 <a href="#">[3]</a>	Treat caveated UNCLASSIFIED as RELIDO unless explicitly specified	N	N	N	F
Feb 2014					

Driver	Feature	V8	V9	V10	V11
Required Date					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> <sup>[3]</sup>	Allow commingling of SBU and SUB-NF with classified information in portions	N	N	N	F
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> <sup>[3]</sup>	50X1 and 50X6	N	N	N	F
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> , “CAPCO Manual Appendix B NATO Protective Markings Appendix B” <sup>[11]</sup> , Section 4	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	N	N	N	P
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> <sup>[3]</sup>	Allow JOINT classification markings with SCI, SAP, AEA, IC and non-IC Dissemination Control Markings (excluding NOFORN)	N	N	N	F
Feb 2014					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> , “CAPCO Manual Appendix A Non-US Protective Markings Annex A” <sup>[10]</sup> , Enclosure 1	Allow Non-US classification markings with US SCI, SAP, AEA, IC and non-IC Dissemination control markings (excluding NOFORN)	N	N	N	F
Feb 2014					

A.1.6.1. Features Partial and N/A from V8 to V11

Table 38 - ISM Feature Comparison V8 to V11

Driver	Feature	V8	V9	V10	V11
Required Date					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
June 23, 2013					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	F	F	N/A	N/A
June 28, 2010					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	F	F	N/A	N/A
March 11, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v6.0</i> , “CAPCO Manual Appendix B NATO Protective Markings Appendix B” <sup>[11]</sup> , Section 4	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	N	N	N	P
Feb 2014					

A.1.7. Features from V5 to V8

Table 39 - ISM Feature Comparison V5 to V8

Driver	Feature	V5	V6	V7	V8
Required Date					
DoD Manual 5200.01 <sup>[19]</sup>	DoD ACCM Markings	N	F	F	F
January 1997					
<i>Authorized Classification and Control Markings Register</i> v4.2 <sup>[5]</sup>	SSI	N	F	F	F
May 31, 2011					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	TFNI	N	F	F	F
June 28, 2010					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	HCS subcompartments	N	F	F	F
December 10, 2010					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	MCFI Remove	P	F	F	F
November 16, 2010 (date disestablished)					
<i>Authorized Classification and Control Markings Register</i> v4.2 <sup>[5]</sup>	MIFH, EUDA and EFOR removed	P	P	F	F
May 31, 2011					
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	N	N	F	F
June 28, 2010					
IC CIO enhance data quality	SouthSudan	N	N	F	F
See IC ESB					
ICD 710 <sup>[39]</sup>	710 POC	N	N	F	F
September 11, 2009					
DNI ORCON Memo <sup>[64]</sup>	ORCON POC	N	N	F	F
March 11, 2011					
ISOO Marking Booklet <sup>[58]</sup>	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	F	F
December 2010					
IC CIO enhance data quality	RD, FRD, and Sigma rolldown enforced	N	N	N	F
See IC ESB					
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	F
IC CIO enhance data quality					
See IC ESB	@ism:excludeFromRollup=true() allowed to not have an ICD-710 foreign release indicator	N	N	N	F

Driver	Feature	V5	V6	V7	V8
Required Date					
<i>Authorized Classification and Control Markings Register v4.1</i> <sup>[6]</sup>	SINFO Remove	P	P	P	F
December 10, 2011 (1 Year after 4.1)					
<i>Authorized Classification and Control Markings Register v4.1</i> <sup>[6]</sup>	SC Remove	P	P	P	F
December 10, 2011 (1 Year after 4.1)					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v5.1</i> <sup>[4]</sup>	RSV	N	N	N	F
December 30, 2011					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual v5.1</i> <sup>[4]</sup>	Require using 50X1-HUM instead of 25X1-human	P	P	P	F
December 30, 2011					

A.1.7.1. Features Partial and N/A from V5 to V8

Table 40 - ISM Feature Comparison V5 to V8

Driver	Feature	V5	V6	V7	V8
Required Date					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
June 23, 2013					

A.1.8. Features from V2 to V5

Table 41 - ISM Feature Comparison V2 to V5

Driver	Feature	V2	V3	V4	V5
Required Date					
<i>Authorized Classification and Control Markings Register v3.1</i> <sup>[7]</sup>	LES	N	F	F	F
May 7, 2010					
<i>Authorized Classification and Control Markings Register v3.1</i> <sup>[7]</sup>	LES-NF	N	F	F	F
May 7, 2010					
<i>Authorized Classification and Control Markings Register All versions pre 2008</i>	Require Notices	N	F	F	F
Pre 2008					
<i>Authorized Classification and Control Markings Register v4.1</i> <sup>[6]</sup>	KDK	N	F	F	F



Driver	Feature	V2	V3	V4	V5
Required Date					
December 10, 2010					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	P	F	F	F
September 11, 2009					
E.O. 13526 <sup>[24]</sup>	DeclassReasons/Dates	P	F	F	F
December 29, 2009					
IC CIO enhance data quality	Schema validation of values	N	N	F	F
See Intelligence Community Enterprise Standards Baseline (IC ESB)					
DoD Instruction 5230.24 <sup>[16]</sup>	DoD Distro Statements	N	N	F	F
March 18, 1987					
DoD Directive 5240.01 <sup>[17]</sup>	US Person Notice	P	P	P	F
August 27, 2007					
<i>Authorized Classification and Control Markings Register</i> v2.2 <sup>[8]</sup>	Remove SAMI	P	P	P	F
September 25, 2010 (1 Year after 2.2)					
ISOO Marking Booklet 2010 <sup>[58]</sup> / ISOO Notice 2009-13 <sup>[59]</sup>	Remove exempted source	P	P	P	F
December 2010					
E.O. 13526 <sup>[24]</sup>	derivativelyClassifiedBy	P	P	P	F
December 29, 2009					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	Atomic Energy New banner location	N	N	N	F
December 10, 2011 (1 Year after 4.1)					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	Display Only	N	N	N	F
December 10, 2011 (1 Year after 4.1)					
IC CIO enhance data quality	Schematron <sup>[69]</sup> Implementation of rules	N	N	N	F
See IC ESB					
E.O. 13526 <sup>[24]</sup>	50X1-Hum 50X2-WMD	N	N	N	F
December 29, 2009					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <sup>[4]</sup>	Require using 50X1-HUM instead of 25X1-human	N	N	N	P
December 30, 2011					



A.1.8.1. Features Partial and N/A from V2 to V5

Table 42 - ISM Feature Comparison V2 to V5

Driver	Feature	V2	V3	V4	V5
Required Date					
ICD 710 <sup>[39]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A
June 23, 2013					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	MCFI Remove	P	P	P	P
November 16, 2010 (date disestablished)					
<i>Authorized Classification and Control Markings Register</i> v4.2 <sup>[5]</sup>	MIFH, EUDA and EFOR removed	P	P	P	P
May 31, 2011					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	SINFO Remove	P	P	P	P
December 10, 2011 (1 Year after 4.1)					
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup>	SC Remove	P	P	P	P
December 10, 2011 (1 Year after 4.1)					
<i>Intelligence Community Authorized Classification and Control Markings Register and Manual</i> v5.1 <sup>[4]</sup>	Require using 50X1-HUM instead of 25X1-human	N	N	N	P
December 30, 2011					

A.1.9. Features from V1 to V2

Table 43 - ISM Feature Comparison V1 to V2

Driver	Feature	V1	V2
Required Date			
<i>Authorized Classification and Control Markings Register</i> v2.1 <sup>[9]</sup>	Declass Removed from Banner	N	F
January 22, 2009 (1 year after 2008 memo)			
E.O. 13526 <sup>[24]</sup>	Compilation Reason	N	F
December 29, 2009			
<i>Authorized Classification and Control Markings Register</i> v3.1 <sup>[7]</sup>	LES	P	N
May 7, 2010			
<i>Authorized Classification and Control Markings Register</i> v3.1 <sup>[7]</sup>	LES-NF	P	N
May 7, 2010			
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[51]</sup>	Multivalue declassException	F	N
June 28, 2010			

A.1.9.1. Features Partial and N/A from V1 to V2

Table 44 - ISM Feature Comparison V1 to V2

Driver	Feature	V1	V2
Required Date			
ICD 710 <sup>[39]</sup> September 11, 2009	710 Foreign Disclosure or Release	P	P
ICD 710 <sup>[39]</sup> June 23, 2013	710 Foreign Disclosure or Release	N/A	N/A
E.O. 13526 <sup>[24]</sup> December 29, 2009	DeclassReasons/Dates	P	P
DoD Directive 5240.01 <sup>[17]</sup> August 27, 2007	US Person Notice	P	P
<i>Authorized Classification and Control Markings Register</i> v2.2 <sup>[8]</sup> September 25, 2010 (1 Year after 2.2)	Remove SAMI	P	P
ISOO Marking Booklet 2010 <sup>[58]</sup> / ISOO Notice 2009-13 <sup>[59]</sup> December 2010	Remove exempted source	P	P
E.O. 13526 <sup>[24]</sup> December 29, 2009	derivativelyClassifiedBy	P	P
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup> November 16, 2010 (date disestablished)	MCFI Remove	P	P
<i>Authorized Classification and Control Markings Register</i> v4.2 <sup>[5]</sup> May 31, 2011	MIFH, EUDA and EFOR removed	P	P
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup> December 10, 2011 (1 Year after 4.1)	SINFO Remove	P	P
<i>Authorized Classification and Control Markings Register</i> v4.1 <sup>[6]</sup> December 10, 2011 (1 Year after 4.1)	SC Remove	P	P

## Appendix B Change History

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

**Table 45 - DES Version Identifier History**

Version	Date	Purpose
1	August 2008	Initial Release
2	December 24, 2009	Routine revision to technical specification. For details of changes, see <a href="#">Section B.25 - V2 Change Summary</a>
3	June 4, 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.24 - V3 Change Summary</a>
4	September 7, 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.23 - V4 Change Summary</a>
5	December 6, 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.22 - V5 Change Summary</a>
6	April 11, 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.21 - V6 Change Summary</a>
7	August 9, 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.20 - V7 Change Summary</a>
8	February 27, 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.19 - V8 Change Summary</a>
9	July 17, 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.18 - V9 Change Summary</a>
10	January 21, 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.17 - V10 Change Summary</a>
11	April 5, 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.16 - V11 Change Summary</a>
12	August 16, 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.15 - V12 Change Summary</a>
13	March 14, 2014	Routine revision to technical specification. For details of changes, see <a href="#">Section B.14 - V13 Change Summary</a>

Version	Date	Purpose
2014-DEC	December 4, 2014	Routine revision to technical specification. For details of changes, see <a href="#">Section B.13 - V2014-DEC Change Summary</a>
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see <a href="#">Section B.12 - V2015-AUG Change Summary</a>
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see <a href="#">Section B.11 - V2016-SEP Change Summary</a>
2016-SEPr2017-JUL	July 21, 2017	Routine revision to technical specification. For details of changes, see <a href="#">Section B.10 - V2016-SEPr2017-JUL Change Summary</a>
2016-SEPr2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see <a href="#">Section B.9 - V2016-SEPr2018-APR Change Summary</a>
2016-SEPr2018-JUL	July 31, 2018	Routine revision to technical specification. For details of changes, see <a href="#">Section B.8 - V2016-SEPr2018-JUL Change Summary</a>
2016-SEPr2018-NOV	November 26, 2018	Routine revision to technical specification. For details of changes, see <a href="#">Section B.7 - V2016-SEPr2018-NOV Change Summary</a>
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.6 - V2019-MAR Change Summary</a>
2019-MARr2019-JUN	June 19, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.5 - V2019-MARr2019-JUN Change Summary</a>
2019-MARr2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - V2019-MARr2019-SEP Change Summary</a>
2019-MARr2020-OCT	October 1, 2020	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V2019-MARr2020-OCT Change Summary</a>
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V2021-NOV Change Summary</a>
2021-NOVr2022-NOV	November 29, 2022	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2021-NOVr2022-NOV Change Summary</a>

## B.1 - V2021-NOVr2022-NOV Change Summary

Significant drivers for version 2021-NOVr2022-NOV include:

- ODNI Special Programs
- DOD SAPCO.

[Table 46](#) summarizes the changes made to this technical specification from version 2021-NOV to version 2021-NOVr2022-NOV.

**Table 46 - Data Encoding Specification 2021-NOVr2022-NOV Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Modify SAP values in CVEnum-ISMSAR.xml to have a "SAR-" prefix (CR-2022-029)	<p>Documentation</p> <p>CVEnumISMSAR.xml modified</p> <p>Schematron:</p> <ul style="list-style-type: none"> <li>• ISM-ID-00527 modified</li> <li>• ISM-ID-00529 modified</li> <li>• ISM-ID-00530 modified</li> <li>• ValidateTokenValuePrefixesExistenceInList.sch</li> <li>• ISM-ID-00534 modified</li> </ul> <p>Rendering stylesheets:</p> <ul style="list-style-type: none"> <li>• IC-ISM-PortionMark.xsl modified</li> <li>• IC-ISM-SecurityBanner modified</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• SAR-classified-1.xml modified</li> </ul>	Data systems must change their representation of SARs.

## B.2 - V2021-NOV Change Summary

Significant drivers for version 2021-NOV include:

- CMIWG
- ODNI Special Programs
- DOD SAPCO.

[Table 47](#) summarizes the changes made to this technical specification from version 2019-MARr2020-OCT to version 2021-NOV.

**Table 47 - Data Encoding Specification 2021-NOV Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated DoD 5200.1 citations to 5200.01. (CR-2020-033)	Documentation	No impact to systems.
2	Add Enterprise Role access profile into ISM for ALEP attribute (CR-2019-013)	Documentation CVENTKAccessPolicy CVENTKProfileDes Schematron ISM-ID-00477 added ISM-ID-00489 added ISM-ID-00490 added ISM-ID-00508 added ISM-ID-00509 added	Systems need to be updated to accommodate this change.
3	Add phases to schematron validation; move schematron variable declarations from TypeConstraintPatterns library to main schematron file (CR-2019-104, CR-2019-012)	Documentation Schematron ISM_XML.sch modified TypeConstraintPatterns.sch deleted	Systems need to be updated to accommodate this change.
4	Updated ISM rule to check USAgency version (CR-2019-161)	Schematron ISM-ID-00436 modified	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
5	Incorporate CUI into ISM (CR-2019-101, CR-2021-035)	Documentation Schema CVCEnumISM CUI Basic added CVCEnum-ISM CUI Specified added CVCEnum-ISM Dissem Commingled added CVCEnumISM Dissem Cui added CVCEnumISM Dissem lcrm added CVCEnum-ISM Complies With modified CVCEnumISM Dissem modified CVCEnumISM Notice modified CVCEnumISM Attributes modified Schematron ISM-ID-00012 modified ISM-ID-00139 modified ISM-ID-00150 modified ISM-ID-00151 modified ISM-ID-00352 modified ISM-ID-00475 added ISM-ID-00476 added ISM-ID-00478 added	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00479 added	
		ISM-ID-00480 added	
		ISM-ID-00481 added	
		ISM-ID-00482 added	
		ISM-ID-00483 added	
		ISM-ID-00484 added	
		ISM-ID-00485 added	
		ISM-ID-00486 added	
		ISM-ID-00487 added	
		ISM-ID-00488 added	
		ISM-ID-00491 added	
		ISM-ID-00492 added	
		ISM-ID-00493 added	
		ISM-ID-00494 added	
		ISM-ID-00495 added	
		ISM-ID-00496 added	
		ISM-ID-00497 added	
		ISM-ID-00498 added	
		ISM-ID-00499 added	
		ISM-ID-00500 added	
		ISM-ID-00501 added	
		ISM-ID-00502 added	
		ISM-ID-00503 added	
		ISM-ID-00504 added	
		ISM-ID-00505 added	
		ISM-ID-00506 added	



#	Change	Artifacts changed	Compatibility Notes
6	Require resourceNode on all arh:Security elements (CR-2019-166)	Documentation Schema ISM-ID-00510 added ISM-ID-00511 added	Systems need to be updated to accommodate this change
7	Add support for a second line classification banner (CR-2019-102)	Documentation Schema CVENum-ISMSecondBannerLine.xml controlled vocabulary added ISM formatting stylesheet for banner modified Schematron ISM-ID-00512 added ISM-ID-00513 added ISM-ID-00514 added ISM-ID-00515 added ISM-ID-00516 added ISM-ID-00517 added	Systems need to be updated to accommodate this change
8	Add Phases to ISM Schematron rules to enable validation of only portions, only environment, etc. (CR-2019-104)	Schematron	Systems need to be updated to accommodate this change.
9	Fix Saxon warnings by updating ISM XSL functions that computes atomic values to using xsl:sequence rather than xsl:value-of (CR-2020-008)	Schematron	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
10	Removed Rules made obsolete by XSLT sorting. (CR-2020-004)	Schematron ISM-ID-00026 deleted ISM-ID-00035 deleted ISM-ID-00041 deleted ISM-ID-00042 deleted ISM-ID-00095 deleted ISM-ID-00096 deleted ISM-ID-00100 deleted ISM-ID-00121 deleted ISM-ID-00167 deleted ISM-ID-00178 deleted	Systems need to be updated to accommodate this change.
11	Enabled Out-of-Band Notices in ISM. (CR-2020-001)	Documentation Schema CVEnum-ISMNoticeProse.xml added CVEnum-ISMAAttributes.xml modified Schematron ISM-ID-00518 added ISM-ID-00519 added	Systems need to be updated to accommodate this change.
12	Added DESVersion warning enforcement rules (CR-2021-001)	Schematron ISM-ID-00520 added	No impact to systems.
13	Add new entries to CUI list of limited dissemination controls (CR-2020-032)	CVEnumISMDissem.xml and related CVEnum-ISMDissem CVEs modified Schematron ISM-ID-00507 added	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
14	Create Better ISM Examples & Use Cases with Textual Paragraphs (CR-2020-045)	Examples modified	No impact to systems.
15	Roll-Up Rules for Unclass Doc w/ U//REL Portion (CR-2018-061)	Schematron ISM-ID-00521 added	Systems need to be updated to accommodate this change.
16	FAC.CES <sup>[26]</sup> was updated to have four read-on values for NATO instead of just one: NATO-R, NATO-C, NATO-S and NATO-TS. This required the creation of a new <b>@ism:highWaterNATO</b> attribute along with Schematron rules for the new attribute. (CR-2020-005)	Documentation  Schema  CVCEnum-ISMhighWaterNATO added  Schematron  ISM-ID-00522 added  ISM-ID-00523 added  ISM-ID-00524 added  ISM-ID-00525 added  ISM-ID-00526 added	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
17	Modify handling of SAP accesses to support DOD SAPCO rules. (CR-2021-024)	Documentation CVerumISMSAR modified  CVerum-ISMSARAuthorities added  Schematron ISM-ID-00527 added ISM-ID-00529 added ISM-ID-00530 added ISM-ID-00531 added ISM-ID-00532 added ISM-ID-00533 added ISM-ID-00534 added ISM-ID-00535 added	Systems need to be updated to accommodate this change.
18	Add Exempt From ICD 501 Discovery dissemination control (CR-2021-026)	Documentation CVerumISMDissem modified  CVerum-ISMDissemCommingled modified  CVerumISMDissemCUI modified  CVerumISMDissemIcrm modified  Schematron ISM-ID-00528 added	Systems need to be updated to accommodate this change.
19	Removed ACSS PKI CA from ISM (CR-2021-021)	Documentation	Systems need to be updated to accommodate this change.
20	Document deviations from policy in ISM DES (CR-2021-028)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
21	Fixed code in ISM 376 to correctly check the tetratoken and not the overall tetragraph for the releasability (CR-2021-039)	Schematron ISM-ID-00376 modified	Systems need to be updated to accommodate this change.

### B.3 - V2019-MARr2020-OCT Change Summary

Significant drivers for version V2019-MARr2020-OCT include:

- CMIWG
- ODNI Special Programs

[Table 48](#) summarizes the changes made to this technical specification from version 2019-MARr2019-SEP to version V2019-MARr2020-OCT.

#### Table 48 - Data Encoding Specification V2019-MARr2020-OCT Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Add ITAR/EAR warning notice type to ISM to align with DoDI 5230.24 Change 3, dated October 15, 2018(CR-2019-103)	CVEnumISMNotice Schematron ISM-ID-00460 added ISM-ID-00461 added ISM-ID-00227 modified	Systems need to be updated to accommodate this change.
2	Deprecate DoD Distribution Statement X in ISM (CR-2019-131)	CVEnumISMNotice CVEnumISMPocType Schematron ISM-ID-00155 modified ISM-ID-00162 modified ISM-ID-00227 modified ISM-ID-00237 modified ISM-ID-00238 modified	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
3	Created a rule to forbid the use of ACCM when ism:classification='U' (CR-2019-162)	Schematron ISM_XML.sch modified ISM-ID-00462 added	Systems need to be updated to accommodate this change.
4	Updated ISM rule to ensure Joint documents have releaseableTo properly decomposed (CR-2019-174)	Schematron ISM-ID-00377 modified	Systems need to be updated to accommodate this change.
5	Add ISM resource level unclassified examples to show how to mark up classified information (CR-2015-085)	Examples	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
6	Modified for August 2019 Register and Manual: Changes to SCI Controls: BUR, HCS, KLM, MARVEL, and RSV. Change to PROPIN access policy. Added 75X declassification exemption to vocabulary for <b>@ism:declassException</b> . Allowed multiple tokens in <b>@ism:declassException</b> . (CR-2019-163)	Documentation  Schema  CVerenum-ISMSCIControls.xml modified  CVerenumISM25X.xml modified  Schematron  ISM-ID-00048 modified  ISM-ID-00277 modified  ISM-ID-00393 modified  ISM-ID-00463 added  ISM-ID-00464 added  ISM-ID-00465 added  ISM-ID-00466 added  ISM-ID-00467 added  ISM-ID-00468 added  ISM-ID-00469 added  ISM-ID-00470 added  ISM-ID-00471 added  ISM-ID-00472 added  ISM-ID-00473 added  ISM-ID-00474 added	Systems need to be updated to accommodate this change
7	ISM banner builder incorrectly handles RAWFISA (CR-2020-007)	CVE  CVerenumISMDissem.xml	Systems need to be updated to accommodate this change
8	Remove regex in Atomic Energy CVE. (CR-2020-010).	CVE  CVerenum-ISMAAtomicEnergyMarkings	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
9	ISM XSL Rendering ACCM incorrectly. (CR-2020-003).	XSLT version 1 stylesheets	Systems need to be updated to accommodate this change.
10	Update DES guidance/rules for portion marking. (CR-2019-011).	Documentation	Systems may need to be updated to accommodate this change.
11	Change sub-compartment to subcompartment for ISM and ISM-ACES. (CR-2020-015).	Documentation	No impact to systems.
12	Removed one dissemination control. (CR-2020-018).	CVEnumISMDissem.xml modified Documentation Schematron ISM-ID-00390 deleted ISM-ID-00395 deleted	Systems may need to be updated to accommodate this change.
13	Change Rule ISM-ID-00474 Require HCS Compartments to Warning. (CR-2020-019).	ISM-ID-00474 modified	Systems may need to be updated to accommodate this change.

## B.4 - V2019-MARr2019-SEP Change Summary

Significant drivers for version 2019-MARr2019-SEP include:

- CMIWG
- ODNI Special Programs

[Table 49](#) summarizes the changes made to this technical specification from version 2019-MARr2019-JUN to version 2019-MARr2019-SEP.

**Table 49 - Data Encoding Specification 2019-MARr2019-SEP Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Add HCS-X to SCIcontrls (CR-2019-078)	CVEnumISMSCIcontrls Schematron ISM-ID-00459 added	Systems need to be updated to accommodate this change.
2	Update libraries to render rule numbers (CR-2019-085)	Schematron	No impact to systems. Users will get better error messages.



#	Change	Artifacts changed	Compatibility Notes
3	Update SCIControls CVE per requirements from Special Programs (CR-2019-090)	CVEnumISMSCIControls	Systems need to be updated to accommodate this change.
4	ISM-ID-00436 checks the specVersion on the MN and LIC CVEs against the version declared in the document. Change rule from error to warning to match the behavior of the checking for other version attributes. (CR-2019-063)	Schematron ISM-ID-00436 modified.	Systems need to be updated to accommodate this change.
5	Updated rule documentation to remove use of “we” (CR-2019-020)	Schematron ISM-ID-00449 modified ISM-ID-00451 modified	No impact to systems.

## B.5 - V2019-MARr2019-JUN Change Summary

Significant drivers for Version 2019-MARr2019-JUN include:

- Schematron bug fixes

The following table summarizes the changes made to 2019-MAR in developing 2019-MARr2019-JUN.

**Table 50 - Data Encoding Specification 2019-MARr2019-JUN Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Fix GEOCAP notice check. (CR-2019-070).	Schematron ISM-ID-00387 modified	Systems need to be updated to accommodate this change.
2	Fix Tetragraph releasability check. (CR-2019-076).	Schematron ISM-ID-00358 modified	Systems need to be updated to accommodate this change.

## B.6 - V2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Community Change Requests CR-2019-070

The following table summarizes the changes made to 2016-SEPr2018-JUL in developing 2019-MAR.

**Table 51 - Data Encoding Specification 2019-MAR Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Cleanup obsolete rules after ARH.XML and NTK.XML consolidation into ISM.XML (CR-2018-095).	Schematron ISM-ID-00366 deleted.	Systems need to be updated to accommodate this change.
2	Merge ARH.XML and NTK.XML documentation into ISM.XML documentation. (CR-2018-095, CR-2018-067, CR-2018-007, CR-2017-238, CR-2017-108)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
3	Merge ARH.XML, ISM.XML and NTK.XML schematron into ISM.XML. (CR-2018-095, CR-2017-100, CR-2017-210)	Schematron ISM-ID-00399 added. ISM-ID-00400 added. ISM-ID-00401 added. ISM-ID-00402 added. ISM-ID-00403 added. ISM-ID-00404 added. ISM-ID-00405 added. ISM-ID-00406 added. ISM-ID-00407 added. ISM-ID-00408 added. ISM-ID-00409 added. ISM-ID-00410 added. ISM-ID-00411 added. ISM-ID-00412 added. ISM-ID-00413 added. ISM-ID-00414 added. ISM-ID-00415 added. ISM-ID-00416 added. ISM-ID-00417 added. ISM-ID-00418 added. ISM-ID-00419 added. ISM-ID-00420 added. ISM-ID-00421 added. ISM-ID-00422 added. ISM-ID-00423 added.	Data generation and ingestion systems need to be updated to accommodate the changes.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00424 added.	
		ISM-ID-00425 added.	
		ISM-ID-00426 added.	
		ISM-ID-00427 added.	
		ISM-ID-00428 added.	
		ISM-ID-00429 added.	
		ISM-ID-00430 added.	
		ISM-ID-00431 added.	
		ISM-ID-00432 added.	
		ISM-ID-00433 added.	
		ISM-ID-00434 added.	
		ISM-ID-00435 added.	
		ISM-ID-00436 added.	
		ISM-ID-00437 added.	
		ISM-ID-00438 added.	
		ISM-ID-00439 added.	
		ISM-ID-00440 added.	
		ISM-ID-00449 added.	
		ISM-ID-00450 added.	
		ISM-ID-00451 added.	
		ISM-ID-00452 added.	
		ISM-ID-00453 added.	
		ISM-ID-00454 added.	
		ISM-ID-00455 added.	
		ISM-ID-00456 added.	
		ISM-ID-00457 added.	

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00458 added.	
4	Add NATO to ISM.XML Notice CVE. (CR-2018-002)	CVE CVEnumISMNotice modified	Data generation and ingestion systems need to be updated to accommodate the changes.
5	Add ISM rule to enforce HCS-P subcompartments being TS. (CR-2018-114)	Schematron ISM-ID-00453 added	Data generation and ingestion systems need to be updated to accommodate the changes.
6	Update ISM-ID-00316 updated to require a NATO declass exemption for documents containing FGI NATO at the resource/banner level. (CR-2018-003)	Schematron ISM-ID-00316 modified	Data generation and ingestion systems need to be updated to accommodate the changes.
7	Update ISM-ID-00142 updated to allow the rule to fire on all elements that have <code>@ism:resourceElement="true"</code> . (CR-2018-076)	Schematron ISM-ID-00142 modified	Data generation and ingestion systems need to be updated to accommodate the changes.
8	Added ISM.XML attributes to incorporated ARH.XML Schematron files to mark up the documentation. (CR-2017-293)	Schematron	No impact to systems.
9	Added <code>@id</code> and <code>@role</code> to all <code>sch:rule</code> elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-217)	Schematron	No impact to existing systems. Additional capabilities.
10	Changed "Multipurpose Internet Mail Extensions" to "Media Type". (CR-2018-051)	Documentation	No impact to systems.
11	Updated documentation to use the specification framework. (CR-2018-126)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
12	Create new rules to verify that IMC, RSEN, and IMCON_RSEN notices all require the proper types of data be present. This required refactoring a library that had minor impact on several rules.(CR-2017-009)	Schematron NoticeHasCorresponding Data modified ISM-ID-00441 added ISM-ID-00442 added ISM-ID-00443 added ISM-ID-00444 added ISM-ID-00135 modified ISM-ID-00136 modified ISM-ID-00139 modified ISM-ID-00151 modified ISM-ID-00153 modified ISM-ID-00357 modified	Data generation and ingestion systems need to be updated to accommodate the changes if they were using the notices incorrectly.
13	Update min version rules to check infrastructure instead of instance documents (CR-2018-133)	Schematron ValidateValidationEnvCVE added ValidateValidationEnvSchema added ISM-ID-00445 added ISM-ID-00446 added ISM-ID-00447 added ISM-ID-00448 added ISM-ID-00375 modified ISM-ID-00322 removed	Validation systems need to ensure they are compliant with min versions.
14	Removed the Dependency Over Time table. (CR-2018-152)	Documentation	No impact to systems.
15	Added clarification for validation when ISM.XML elements are extracted for validation. (CR-2019-001)	Documentation	Validation systems extracting ISM.XML elements need to be updated.

#	Change	Artifacts changed	Compatibility Notes
16	Added new registered @ism:noticeType for "RC_Dissemination_Control_Required". (CR-2018-141)	CVE CVENumISMNotice modified	Data generation and ingestion systems need to be updated to accommodate the changes.
17	Update for new control system. (CR-2018-136)	CVE CVENum-ISMSCIControls.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.

## B.7 - V2016-SEPr2018-NOV Change Summary

Significant drivers for Version 2016-SEPr2018-NOV include:

- CMIWG

The following table summarizes the changes made to 2016-SEPr2018-JUL in developing 2016-SEPr2018-NOV.

**Table 52 - Data Encoding Specification 2016-SEPr2018-NOV Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Add RAW-FISA (CR-2018-135)	CVE CVENumISMDissem.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Update for new control system. (CR-2018-137)	CVE CVENum-ISMSCIControls.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.
3	Update for KLM-R to ISM. (CR-2018-137)	CVE CVENum-ISMSCIControls.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Fix validity of JSON-LD CVEs. (CR-2018-143)	CVE	Data generation and ingestion systems using JSON need to be updated to accommodate the changes.

## B.8 - V2016-SEPr2018-JUL Change Summary

Significant drivers for Version 2016-SEPr2018-JUL include:

- CMIWG

The following table summarizes the changes made to 2016-SEPr2017-APR in developing 2016-SEPr2018-JUL.

**Table 53 - Data Encoding Specification 2016-SEPr2018-JUL Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Add KLM to ISM. (CR-2018-109)	CVE  CVerenum- ISMSCIControls.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.

## B.9 - V2016-SEPr2018-APR Change Summary

Significant drivers for Version 2016-SEPr2018-APR include:

- Community Change Requests
- CMIWG

The following table summarizes the changes made to 2016-SEPr2017-JUL in developing 2016-SEPr2018-APR.

**Table 54 - Data Encoding Specification 2016-SEPr2018-APR Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added validation of rules for @ism:joint. (CR-2017-148)	Schematron  ISM-ID-00382 added  ISM-ID-00383 added	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Create RelaxNG CVE Fragments for ISM. (CR-2017-177)	CVEs	No impact to systems.



#	Change	Artifacts changed	Compatibility Notes
3	Added IMCON_RSEN notice for when both IMCON and RSEN are used in combination. (CR-2016-055)	CVE CVEnumISMNotice.xml modified Schematron DataHasCorrespondingNotice modified ISM-ID-00127 modified ISM-ID-00129 modified ISM-ID-00130 modified ISM-ID-00134 modified ISM-ID-00137 deleted ISM-ID-00152 modified ISM-ID-00356 modified ISM-ID-00384 added	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Added GEOCAP warning statement that is required with any TK compartments and subcompartment. (CR-2017-263)	CVE CVEnumISMNotice.xml modified Schematron DataHasCorrespondingNoticeWithRegex added NoticeHasCorrespondingDataWithRegex added ISM-ID-00386 added ISM-ID-00387 added	Data generation and ingestion systems need to be updated to accommodate the changes.
5	Corrected seven schematron rules with empty @role attribute. (CR-2017-266)	Schematron	Data generation and ingestion systems need to be updated to accommodate the changes.
6	Updated portion mark stylesheet to properly handle FGI protected information commingled with US classified information. (CR-2017-284)	IC-ISM-PortionMark.xsl	Data rendering systems need to be updated to use the latest rendering logic.

#	Change	Artifacts changed	Compatibility Notes
7	Created new rule to enforce the IC/DOD CMIWG policies <sup>a</sup> which require a declassDate to accompany declassEvent. (CR-2017-274)	Schematron ISM-ID-00385 added ISM-ID-00329 deleted	Data generation and ingestion systems need to be updated to accommodate the changes.
8	Correct rollup rules relating to deprecated tetragraphs. (CR-2017-275)	Schematron ISM-XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes.
9	Create generalized schematron rule for ensuring all SCI compartments specify their Control System and all SCI subcompartments specify their compartment. This eliminates several custom rules and reduces need for new rules. (CR-2017-322)	Schematron ISM-ID-00388 added ISM-ID-00186 deleted ISM-ID-00187 deleted ISM-ID-00241 deleted ISM-ID-00304 deleted ISM-ID-00305 deleted ISM-ID-00306 deleted ISM-ID-00307 deleted ISM-ID-00308 deleted ISM-ID-00309 deleted ISM-ID-00310 deleted ISM-ID-00311 deleted ISM-ID-00331 deleted ISM-ID-00333 deleted	Data generation and ingestion systems already properly marking will have no impact.
10	Updated CESVersion and DESVersion attributes to generic regex in the schema (CR-2017-340)	Schema	No impact to systems.
11	Added schema PDF. (CR-2018-032)	Documentation	No impact to systems.
12	Added XSL PDF. (CR-2018-033)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
13	Added ISM.XML attributes to Schematron files to mark up the documentation. (CR-2017-306)	Schematron	No impact to systems.
14	Updated section on Understanding Access Control to more accurately represent all of the specifications that participate in access control decisions. (CR-2018-071)	Documentation	No impact to systems.
15	Removed deprecation date from EYES as the CMIWG approved it being a mark until some future date when the marking owner may ask again for it to be withdrawn. (CR-2018-077)	CVE	Systems needing EYES should no longer be impacted by the passing of date based deadlines.
16	Updated CSV generation to include a column for deprecation date information. (CR-2018-091)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.

<sup>a</sup>During the September 2017 CMIWG meeting the DoD representative and the CMIWG chair agreed with a recommendation from ISOO to required dates on all events. This is to be further promulgated in the next version of the IC Markings System Register and Manual which, as of May 2018, has not yet been published.

## B.10 - V2016-SEPr2017-JUL Change Summary

Significant drivers for Version 2016-SEPr2017-JUL include:

- Community Change Requests
- Alignment with December 2016 *Intelligence Community Markings System Register and Manual* <sup>[30]</sup>
- Alignment with DoD Manual 5200.01 <sup>[19]</sup>

The following table summarizes the changes made to 2016-SEP in developing 2016-SEPr2017-JUL.

**Table 55 - Data Encoding Specification 2016-SEPr2017-JUL Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Moving ECRU and NONBOOK as subcompartments under SI and handling the removal of ENDSEAL (CR-2015-097)	CVEs CVEnum-sISMSCIControls.xml Schematron ISM-ID-00301 deleted ISM-ID-00310 modified ISM-ID-00311 modified	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Align ACCM value ordering per DoD Manual 5200.1 volume 2 (CR-2016-065)	CVEs CVEnumISMNonIC.xml Schematron ISM_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
3	Create JSON version of CVEs in ISM (CR-2017-058)	CVEs	No impact to systems.
4	Create CSV version of CVEs in ISM (CR-2017-036)	CVEs	No impact to systems.
5	Updated ISM to use fully decomposed/denormalized ISMCAT tetragraph CVE(CR-2017-008)	Schematron ISM_XML.sch modified	No impact to systems.
6	Updated DESVersion enforcement rule to be warning (CR-2017-085)	Schematron ISM-ID-00300 modified ISM_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.
7	Added ISM rule that enforces members of ownerProducer are in releasableTo when joint=true (CR-2017-073)	Schematron ISM-ID-00377 added ISM_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.
8	Added ISM rule which ensures that Joint is a boolean value (CR-2017-103)	Schematron ISM-ID-00378 added ISM_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.

#	Change	Artifacts changed	Compatibility Notes
9	Add/Update rule and code descriptions for CheckCommonCountries Rules and Schematron (CR-2017-106)	Schematron ISM-ID-00320 modified ISM-ID-00318 modified CheckCommonCountries.sch modified	No impact to systems.
10	Updated the rule description of ISM-ID-00318 to show that the rule decomposes most Tetragraphs. (CR-2017-005)	Schematron ISM-ID-00318 modified	No impact to systems.
11	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-116, CR-2017-199)	Documentation	No impact to systems.
12	Timezone information no longer permitted on declassDate and noticeDate. (CR-2017-161)	Schema Schematron ISM-ID-00379 added ISM-ID-00380 added ISM_XML.sch modified	Systems need to be updated to enforce the new restriction.
13	Add declassException values [NATO], [AEA] and [NATO-AEA] to the list of values that must not be combined with declassDate and declassEvent. (CR-2017-001)	Schematron ISM-ID-00133 modified	Data generation and ingestion systems need to be updated to accommodate the changes to the rules.
14	Add rule that enforces USGov when USIC or USDOD is specified. (CR-2017-003)	Schema Schematron ISM-ID-00381 added ISM_XML.sch modified	Systems need to be updated to enforce the new restriction.
15	Updated rule description of ISM-ID-00066 to include DISPLAYONLY and FOUO. (CR-2017-007)	Schematron ISM-ID-00066 modified	Data generation and ingestion systems need to be updated to enforce the new rule.

#	Change	Artifacts changed	Compatibility Notes
16	Update ISM rules to fully account for sensitivity of ISMCAT tetras preventing portions or documents from being under classified based on the Tetra. (CR-2016-070)	Schematron ISM-ID-00358 modified ISM-ID-00359 modified ISM-ID-00360 modified	Data generation and ingestion systems need to be updated to enforce the new rule.
17	Corrected decomposition of tetragraph memberships to account for members of organizations that can also be decomposed. (CR-2017-008)	Schematron ISM_XML.sch modified ISM-ID-00375 added	
18	Corrected issues with ISM identified in work on ISMv13-r2017-JAN. Includes updating deprecation date of EYES Dissemination control to 11-01-2017 (CR-2017-018)	Schematron ISM-ID-00300 modified ISM-ID-00322 modified ISM-ID-00376 added CVEs CVEnumISMDissem modified	Data generation and ingestion systems need to be updated to enforce the new rule.
19	Corrected boolean tests in schematron. Boolean values are being tested against a string value (e.g., "true") and not a boolean value (e.g., true()) (CR-2017-138)	Schematron ISM_XML.sch modified ISM-ID-00150 modified ISM-ID-00239 modified ISM-ID-00240 modified ISM-ID-00248 modified ISM-ID-00358 modified ISM-ID-00359 modified ISM-ID-00360 modified ISM-ID-00364 modified ISM-ID-00376 modified ISM-ID-00377 modified	Data generation and ingestion systems need to be updated to enforce the new rule.

#	Change	Artifacts changed	Compatibility Notes
20	Updated descriptions in schema for both LongStringType and ShortStringType (CR-2017-150)	Schema	Documentation update only. No impact to systems.
21	Added the revision constraint section since this is the first revision of ISM.	Documentation	Data generation and ingestion systems will may need to be updated to properly validate against the right revisions of specifications.
22	Removed erroneous value-of text from error text (CR-2017-196)	Schematron ISM-ID-00066 modified	No impact to data generation and ingestion systems. Solely an update to error text output.
23	Updated reference to the <i>Intelligence Community Markings System Register and Manual</i> <sup>[30]</sup> . (CR-2017-200)	Documentation	Documentation update only. No impact to systems.
24	Updated rule description for ISM-ID-00278. (CR-2017-203)	Schematron ISM-ID-00278 modified	No impact to data generation and ingestion systems. Solely an update to error text output.
25	Updated rule documentation to remove use of “we”. (CR-2017-214)	Schematron ISM-ID-00330 modified ISM-ID-00332 modified ISM_XML.sch modified	No impact to systems.
26	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-216)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
27	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-237)	Documentation	No impact to systems.
28	Modified cardinality rendering. (CR-2016-080)	CVEs	No impact to existing systems, documentation rendering change only.

## B.11 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests
- Alignment with December 2015 *Intelligence Community Markings System Register and Manual*<sup>[31]</sup>

The following table summarizes the changes made to 2015-AUG in developing 2016-SEP.

**Table 56 - Data Encoding Specification 2016-SEP Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Use the tetragraph taxonomy from ISMCAT in rollup validation processes (CR-2015-091, CR-2015-093, CR-2015-096)	Schematron ISM-ID-00358 added ISM-ID-00359 added ISM-ID-00360 added ISM-ID-00320 updated	Data generation and ingestion systems need to be updated to enforce the new rule.
2	Added new attribute <b>@ism:hasApproximateMarkings</b> (CR-2015-050)	DES Schema CVCEnumISMAttributes Schematron ISM-ID-00361 added	Data generation and ingestion systems need to be updated to enforce the new rule.
3	Added new attribute <b>@ism:noAggregation</b> (CR-2015-084)	DES Schema Schematron ISM-ID-00364 added ISM-ID-00365 added	Data generation and ingestion systems need to be updated to enforce the new rule.
4	Added RSEN to CVCEnum-ISMNotice so that it can be used with the <b>@ism:noticeType</b> attribute. (CR-2016-059)	CVCEnumISMNotice	None
5	Removed Schematron rules related to HCS-O subcompartments (CR-2016-059)	DES Schematron ISM-ID-00334 removed	None
6	Added Schematron rules to enforce that HCS-P subcompartments and HCS-O are not to be used with OC-USGOV (CR-2016-059)	Schematron ISM-ID-00362 added ISM-ID-00363 added	Data generation and ingestion systems need to be updated to enforce the new rule.



#	Change	Artifacts changed	Compatibility Notes
7	Relax value-based constraints for SCIs, SAP/SAR, and ACCMs when excludeFromRollup is true (CR-2015-039)	Schematron ISM-ID-00035 updated ISM-ID-00042 updated ISM-ID-00121 updated ISM-ID-00261 updated ISM-ID-00266 updated ISM-ID-00267 updated	Data generation and ingestion systems need to be updated to enforce the new rule.
8	Updated schematron rules to enforce minimum versions defined in specification dependency table 1.7	Schematron ISM-ID-00322 updated ISM-ID-00366 added	Data generation and ingestion systems need to be updated to accommodate this change.
9	Updated schematron rules to exclude checks if the only ISM content is the use of @ism:ISMCATCESVersion since UIAS examples are SAML centric and does not use other ISM elements or attributes such as @ism:DESVersion or @ism:resourceElement (CR-2015-034)	Schematron ISM-ID-00102 updated ISM-ID-00103 updated	Data generation and ingestion systems need to be updated to accommodate this change.
10	The schema change logs will no longer be maintained as of the 2016-SEP release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2016-SEP, reference the change history in the DES.	Schema	No impact to systems.
11	Updated schematron rules to resolve a bug allowing combinations of classification blocks that should not be used together. (CR-2016-018)	Schematron ISM-ID-00013 removed ISM-ID-00221 updated ISM-ID-00367 added	Data generation and ingestion systems need to be updated to accommodate this change.
12	Added attribute Usage Info in ISM CVE descriptive information. (CR-2016-019)	CVE	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
13	Update rendering for nonUScontrols to align with <i>Intelligence Community Markings System Register and Manual</i> . (CR-2014-092)	IC-ISM-PortionMark.xml IC-ISM-SecurityBanner.xml	Rendering systems need to be updated.
14	Removed KDK and moved KDK subcompartments under TK to align with IC Markings Register and Manual. (CR-2016-024)	CVE CVEnumISMSCIControls Schematron ISM-ID-00122 removed ISM-ID-00123 removed ISM-ID-00304 updated ISM-ID-00305 updated ISM-ID-00306 updated ISM-ID-00307 updated ISM-ID-00308 updated ISM-ID-00309 updated ISM-ID-00368 added ISM-ID-00369 added ISM-ID-00370 added ISM-ID-00371 added	Data generation and ingestion systems need to be updated to accommodate this change.
15	Fix errors in ISM Schematron rules that prevent presence of nonICMarkings, disseminationControls, and atomicEnergyMarkings without an excludeFromRollup. (CR-2016-049)	Schematron ISM-ID-00161 updated ISM-ID-00239 updated ISM-ID-00240 updated	Data generation and ingestion systems need to be updated to accommodate this change.
16	Updated rules to correct bugs with SBU-NF and LES-NF. (CR-2016-029)	Schematron ISM-ID-00104 updated ISM-ID-00149 updated ISM-ID-00372 added	Data generation and ingestion systems need to be updated to enforce the new rules.

#	Change	Artifacts changed	Compatibility Notes
17	Add SSI rollup and rolldown rules.(CR-2016-056)	Schematron ISM-ID-00373 added ISM-ID-00374 added	Data generation and ingestion systems need to be updated to accommodate this change.
18	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.
19	Updated rules ISM-ID-00318 and ISM-ID-00320 to reduce recursion and improve memory performance for LNI using community provided code. (CR-2016-020)	Schematron ISM-ID-00318 modified ISM-ID-00320 modified	Data generation and ingestion systems may need to be updated to enforce the new rule.

## B.12 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests
- Alignment with December 2014 IC Marking System Register and Manual<sup>[32]</sup>

The following table summarizes the changes made to 2014-DEC in developing 2015-AUG.

**Table 57 - Data Encoding Specification 2015-AUG Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated the abstract rules to correctly include the name of the attribute that failed.	Schematron AttributeValueDeprecatedError AttributeValueDeprecatedWarning	Data validation systems that update will have improved error messages.
2	Added restriction to ISM createDate attribute; timezone information no longer permitted.	Schematron ISM-ID-00274 modified	Systems need to be updated to enforce the new restriction.
3	Added rule ISM-ID-00345 requiring the attribute releasableTo is specified with the token values of [USA], [AUS], [CAN], [GBR] or [NZL] for each element which specifies the attribute disseminationControls with the value of [EYES].	Schematron ISM-ID-00345 added	Data generation and ingestion systems need to be updated to enforce the new rule.

#	Change	Artifacts changed	Compatibility Notes
4	Modified rule ISM-ID-00318 and ISM-ID-00320 to better handle special tetras and U portion handling.	Schematron ISM-ID-00318 modified ISM-ID-00320 modified	Data generation and ingestion systems may need to be updated to enforce the new rule.
5	Modified rule ISM-ID-00084 and added rule ISM-ID-00346 to ensure that LIMDIS portion marks only appear in the banner for UNCLASSIFIED information, and where content is portion-marked with U.	Schematron ISM-ID-00084 modified ISM-ID-00346 added	Data generation and ingestion systems may need to be updated to enforce the new rule.
6	Modified rule ISM-ID-00157 to restrict it to triggering on documents claiming DOD compliance.	Schematron ISM-ID-00157 modified	Data generation and ingestion systems may need to be updated to reduce the scope of the rule.
7	Updated to use the new URIs for <b>ntk:ProfileDes</b> and <b>ntk:AccessPolicy</b> .	Schematron ISM-ID-00326 modified	Data generation and ingestion systems need to be updated to use the new URI.
8	Updated code descriptions to improve readability.	Schematron	No impact to data generation and ingestion systems.
9	Updated ISM-ID-00322 to account for customization string on ISMCAT version.	Schematron ISM-ID-00322 modified	Data generation and ingestion systems should be updated to handle the customization string on the ISMCATCESVersion.
10	Updated ISM-ID-000324 to consider uncaveated UNCLASSIFIED resources as being exempt from requiring portions.	Schematron ISM-ID-00324 modified	Data generation and ingestion systems should be updated to account for the relaxation of portion requirements.
11	Added rules to require the corresponding NTK when ISM has PROPIN, NODIS, and EXDIS, and conversely require the markings for PROPIN, NODIS, EXDIS, and ORCON when the corresponding NTK exists.	Schematron ISM-ID-00349 added ISM-ID-00350 added ISM-ID-00351 added ISM-ID-00352 added ISM-ID-00353 added ISM-ID-00354 added ISM-ID-00355 added	Data generation and ingestion systems need to be updated to handle these rule additions.

#	Change	Artifacts changed	Compatibility Notes
12	Added rollup and rolldown rules for SARIdentifier.	Schematron ISM-ID-00347 added ISM-ID-00348 added	Data generation and ingestion systems need to be updated to handle these rule additions.
13	Added 50X declassification exemption codes 50X2, 50X3, 50X4, 50X5, 50X7, 50X8, and 50X9 to CVE.	CVEnumISM25X.xml	Data generation and ingestion systems need to be updated to handle the new values.
14	Added abstract patterns and modified rules to allow unknown SCIcontrols, SARIdentifiers, and ACCMs used on portions that do not contribute to rollup to only throw a warning instead of an error.	Schematron ValidateTokenValuesExistenceInListWithException added ValuesOrderedAccordingToCveWithException added ISM-ID-00035 modified ISM-ID-00042 modified ISM-ID-00121 modified ISM-ID-00225 modified ISM-ID-00261 modified ISM-ID-00266 modified ISM-ID-00267 modified	Data ingestion systems should be updated to handle the rule relaxation on external references.
15	Make @ism:ISMCACTCESVersion optional in ISMRootNodeAttributeOptionGroup	Schema	No impact to data generation and ingestion systems. Impacts systems designing new schema using ISM.
16	Added rule to require RD notice for RD data	Schematron ISM-ID-00356 added	Data generation and ingestion systems need to be updated to handle the new values.
17	Added rule to require SSI notice for SSI data	Schematron ISM-ID-00357 added	Data generation and ingestion systems need to be updated to handle the new values.
18	Updated util:recursivelyCheckDisplayTo for correctness (CR-2015-011)	Schematron ISM_XML.sch	Data generation and ingestion systems need to be updated.

## B.13 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- December 2014 IC Marking System Register and Manual<sup>[32]</sup>

The following table summarizes the changes made to V13 in developing 2014-DEC.

**Table 58 - Data Encoding Specification 2014-DEC Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added the line <xsl:output method="text" encoding="UTF-8" media-type="text-plain" indent="no"/> along the top of the three rendering stylesheets.	IC-ISM-ClassDeclass.xsl IC-ISM-SecurityBanner.xsl IC-ISM-PortionMark.xsl	Any stylesheet that imports these and does NOT want its output to be text MAY need to add a similar output element with the non text method desired.
2	If SClcontrols contains SI-G or an SI-G subs, then ism:disseminationControls cannot contain OC-USGOV.	Schematron ISM-ID-00341 added.	Data generation and ingestion systems need to be updated to handle this rule addition.
3	Updated existing ISM rule that limits use of the RD/FRD sigmas with TS, S, or C and removed the C from the equation. Removed all instances of "C" and "Confidential" from RD/FRD sigmas.	Schematron ISM-ID-00173 revised	Data generation and ingestion systems need to be updated to use the modified Schematron rules.
4	Updated definition of \$partTags in ISM_XML.sch. Fixes bug for CR-2014-005.	ISM_XML.sch	Data generation and ingestion systems need to be updated to use the modified Schematron file.
5	Updated CVEs to comment out regular expressions. They were commented out instead of completely removed to act as an aid for a starting point for those who need to extend the specification.	CVEnum-ISMSCIControls.xml CVEnumISM SAR.xml CVEnumISMNonIC.xml	Data generation and ingestion systems need to be updated to handle the removal of the ISM.XML CVE file.
6	Updated Banner and Portion StyleSheets for North Atlantic Treaty Organization (NATO) North Atlantic Council (NAC) rendering issues.	IC-ISM-PortionMark.xsl updated IC-ISM-SecurityBanner.xsl updated	Data rendering systems should update their stylesheets.

#	Change	Artifacts changed	Compatibility Notes
7	Updated Banner and Portion StyleSheets for multi-country non-Joint rendering issues.	IC-ISM-PortionMark.xml updated  IC-ISM-SecurityBanner.xml updated	Data rendering systems should update their stylesheets.
8	Correct Rule ISM-ID-00119 to properly not fire when ism:exemptFrom="IC_710_MANDATORY_FDR" is set.	Schematron  ISM-ID-00119 revised	Data generation and ingestion systems need to be updated to use the modified Schematron file.
9	Modified rules ISM-ID-00104 and ISM-ID-00149 where SBU-NF and LES-NF appearing in the banner now depends on the presence of NF.	Schematron  ISM-ID-00104 revised  ISM-ID-00149 revised	Data generation and ingestion systems need to be updated to use the modified Schematron files.
10	Modified rules ISM-ID-00163, ISM-ID-00315, ISM-ID-00316, ISM-ID-00317 to include NATO NACs wherever NATO was previously being checked.	Schematron  ISM-ID-00163 revised  ISM-ID-00315 revised  ISM-ID-00316 revised  ISM-ID-00317 revised	Data generation and ingestion systems need to be updated to use the modified Schematron files.
11	Changed DESVersion to represent the year and month of release. Also allowed for extension of specification by adding a '-' followed by a string to denote a custom implementation. Modified rule ISM-ID-00300 for changes to the DESVersion format.	DES  Schematron  ISM-ID-00300 revised	Data generation and ingestion systems need to be updated to use the modified Schematron file.
12	Updated FRD-SIGMA rollup to properly reflect that RD trumps FRD for SIGMA rollup.	Schematron  ISM-ID-00231 revised	Data generation and ingestion systems need to be updated to use the modified Schematron file.
13	Removed ORCON-USGOV exception from rule ISM-ID-00326 because an OC-NTK is still required to denote the originating agency even if it is USGOV.	Schematron  ISM-ID-00326 revised	Data generation and ingestion systems need to be updated to enforce this change.

#	Change	Artifacts changed	Compatibility Notes
14	Added rule to enforce roll-up and roll-down of all SCI controls.	Schematron ISM-ID-00060 removed ISM-ID-00061 removed ISM-ID-00062 removed ISM-ID-00063 removed ISM-ID-00111 removed ISM-ID-00112 removed ISM-ID-00113 removed ISM-ID-00116 removed ISM-ID-00343 added ISM-ID-00344 added	No impact for properly marked documents. Data generation and ingestion systems need to be updated to use the modified Schematron rules.
15	RELIDO and DISPLAYONLY may be used with markings containing FGI.	Schematron ISM-ID-00233 removed ISM-ID-00234 removed	Data generation and ingestion systems need to be updated to account for the removal of these rules.

## B.14 - V13 Change Summary

Significant drivers for Version 13 include:

- IC Marking System Register and Manual 31 December 2013<sup>[33]</sup>
- ICD 710 as revised June 2013
- Move to an opt-out methodology of rule application to prevent accidental omission from applicable rules.

The following table summarizes the changes made to V12 in developing V13.



**Table 59 - Data Encoding Specification V13 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	<p>Attribute ism:compliesWith now must be specified on all resource (ism:resourceElement="true") nodes within a document. Allowed values for ism:compliesWith are USGov, USDOD, USIC, and OtherAuthority. USDOD and USIC require USGov. Note that ism:compliesWith MUST contain USGov when the ism:ownerProducer attribute for the containing resource node contains USA.</p> <p>Specific exemptions within a rule set - for example exemption from ICD 710 FD&amp;R requirements, must be declared in the ism:exemptFrom attribute (also on the resource node).</p>	<p>CVEnum-ISMExemptFrom added</p> <p>Schematron</p> <p>All of the ISM.XML rules were updated in accordance with the new ISM.XML paradigm. The following rules have additional changes.</p> <p>ISM-ID-00119 revised</p> <p>ISM-ID-00155 revised</p> <p>ISM-ID-00158 revised</p> <p>ISM-ID-00162 revised</p> <p>ISM-ID-00225 revised</p> <p>ISM-ID-00251 revised</p> <p>ISM-ID-00255 revised</p> <p>ISM-ID-00273 revised</p> <p>ISM-ID-00337 added</p> <p>ISM-ID-00338 added</p> <p>ISM-ID-00339 added</p> <p>ISM-ID-00340 added</p>	<p>Data generation and ingestion systems need to be updated to handle the mandatory application of the compliesWith attribute and the appropriate exemptions within a rule set.</p> <p>Systems will also need to be updated to understand the full impact of the ICD 710 changes regarding FD&amp;R for their environment.</p>
2	Fixed error in ISM-ID-00189 that had incorrect CVE name and specification.	<p>Schematron</p> <p>ISM-ID-00189 revised</p>	The intent of the rule has not changed so systems complying with the intent should not need to be updated.
3	Removed ISM-ID-00222 due to a removal of the requirement for ICD 710 POC.	ISM-ID-00222 removed	Data generation and ingestion systems should be aware of the rule removal.

## B.15 - V12 Change Summary

Significant drivers for Version 12 include:

- Added a dependency on the *XML Encoding CVE Specification for ISM Country Codes and Tetragraphs* [\[49\]](#)
- Controlled Access Program Coordination Office (CAPCO) Register and Manual 6.0 Administrative Update [\[2\]](#)
- HCS Classification updates given to CAPCO but not yet published in the Register and Manual.

The following table summarizes the changes made to V11 in developing V12.


**Table 60 - Data Encoding Specification V12 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added rule to prohibit the simultaneous use of @ism:declassDate and @ism:declassEvent. The attributes are mutually exclusive.	Schematron ISM-ID-00329	Data generation and ingestion systems need to be updated to handle the new attribute.
2	Modified the schematron rules to ensure the following precedence is enforced both on elements and in rollup rules: NODIS (ND) > EXDIS (XD) > SBU-NF > SBU > FOUO.	Schematron ISM_ID_00038.sch updated ISM_ID_00066.sch updated ISM_ID_00104.sch updated ISM_ID_00105.sch updated MutuallyExclusiveAttributeValues.sch updated	Data generation and ingestion systems need to be updated to use the modified Schematron rules.
3	Updated the enumeration defining the currently authorized authority block declass date/event exemptions to no longer allow multi-values.	CVEnumISM25X	Data and ingestion systems need to ensure they are not allowing multi-values for any ISM25X typed elements.
4	Added rule to enforce that ORCON and ORCON-USGOV may not be used with RELIDO.	Schematron ISM-ID-00325 Added	Data generation and ingestion systems need to be updated to use the new Schematron rule.

#	Change	Artifacts changed	Compatibility Notes
5	Added rule to require presence of NTK with an Originator Controlled Need-to-Know (OC-NTK)OC-NTK profile when the value [OC] is present without [OC-USGOV].	Documentation Schematron ISM-ID-00326	Data generation and ingestion systems need to be updated to handle the new attribute.  This change may not be compatible with some specs that allow a range of versions.

#	Change	Artifacts changed	Compatibility Notes
6	Decoupled the Country Code and Tetragraph CVEs from ISM.XML and created the ISMCAT.CES CVE Encoding Specification. The schema and schematron rules were modified to point to ISMCAT.CES where applicable. Added a schematron rule to enforce the existence of the ISMCATCESVersion attribute and that the value is 1.	Schema CVENumISMFGIOpen CVENum-ISMFGIProtected CVENum-ISMOwnerProducer CVENumISMReITo Schematron ISM_ID_00100.sch updated ISM_ID_00166.sch updated ISM_ID_00170.sch updated ISM_ID_00179.sch updated ISM_ID_00180.sch updated ISM_ID_00188.sch updated ISM_ID_00189.sch updated ISM_ID_00190.sch updated ISM_ID_00191.sch updated ISM_ID_00192.sch updated ISM_ID_00193.sch updated ISM_ID_00194.sch updated	Data generation and ingestion systems need to be updated to handle the new ISMCAT.CES <sup>[49]</sup> dependency, the removal of the ISM.XML CVE files, and to use the new/modified schematron rules.

#	Change	Artifacts changed	Compatibility Notes
		ISM_ID_00195.sch updated	
		ISM_ID_00196.sch updated	
		ISM_ID_00197.sch updated	
		ISM_ID_00198.sch updated	
		ISM_ID_00199.sch updated	
		ISM_ID_00200.sch updated	
		ISM_ID_00201.sch updated	
		ISM_ID_00202.sch updated	
		ISM_ID_00203.sch updated	
		ISM_ID_00204.sch updated	
		ISM_ID_00205.sch updated	
		ISM_ID_00206.sch updated	
		ISM_ID_00207.sch updated	
		ISM_ID_00208.sch updated	
		ISM_ID_00209.sch updated	
		ISM_ID_00210.sch updated	
		ISM_ID_00211.sch updated	

#	Change	Artifacts changed	Compatibility Notes
		ISM_ID_00263.sch updated  ISM_ID_00322.sch added  ISM_ID_00323.sch added	
7	Added a schematron rule to enforce an ISM.XML document to have at least one portion marking in addition to the banner.	Schematron  ISM_ID_00324.sch added	Data generation and ingestion systems need to be updated to properly use the new rule.
8	Added reference to ACES.	Documentation	Access control systems using ISM.XML need to review ACES to ensure compliance.
9	<p>HCS compartments and subcompartments are no longer designated For Official Use Only. Rules relating to these values have been moved into the Unclassified rule number range.</p>  <p><b>Note</b> This change is ahead of the CAPCO Register and Manual.</p>	<p>Schematron</p> <p>ISM_ID_00330.sch added</p> <p>ISM_ID_00331.sch added</p> <p>ISM_ID_00332.sch added</p> <p>ISM_ID_00333.sch added</p> <p>ISM_ID_00334.sch added</p> <p>ISM_ID_00335.sch added</p> <p>ISM_ID_00336.sch added</p>	Data generation and ingestion systems may need to be updated to properly handle this change.

## B.16 - V11 Change Summary

Significant drivers for Version 11 include:

- CAPCO Register and Manual 6.0 (Note: Any CAPCO Register and Manual, V6.0 revisions not included in V11 will be addressed in a future version.)<sup>[3]</sup>
- CAPCO Register and Manual 5.1<sup>[4]</sup>

The following table summarizes the changes made to V10 in developing V11.

**Table 61 - Data Encoding Specification V11 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added @ism:joint attribute to indicate if multiple values in the @ism:ownerProducer attribute are JOINT producers. (i.e. // JOINT S) enabling the use of multiple ism:ownerProducer values to be used without indicating JOINT ownership. Was present in CAPCO Register and Manual V5.1, however we missed noticing it until now.	Schema Rendering Stylesheets	Data generation and ingestion systems need to be updated to handle the new attribute.
2	Added ORCON-USGOV as a value for disseminControls and created schematron rules to enforce correct usage.	CVEnumISMDissem  Schematron  ISM_ID_00302.sch added  ISM_ID_00303.sch added	Data generation and ingestion systems need to be updated to handle the new value, including making handling decisions based on it, and to properly use the new rules.
3	Updated the schematron rule that checks for the ism:DESVersion number.	Schematron  ISM_ID_00300.sch Changed	Data generation and ingestion systems need to be updated to properly use the new rule.
4	Restore support for HCS subcompartments.	Schematron  ISM-ID-10005 Restored  ISM-ID-10006 Restored  ISM-ID-10007 Restored  ISM-ID-10008 Restored  ISM-ID-10009 Restored  ISM-ID-10010 Restored  ISM-ID-10011 Restored	Data generation and ingestion systems need to be updated to properly use the rules.
5	Change rollup rules to treat caveated Unclassified as RELIDO per latest CAPCO guidance.	Schematron  ISM-ID-00088 Changed	Data generation and ingestion systems need to be updated to properly use the updated rule.

#	Change	Artifacts changed	Compatibility Notes
6	Added support for precedence of RD over FRD. Only RD notice required if on banner line.	Schematron ISM-ID-00075 Changed ISM-ID-00077 Changed ISM-ID-00128 Changed ISM-ID-000321 Added	Data generation and ingestion systems need to be updated to properly use the new and updated rules.
7	Removed obsolete rule ISM-ID-00126.	Schematron ISM-ID-00126 Removed	Data generation and ingestion systems should be aware of the rule removal.
8	Updated restrictions related to DeclassDate and DeclassEvent to also trigger when declassException of [25X1-EO-12951] is present.	Schematron ISM-ID-00133 Changed ISM-ID-00141 Changed	Data generation and ingestion systems need to be updated to properly use the updated rules.
9	Added two declass exception tokens [50X1] and [50X6].	CVEnumISM25X	Data generation and ingestions systems need to be updated to properly use and accept these tokens.
10	The following markings are now allowed to be commingled at the portion level with classified or unclassified information: DSEN, EXDIS, NODIS, SBU, SBU NOFORN, LES, LES NOFORN, and SSI.	Schematron ISM-ID-00037 Changed	Data generation and ingestion systems need to be updated to properly use the updated rule.
11	Updated banner and portion rendering XSL to handle Non-US Markings in the FGI portion of the banner.	IC-ISM-PortionMark.xsl IC-ISM-SecurityBanner.xsl testConfig.xml	Data rendering systems should be updated to reflect FGI non-US controls rendering.
12	Updated ISM-ID-00236 to exclude the derivedFrom and classificationReason attributes since their content is free text and should not be subject to the duplicate token restrictions.	Schematron ISM-ID-00236	Data generation and ingestion systems should be aware of the change.

## B.17 - V10 Change Summary

Significant drivers for Version 10 include:

- CAPCO Register and Manual 5.1 and approved Change Requests<sup>[4]</sup>



- CR-2012-001 KDK compartments/subs
- CR-2012-003 Eyes Only waiver extension
- CR-2012-004 EL and compartments
- CR-2012-005 Removal of ORCON POC
- CR-2012-006 NATO Declass On/DECL ON hierarchy update
- CR-2012-008 Non-IC roll-up rules for NOFORN
- CR-2012-009 EXDIS/NODIS require NOFORN
- CR-2012-010 GENC Standard
- CR-2012-011 Display Only Roll-up rules clarification.
- Decouple ISM.XML from other specifications

The following table summarizes the changes made to V9 in developing V10.

**Table 62 - Data Encoding Specification V10 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added a rule to verify that the DESVersion of ISM.XML is 10.	Schematron ISM_XML.sch	Data generation and ingestion systems need to ensure they are including the abstract rule.
2	Replaced ISO 3166 with Geopolitical Entities, Names, and Codes (GENC) Standard for country trigraph codes based on CAPCO CR CR-2012-010.	CVE CVerenumISMFGIOpen Changed CVerenum- ISMFGIProtected Changed CVerenum- ISMOwnerProducer Changed CVerenumISMRelTo Changed	Data generation and ingestion systems need to be updated to properly use the new values.

#	Change	Artifacts changed	Compatibility Notes
3	Added SCI Control system ENDSEAL (EL) and compartments -ECRU (EU) and -NONBOOK (NK) and associated constraint rules, based on CAPCO CR-2012-004.	CVE Schematron ISM-ID-00301 Added ISM-ID-00310 Added ISM-ID-00311 Added	Data generation and ingestion systems need to be updated to properly use the new values.
4	Changed KDK compartment regular expressions to a defined list containing [KDK-BLFH], [KDK-IDIT], and [KDK-KAND] and added corresponding constraint rules, based on CAPCO CR-2012-001.	CVE Schematron ISM-ID-00304 Added ISM-ID-00305 Added ISM-ID-00306 Added ISM-ID-00307 Added ISM-ID-00308 Added ISM-ID-00309 Added	Data generation and ingestion systems need to be updated to properly use the new values.
5	Added a rule to ensure that an element with a declassException of Atomic Energy Act (AEA) contains atomicEnergyMarkings.	Schematron ISM-ID-00299 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
6	Added a rule to ensure that any document with TFNI markings present in the body also has TFNI in the banner.	Schematron ISM-ID-00298 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
7	Updated the rule to require documents that contain TFNI portions to also have a declassException of AEA (preventing documents containing TFNI portions from having a declassDate).	Schematron ISM-ID-00246 Changed	Data generation and ingestion systems need to be updated to properly use the new rule.

#	Change	Artifacts changed	Compatibility Notes
8	Created schematron rules to validate ISM.XML attribute types.	Schematron TypeConstraintPatterns.sch Added ISM-ID-00268 Added ISM-ID-00269 Added ISM-ID-00270 Added ISM-ID-00271 Added ISM-ID-00272 Added ISM-ID-00273 Added ISM-ID-00274 Added ISM-ID-00275 Added ISM-ID-00276 Added ISM-ID-00277 Added ISM-ID-00278 Added ISM-ID-00279 Added ISM-ID-00280 Added ISM-ID-00281 Added ISM-ID-00282 Added ISM-ID-00283 Added ISM-ID-00284 Added ISM-ID-00285 Added ISM-ID-00286 Added ISM-ID-00287 Added ISM-ID-00288 Added ISM-ID-00289 Added ISM-ID-00290 Added	This change should not affect existing data generation and ingest systems. However, these systems could be updated to rely on schematron rules for validating ISM.XML attribute types instead of using the schema.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00291 Added	
		ISM-ID-00292 Added	
		ISM-ID-00293 Added	
		ISM-ID-00294 Added	
		ISM-ID-00295 Added	
		ISM-ID-00296 Added	
		ISM-ID-00297 Added	

#	Change	Artifacts changed	Compatibility Notes
9	Clarified the description in the Schematron rules that deal with deprecated values in the CVE files [artf13026].	Schematron ISM-ID-00166 Changed ISM-ID-00170 Changed ISM-ID-00179 Changed ISM-ID-00180 Changed ISM-ID-00188 Changed ISM-ID-00189 Changed ISM-ID-00190 Changed ISM-ID-00191 Changed ISM-ID-00192 Changed ISM-ID-00193 Changed ISM-ID-00194 Changed ISM-ID-00195 Changed ISM-ID-00196 Changed ISM-ID-00197 Changed ISM-ID-00198 Changed ISM-ID-00199 Changed ISM-ID-00200 Changed ISM-ID-00201 Changed ISM-ID-00202 Changed ISM-ID-00203 Changed ISM-ID-00204 Changed ISM-ID-00205 Changed ISM-ID-00206 Changed ISM-ID-00207 Changed ISM-ID-00208 Changed	Should not impact data.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00209 Changed ISM-ID-00210 Changed ISM-ID-00211 Changed	
10	Created schematron rules to check that the value(s) of an ISM.XML attribute are defined in the CVE file for that attribute.	Schematron ValidateTokenValuesExistenceInList.sch Added ISM-ID-00253 Added ISM-ID-00254 Added ISM-ID-00255 Added ISM-ID-00256 Added ISM-ID-00257 Added ISM-ID-00258 Added ISM-ID-00259 Added ISM-ID-00260 Added ISM-ID-00261 Added ISM-ID-00262 Added ISM-ID-00263 Added ISM-ID-00264 Added ISM-ID-00265 Added ISM-ID-00266 Added ISM-ID-00267 Added	This change should not affect existing data generation and ingest systems. However, these systems could be updated to rely on Schematron rules for checking allowed ISM.XML CVE values instead of using the schema.
11	New rule ISM-ID-00320 handles the intent of ISM-ID-00171 and includes additional rollup logic resulting in ISM-ID-00171 being removed.	ISM-ID-00171 Removed	Generation and ingest systems should be aware of this change, but if the intent of the rule was being followed there should be no effect.
12	Corrected bug in rollup logic of disseminationControls token "REL" that prevented legal rollups.	ISM-ID-00088 Changed	Generation and ingest systems should be aware of this change, but if the intent of the rule was being followed there should be no effect.

#	Change	Artifacts changed	Compatibility Notes
13	Refactored Schematron to use xsl function for contributesToRollup.	ISM-XML DataHasCorrespondingNotice Added NoticeHasCorrespondingData Added ISM-ID-00119 Changed ISM-ID-00244 Changed ISM-ID-00245 Changed ISM-ID-00219 Changed	No change in logic, centralized code to reduce maintenance risks.
14	Corrected typo of duplicate "[" in error message.	ISM-ID-00242 Changed	No change in logic.
15	Correct regular expression for SI-G subcompartments to disallow more than 4 characters.	ISM-ID-00186 Changed	Generation and ingest systems should be aware of this change, but if the CAPCO Register and Manual was being followed there should be no effect.
16	Change Warning to Error given that notices for FISA or RD data are always required.	ISM-ID-00135 Changed ISM-ID-00139 Changed	Generation and ingest systems should be aware of this change, but if the CAPCO Register and Manual was being followed there should be no effect.
17	Added requirement for ND and XD data to be marked NF, based on CAPCO CR CR-2012-009.	ISM-ID-00313 Added ISM-ID-00314 Added	Data generation and ingestion systems need to be updated to properly use the new rules.
18	Extended deprecation date of EYES to 2014-09-11, based on CAPCO CR CR-2012-003.	CVE CVEnumISMDissem Changed	Data generation and ingestion systems need to be updated to properly use the deprecation value.
19	Add NATO declass exemption to potential exemptions, based on ISOO Notice 2013-01 <sup>[61]</sup> and CAPCO CR-2012-006.	CVE CVE ISM25X Changed ISM-ID-00141 Changed ISM-ID-00246 Changed ISM-ID-00315 Added ISM-ID-00316 Added ISM-ID-00317 Added	Data generation and ingestion systems need to be updated to properly use the values.

#	Change	Artifacts changed	Compatibility Notes
20	Changed type of <code>ism:declassException</code> to <code>NMToken</code> to comply with only one <code>declassException</code> being permitted per CAPCO.	ISM-ID-00277 Changed	Generation and ingest systems should be aware of this change.
21	ORCON POC is no longer required on documents, based on CAPCO CR-2012-005.	ISM-ID-00224 Removed ISM-ID-00247 Removed	Generation and ingest systems should be aware of this change.
22	Added rule to enforce rollup constraints for <code>releasableTo</code> attribute. Based on existing Foreign Disclosure & Release markings roll-up rules.	Schematron ISM-ID-00318 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
23	Added rule to enforce rollup constraints for <code>displayOnlyTo</code> attribute. Based on CR-2012-011 Display Only Roll-up rules clarification.	Schematron ISM-ID-00320 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
24	Fixed ISM-ID-00105 to take into account SUB-NF when determining if SBU should be in a banner.	Schematron ISM-ID-00105 Changed	Generation and ingest systems should be aware of this change, but if the intent of the rule was being followed there should be no effect.

## B.18 - V9 Change Summary

Significant drivers for Version 9 include:

- CAPCO Register and Manual 5.1<sup>[4]</sup>

The following table summarizes the changes made to V8 in developing V9.

**Table 63 - Data Encoding Specification V9 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Added support for alphanumeric <code>@ism:DESVersion</code> identifiers [artf12167].	Schema	Should not impact data but ingestion systems may need to account for it.
2	Added support for KDK subcompartments and sub-subcompartments [artf12261].	Schema CVE	Data generation and ingestion systems need to be updated to handle these new values.
3	Changed declaration of <code>NoticeText</code> from <code>complexContent</code> to <code>simpleContent</code> [artf12153].	Schema	Should only impact some code generation systems.



#	Change	Artifacts changed	Compatibility Notes
4	Corrected RSV to not be a regular expression and make SI-[A-Z]{3} and SI-[A-Z]{3}-[A-Z]{4} into regular expressions [artf12269].	Schema CVE	Data generation and ingestion systems need to be updated to properly use the new values.
5	Added ism external notice attribute to indicate that a notice data refers to external content. Add convenience elements of NoticeExternal and NoticeExternalList Updated schematron rules to reflect change.	Schema Schematron ISM-ID-00127 updated ISM-ID-00128 updated ISM-ID-00129 updated ISM-ID-00130 updated ISM-ID-00134 updated ISM-ID-00135 updated ISM-ID-00136 updated ISM-ID-00137 updated ISM-ID-00138 updated ISM-ID-00139 updated ISM-ID-00150 updated ISM-ID-00151 updated ISM-ID-00152 updated ISM-ID-00153 updated ISM-ID-00158 updated ISM-ID-00159 updated ISM-ID-00161 updated ISM-ID-00244 updated ISM-ID-00245 updated ISM-ID-00248 Added	Data generation and ingestion systems need to be updated to properly use the new values.

#	Change	Artifacts changed	Compatibility Notes
6	Added rule to ensure an ORCON POC is not also marked as ORCON dissemination. [artf11980].	ISM-ID-00247 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
7	Remove support for HCS subcompartments.	ISM-ID-10005 Removed ISM-ID-10006 Removed ISM-ID-10007 Removed ISM-ID-10008 Removed ISM-ID-10009 Removed ISM-ID-10010 Removed ISM-ID-10011 Removed	Data generation and ingestion systems need to be updated to no longer use these values.
8	By ICD 710, only intelligence products required the ICD 710 POC. Added a separate designator to compliesWith to support this separation from ICDocument.	ISM-ID-00222 Changed CVerenum-ISMCompliesWith.xml Changed	Data generation and ingestion systems need to be updated to no longer use these values.
9	Removed rule enforcing @noticeType definition on external notices. All Notice elements now require either @noticeType or @unregisteredNoticeType to be defined.	ISM-ID-00249 Removed ISM-ID-00250 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
10	Added OSTY Open Skies Treaty.	CVerenum-ISMOwnerProducer.xml Changed CVerenum-ISMFGIProtected.xml Changed CVerenumISMRelTo.xml Changed CVerenum-ISMFGIOpen.xml Changed	Data generation and ingestion systems need to be updated to properly use the new value.

#	Change	Artifacts changed	Compatibility Notes
11	Added COMSEC notice and NNPI for use outside of the IC only.	CVEnumISMNotice.xml CVEnumISMNonIC.xsd ISM-ID-00251 Added ISM-ID-00225 Changed	Data generation and ingestion systems need to be updated to properly use the new value.
12	Update ISM-ID-00132 to account for the need of RELIDO on Unclass portions that have explicit release specified.	ISM-ID-00132 Changed	Data generation and ingestion systems need to be updated to properly use the new rule.
13	Update ISM-ID-00088 to account for ISM attributes such as NoticeType that should not factor into this rule.	ISM-ID-00088 Changed	Data generation and ingestion systems need to be updated to properly use the new rule.

## B.19 - V8 Change Summary

Significant drivers for Version 8 include:

- CAPCO Register and Manual 5.1<sup>[4]</sup>
- ISOO Guidance ISOO Notice 2012-02<sup>[60]</sup>
- ISO 3166-1<sup>[50]</sup>

The following table summarizes the changes made to V7 in developing V8.

**Table 64 - Data Encoding Specification V8 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated country code descriptions in the ISO 3166-1 <sup>[50]</sup> CVEs to reflect ISO newsletter changes.	schema Changed CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and ingestion systems need to be updated to properly use the new values.

#	Change	Artifacts changed	Compatibility Notes
2	Allow use of RSV.	schema Changed CVEnumISMSCIControls Changed	Data generation and ingestion systems need to be updated to properly use the new values.
3	Unclassified documents may now be marked as REL, RELIDO, NF, and DISPLAYONLY.	ISM-ID-00016 Changed ISM-ID-00028 Changed ISM-ID-00094 Removed ISM-ID-00140 Removed ISM-ID-00215 Removed	Data generation and ingestion systems need to be updated to handle these policy changes.
4	Added missing rules for enforcing RD and FRD and Sigma data existing when RD or FRD or Sigma respectively is present at the resource level.	ISM-ID-00228 Added ISM-ID-00229 Added ISM-ID-00230 Added ISM-ID-00231 Added	Data generation and ingestion systems need to be updated to handle these policy changes.
5	RELIDO and DISPLAYONLY are no longer permitted on portions containing FGI data.	ISM-ID-00233 Added ISM-ID-00234 Added	Data generation and ingestion systems need to be updated to handle these policy changes.
6	Added unique namespaces to generated CVE schema fragments. Moved schema fragment imports to the base schema.	Schema CVEs	Should not affect data.
7	Added attributeFormDefault="qualified" to make the attributes explicitly require the being namespace prefixed.	Schema	Should not affect data.
8	Fixed a bug in the code implementation of the variable ISM_NSI_EO_APPLIES in the main Schematron file, ISM_XML.sch.	ISM_XML.sch ISM-ID-00142 ISM-ID-00017 ISM-ID-00133 ISM-ID-00013 ISM-ID-00014 ISM-ID-00141	The listed rules utilize the variable ISM_NSI_EO_APPLIES in their logic and may therefore have changes in behavior, but the code for these rules remains unchanged.

#	Change	Artifacts changed	Compatibility Notes
9	Allow portions with @ism:excludeFromRollup=true() to not have an ICD 710 <sup>[39]</sup> foreign release indicator on them. [artf11427].	ISM_XML.sch ISM-ID-00119	Data generation and ingestion systems need to be updated to handle these data changes.
10	Enforce illegal value duplications in ISM.XML attributes.	ISM-ID-00236 Added	Data generation and ingestion systems need to be updated to handle these data changes.
11	Remove SINFO.	ISM-ID-00083 Removed ISM-ID-00037 Changed ISM-ID-00161 Changed CVE	Data generation and ingestion systems need to be updated to reject data still marked SINFO.
12	Remove SC.	ISM-ID-00082 Removed ISM-ID-00036 Removed CVE	Data generation and ingestion systems need to be updated to reject data still marked SC.
13	Remove ECI-AAA.	ISM-ID-00046 Removed ISM-ID-00177 Removed CVE	Data generation and ingestion systems need to be updated to reject data still marked ECI-AAA.
14	Remove 25X1-human.	ISM-ID-00133 Changed ISM-ID-00141 Changed CVE	Data generation and ingestion systems need to be updated to reject data still marked 25X1-human.
15	Consolidated atomicEnergyMarking rules. Moved values from ISM-ID-00182 into ISM-ID-00181.	ISM-ID-00182 Removed ISM-ID-00181 Changed	Data generation and ingestion systems need to be updated to handle these rule changes.
16	Consolidated classification rules. Moved values from ISM-ID-00015 into ISM-ID-00016.	ISM-ID-00015 Removed ISM-ID-00016 Changed	Data generation and ingestion systems need to be updated to handle these rule changes.
17	Removed disseminationControl tokens marked For Official Use Only.	ISM-ID-10001 Removed ISM-ID-10003 Removed	Data generation and ingestion systems need to be updated to handle these data changes.
18	Consolidated rules for mutually exclusive disseminationControl tokens.	ISM-ID-00034 Removed ISM-ID-00169 Changed	Data generation and ingestion systems need to be updated to handle these data changes.

#	Change	Artifacts changed	Compatibility Notes
19	For attribute noticeType, enforce date and point of contact requirements individually.	ISM-ID-00156 Removed ISM-ID-00237 Added ISM-ID-00238 Added	Data generation and ingestion systems need to be updated to handle these rule changes.
20	Split Notice Rule 00160 into 00239 and 00240.	ISM-ID-00160 Removed ISM-ID-00239 Added ISM-ID-00240 Added	Data generation and ingestion systems need to be updated to handle these rule changes.
21	All attributes in the ISM.XML namespace must have a non-null value.	ISM-ID-00002 Changed ISM-ID-00001 Removed	Data generation and ingestion systems need to be updated to handle these rule changes.
22	Consolidated resource element rules. Moves values of ISM-ID-00057 into ISM-ID-00056.	ISM-ID-00057 Removed ISM-ID-00056 modified	Data generation and ingestion systems need to be updated to handle these rule changes.
23	Removes \$ISM_CAPCO_RESOURCE from rules enforcing attributes and elements in the ISM.XML namespace.	ISM-ID-00125 Changed ISM-ID-00223 Changed	Data generation and ingestion systems need to be updated to handle these rule changes.
24	Adds \$ISM_CAPCO_RESOURCE missing from notice rules.	ISM-ID-00135 Changed ISM-ID-00152 Changed	Data generation and ingestion systems need to be updated to handle these rule changes.
25	Added new hierarchy structure to SAR Identifiers.	CVE Changed	Data generation and ingestion systems need to be updated to handle these changes.
26	Added requirement for Critical Nuclear Weapons Design Information (CNWDI) notice with CNWDI data.	ISM-ID-00244 Added ISM-ID-00245 Added CVE Changed	Data generation and ingestion systems need to be updated to handle these rule changes.

## B.20 - V7 Change Summary

Significant drivers for Version 7 include:

- CAPCO Register and Manual 4.2<sup>[5]</sup>
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)<sup>[51]</sup>
- ISO 3166-1<sup>[50]</sup>
- DNI ORCON Memo<sup>[64]</sup>
- ICD 710<sup>[39]</sup>

The following table summarizes the changes made to V6 in developing V7.

**Table 65 - Data Encoding Specification V7 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Resolved attribute composability issue by separating ISM.XML notice attributes from the security attributes.	Schema	Should not affect data.
2	Added elements <b>ism:Notice</b> , <b>ism:NoticeText</b> and <b>ism:NoticeList</b> to represent valid ISM.XML notices, as well as the attribute <b>@ism:unregisteredNoticeType</b> to represent other notices.	Schema CVENumISMElements Added CVENumISMAAttributes Changed ISM-ID-00223 Added ISM-ID-00226 Added	Data generation and ingestion systems need to be updated to use the new values.
3	Added <b>ism:ISMNoticeAttributeGroup</b> to <b>ism:ResourceNodeAttributeGroup</b> and <b>ism:ResourceNodeOptionalAttributeGroup</b> .	Schema	Schema developers need to update to use the corrected attribute group. Instance documents are not impacted.
4	Added new <b>@ism:pocType</b> attribute and <b>ism:POCAttributeGroup</b> to support indicators for a security-related point-of-contact, including ORCON, ICD 710 <sup>[39]</sup> and DoD Distribution statements.	Schema CVENumISMAAttributes Changed CVENumISMPocType-Added ISM-ID-00222 Added ISM-ID-00224 Added	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
5	Added notice attributes to ISM.XML resource node.	Schema	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
6	Replaced "\d" in regular expressions to the more specific "[0-9]."	Schema Constraint Rules	Should not impact data since intent of the new expressions is the same.

#	Change	Artifacts changed	Compatibility Notes
7	Added <b>@ism:unregisteredNoticeType</b> to the exceptions in ISM-ID-00012 and ISM-ID-00019.	ISM-ID-00012 Changed ISM-ID-00019 Changed	No impact on existing ISM.XML data, addition is necessary to prevent unintended changes to IRM. Data generation and ingestion systems will need to be updated to reflect the change.
8	Removed <b>@ism:ACCM</b> and moved its values to <b>@ism:nonICmarkings</b> .	Schema CVCEnumISMACCM Removed ISM-ID-00220 Removed ISM-ID-00225 Added	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
9	Renamed <b>@ism:notice</b> to <b>@ism:noticeType</b> and replaced <b>@ism:noticePOC</b> with <b>@ism:pocType="DoD-Dist"</b> .	Schema CVCEnumISMAttributes Changed Constraint Rules	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
10	Allowed for multiple values to be specified for <b>@ism:declassException</b> .	CVCEnumISM25X Changed ISM-ID-00133 Changed ISM-ID-00141 Changed	Previously valid data should still be valid, but data generated from this release forward will not be backwards-compatible.
11	Added <b>@ism:declassException="50X1-HUM"</b> and <b>@ism:declassException="50X2-WMD"</b> to the exceptions in ISM-ID-00133 and ISM-ID-00141.	ISM-ID-00133 Changed ISM-ID-00141 Changed	Per the ISOO Implementing Directive, ISOO does not require a date or event with 50X1-HUM or 50X2-WMD declassification exceptions.
12	Added rule that prevents <b>@ism:noticeType</b> and <b>@ism:unregisteredNoticeType</b> from being applied to the same element.	ISM-ID-00226 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.
13	Added rule that ensures <b>@ism:noticeType</b> is only used on the resource node when it specifies a DoD Distribution statement.	ISM-ID-00227 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.



#	Change	Artifacts changed	Compatibility Notes
14	As tetragraphs "MIFH", "EUDA" and "EFOR" were removed from the CAPCO Register and Manual, their deprecation dates were added to the CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and ingestion systems need to be updated to remove these tokens before their deprecation dates.
15	Removed deprecation dates for @ism:declassException tokens "25X1-human", and "AEA".	CVEnumISM25X1	Should not affect data.
16	Added country code for South Sudan to the ISO 3166-1 <sup>[50]</sup> CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and ingestion systems need to be updated to properly use the new values.

## B.21 - V6 Change Summary

Significant drivers for Version 6 include:

- CAPCO Register and Manual 4.1 (HCS Sub Cats missed in V5)<sup>[6]</sup>
- Executive Order 13526<sup>[24]</sup>
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)<sup>[51]</sup>

The following table summarizes the changes made to V5 in developing V6.

**Table 66 - Data Encoding Specification V6 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Removed ISM-ID-00212.	ISM-ID-00212 Remove	ISM-ID-00212 was a duplicate of ISM-ID-103.
2	Cleaned up English text of ISM-ID-00124.	ISM-ID-00124 Changed	Corrected an error in text. No change to Schematron.
3	Improved sorting algorithm.	ISM-ID-00026 Changed ISM-ID-00035 Changed  ISM-ID-00041 Changed  ISM-ID-00042 Changed  ISM-ID-00095 Changed  ISM-ID-00096 Changed  ISM-ID-00100 Changed  ISM-ID-00121 Changed  ISM-ID-00167 Changed  ISM-ID-00178 Changed	Corrects small defects and oddities in sorting algorithm.

#	Change	Artifacts changed	Compatibility Notes
4	Modified check for resourceElement to be more accurate only applying to the first occurrence of resourceElement=true().	ISM-ID-00013 Changed ISM-ID-00014 Changed ISM-ID-00056 Changed ISM-ID-00057 Changed ISM-ID-00058 Changed ISM-ID-00059 Changed ISM-ID-00060 Changed ISM-ID-00061 Changed ISM-ID-00062 Changed ISM-ID-00063 Changed ISM-ID-00064 Changed ISM-ID-00065 Changed ISM-ID-00066 Changed ISM-ID-00067 Changed ISM-ID-00068 Changed ISM-ID-00069 Changed ISM-ID-00070 Changed ISM-ID-00071 Changed ISM-ID-00072 Changed ISM-ID-00073 Changed ISM-ID-00074 Changed ISM-ID-00075 Changed ISM-ID-00077 Changed ISM-ID-00078 Changed ISM-ID-00079 Changed ISM-ID-00080 Changed	Now is compliant with intent of ISM.XML check for resourceElement. Only considers the first resourceElement=true() a resource element.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00081 Changed	
		ISM-ID-00082 Changed	
		ISM-ID-00083 Changed	
		ISM-ID-00084 Changed	
		ISM-ID-00085 Changed	
		ISM-ID-00086 Changed	
		ISM-ID-00087 Changed	
		ISM-ID-00090 Changed	
		ISM-ID-00104 Changed	
		ISM-ID-00105 Changed	
		ISM-ID-00108 Changed	
		ISM-ID-00109 Changed	
		ISM-ID-00110 Changed	
		ISM-ID-00111 Changed	
		ISM-ID-00112 Changed	
		ISM-ID-00113 Changed	
		ISM-ID-00116 Changed	
		ISM-ID-00118 Changed	
		ISM-ID-00132 Changed	
		ISM-ID-00135 Changed	
		ISM-ID-00136 Changed	
		ISM-ID-00137 Changed	
		ISM-ID-00138 Changed	
		ISM-ID-00139 Changed	
		ISM-ID-00141 Changed	
		ISM-ID-00145 Changed	

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00146 Changed ISM-ID-00147 Changed ISM-ID-00149 Changed ISM-ID-00150 Changed ISM-ID-00151 Changed ISM-ID-00152 Changed ISM-ID-00153 Changed ISM-ID-00154 Changed ISM-ID-00155 Changed ISM-ID-00160 Changed ISM-ID-00161 Changed ISM-ID-00162 Changed ISM-ID-00165 Changed	
5	Added handling of 3, 4, and 5 Eyes countries when processing rollup.	ISM-ID-00088 Changed ISM-ID-00171 Changed ISM-ID-00172 Changed	This only adds support for considering the countries that are a part of 3, 4, and 5 eyes when processing rollup. Does not affect meaning of the rule.
6	Improved checking for null attributes.	ISM-ID-00002 Changed	Does not affect anything except that the check for null-valued attributes is more accurate.
7	Add rule that enforces if FGIsSourceProtected contains [FGI] then [FGI] is the only value.	ISM-ID-00217 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.
8	Add rule that enforces if FGIsSourceOpen contains [UNKNOWN] then [UNKNOWN] is the only value.	ISM-ID-00216 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.
9	Ensure that for portions where ISM_CONTRIBUTES if [FGI] is a value of ownerProducer or FGIsSourceProtected then both are [FGI].	ISM-ID-00218 Added ISM-ID-00219 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

#	Change	Artifacts changed	Compatibility Notes
10	Corrected bug in code that allowed ISM-ID-00097 to trigger on non-CAPCO resources.	ISM-ID-00097 Changed	No change to intent of the rule.
11	Tetragraph [MCFI] removed from CVEs.	CVEs	Data generation and ingestion systems need to be updated to no longer use the obsolete value.
12	Added support for HCS/HUMINT sub-categories within SCIcontrols.	ISM-ID-10005 Added ISM-ID-10006 Added ISM-ID-10007 Added ISM-ID-10008 Added ISM-ID-10009 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.
13	Added support for TFNI.	CVEs	Data generation and ingestion systems need to be updated to properly use the new value.
14	Added support for SSI.	CVEs	Data generation and ingestion systems need to be updated to properly use the new value.

## B.21.1 - V6 Change Errata

The following table summarizes the changes that were discovered to have been omitted from the original publication of V6.

**Table 67 - Data Encoding Specification V6 Change Errata**

#	Change	Artifacts changed	Compatibility Notes
1	Enforce prohibition of declass reason with derivatively classified documents.	ISM-ID-00221 Added	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

## B.22 - V5 Change Summary

Significant drivers for Version 5 include:

- CAPCO Register and Manual 4.1<sup>[6]</sup>

The following table summarizes the changes made to V4 in developing V5.

**Table 68 - Data Encoding Specification V5 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Change encoding of constraint rules from text to Schematron.	Documentation Constraint Rules	Other than rules whose changes are noted below this should only result in more clarity of definition for the rules.
2	RS now unclassified.	Documentation Constraint Rules ISM-ID-10001 Change ISM-ID-00164 Add ISM-ID-10002 Remove ISM-ID-00165 Add	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.
3	Use single Schematron rule to encode deprecated warnings.	Constraint Rules CVEs ISM-ID-00166 Add	Systems processing the CVEs need to be aware of the deprecation changing from Boolean to date.
4	Add Support for DisplayOnly.	Documentation Schema Constraint Rules ISM-ID-00167 Add ISM-ID-00168 Add ISM-ID-00169 Add ISM-ID-00170 Add ISM-ID-00171 Add ISM-ID-00172 Add	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.

#	Change	Artifacts changed	Compatibility Notes
5	Support AEA data having new location in banner and a new attribute.	Documentation CVEs Schema Constraint Rules ISM-ID-00029 Remove ISM-ID-00078 Change ISM-ID-00079 Change ISM-ID-00173 Add ISM-ID-00028 Change ISM-ID-00174 Add ISM-ID-00027 Remove ISM-ID-00175 Add ISM-ID-00127 Change ISM-ID-00128 Change ISM-ID-00135 Change ISM-ID-00136 Change ISM-ID-00072 Change ISM-ID-00073 Change ISM-ID-00074 Change ISM-ID-00075 Change ISM-ID-00077 Change ISM-ID-00178 Add ISM-ID-00092 Remove ISM-ID-00181 Add ISM-ID-00093 Remove ISM-ID-00182 Add	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.



#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00160 Change	
6	Support AEA data not allowing declass date.	Documentation Constraint Rules ISM-ID-00141 Change ISM-ID-00014 Change ISM-ID-00176 Add	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.
7	Co-constraints on SCI subcompartments and AEA subcompartments.	Constraint Rules ISM-ID-00177 Add ISM-ID-00183 Add ISM-ID-00184 Add ISM-ID-00185 Add ISM-ID-00186 Add ISM-ID-00187 Add	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.
8	Remove SAMI.	CVEs Constraint Rules ISM-ID-00069 Remove ISM-ID-00028 Change ISM-ID-00091 Remove ISM-ID-00106 Remove ISM-ID-00117 Remove	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

#	Change	Artifacts changed	Compatibility Notes
9	Remove rules now enforced by schema enumerations.	ISM-ID-00131 Remove ISM-ID-00024 Remove ISM-ID-00025 Remove ISM-ID-00114 Remove ISM-ID-00003 Remove ISM-ID-00004 Remove ISM-ID-00007 Remove ISM-ID-00039 Remove ISM-ID-00009 Remove ISM-ID-00010 Remove ISM-ID-00011 Remove ISM-ID-00115 Remove	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.
10	Remove <code>@ism:typeOfExemptedSource</code> and <code>@ism:dateOfExemptedSource</code> since ISOO no longer supports that concept.	Documentation Schema ISM-ID-00014 Change ISM-ID-00016 Change ISM-ID-00018 Remove ISM-ID-00019 Remove ISM-ID-00020 Remove ISM-ID-00021 Remove	Data generation and ingestion systems need to be updated to not use these values anymore and to properly enforce the new constraint rules.
11	Remove Appendix H Reading the Schematics.	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.
12	ISM-ID-00037 and ISM-ID-00083 contradict each other when classified material is involved.	ISM-ID-00037 Change	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

#	Change	Artifacts changed	Compatibility Notes
13	Add Rules for deprecated values based off of the CVEs.	ISM-ID-00166 – classification deprecation warning  ISM-ID-00170 – classification deprecation error  ISM-ID-00179 – disseminationControls deprecation warning  ISM-ID-00180 – disseminationControls deprecation error  ISM-ID-00188 – FGIsourceOpen deprecation warning  ISM-ID-00189 – FGIsourceOpen deprecation error  ISM-ID-00190 – FGIsourceProtected deprecation warning  ISM-ID-00191 – FGIsourceProtected deprecation error  ISM-ID-00192 – nonICmarkings deprecation warning  ISM-ID-00193 – nonICmarkings deprecation error  ISM-ID-00194 – notice deprecation warning  ISM-ID-00195 – notice deprecation error  ISM-ID-00196 – ownerProducer deprecation warning	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00197 – ownerProducer deprecation error	
		ISM-ID-00198 – releasableTo deprecation warning	
		ISM-ID-00199 – releasableTo deprecation error	
		ISM-ID-00200 – displayOnlyTo deprecation warning	
		ISM-ID-00201 – displayOnlyTo deprecation error	
		ISM-ID-00202 – SARIdentifier deprecation warning	
		ISM-ID-00203 – SARIdentifier deprecation error	
		ISM-ID-00204 – SCIcontrols deprecation warning	
		ISM-ID-00205 – SCIcontrols deprecation error	
		ISM-ID-00206 – declassException deprecation warning	
		ISM-ID-00207 – declassException deprecation error	
		ISM-ID-00208 – atomicEnergyMarkings deprecation warning	

#	Change	Artifacts changed	Compatibility Notes
		ISM-ID-00209 – atomicEnergyMarkings deprecation error	
		ISM-ID-00210 – nonUSControls deprecation warning	
		ISM-ID-00211 – nonUSControls deprecation error	

## B.22.1 - V5 Change Errata

The following table summarizes the changes that were discovered to have been omitted from the original publication of V5.

**Table 69 - Data Encoding Specification V5 Change Errata**

#	Change	Artifacts changed	Compatibility Notes
1	Added ability to mark US person notice.	CVE	Data generation and ingestion systems need to be updated to properly handle data marked as US Person.

## B.23 - V4 Change Summary

Significant drivers for Version 4 include:

- DoD Directive 5230.24<sup>[16]</sup>
- ICD 710<sup>[39]</sup> (enforce immediately no grace)

The following table summarizes the changes made to V3 in developing V4.

**Table 70 - Data Encoding Specification V4 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Add support for DoD Distribution Statements.	Schema Controlled Value Enumerations ISM-DoD5230.24Applies ISM-ICD-710Applies ISM-ID-00119 ISM-ID-00120 ISM-ID-00155 ISM-ID-00156 ISM-ID-00157 ISM-ID-00158 ISM-ID-00159 ISM-ID-00160 ISM-ID-00161 ISM-ID-00162	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.
2	Refactor how NATO marks are represented.	Schema Controlled Value Enumerations ISM-ID-00163	Data generation and ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules.
3	Use schema to enforce DES version number.	Schema ISM-ID-00102	Forces DES to match version shipped.
4	Enforce ICD 710 <sup>[39]</sup> immediately.	ISM-ID-00088 ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data ingestion systems need to be updated to properly enforce the new constraint rules. Data generation systems compliant with ICD 710 <sup>[39]</sup> need make no changes. Existing data may not be valid anymore.
5	Remove Duplicate or redundant rules.	ISM-ID-00144 ISM-ID-00023	Data validation systems may remove duplicate code.

## B.24 - V3 Change Summary

Significant drivers for Version 3 include:

- Executive Order 13526<sup>[24]</sup> (enforce requirements for Authority block)
- CAPCO Register and Manual 3.1<sup>[7]</sup>
- ICD 710<sup>[39]</sup>

The following table summarizes the changes made to V2 in developing V3.

**Table 71 - Data Encoding Specification V3 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Allow use of KDK.	Controlled Value Enumerations Constraint Rules ISM-ID-00122 ISM-ID-00123	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules.
2	Require appropriate foreign disclosure or release marking on classified national intelligence per ICD 710 <sup>[39]</sup> .	Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
3	Update references to E.O. 12958, as amended <sup>[23]</sup> to refer to NSI-EO.	Documentation Constraint Rules  ISM-ID-00013  ISM-ID-00014  ISM-ID-00017  ISM-ID-00018  ISM-ID-00019  ISM-ID-00020  ISM-ID-00021  ISM-ID-00023	Should not impact data. Will impact constraint checking systems since it changes the name of a condition.
4	Force ordering of SAR.	Constraint Rules  ISM-ID-00121	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
5	Update rules to exclude the resource element from being considered in rollup constraints.	Constraint Rules  ISM-CONTRIBUTES	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.



#	Change	Artifacts changed	Compatibility Notes
6	Update to use ISM-CONTRIBUTES instead of ISM-CONTRIBUTES-USA.	ISM-ID-00108 ISM-ID-00109 ISM-ID-00110 ISM-ID-00111 ISM-ID-00112 ISM-ID-00113 ISM-ID-00116	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
7	Update ISM-ID-00040 to allow for R portions in a USA document.	ISM-ID-00040	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release.
8	Update ISM-ID-00028 to allow use of NF with any classification type (i.e., US, non-US, and JOINT).	ISM-ID-00028	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release.
9	Update rules to prevent RELIDO on portions that do not have USA as one of the ownerProducers.	ISM-ID-00124	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
10	Remove ISM-ID-00022.	ISM-ID-00022	No impact rule was effectively a duplicate of ISM-ID-00011 due to CVE change in V1.
11	Reduce risk of using ISM.XML in a schema with xsd:anyAttribute.	ISM-ID-00125 ISM-ID-00126	Data could have been created that was valid under previous releases that may not be valid under this release.
12	Notices.	ISM-ID-00127 ISM-ID-00128 ISM-ID-00129 ISM-ID-00130 ISM-ID-00131 ISM-ID-00134 ISM-ID-00135 ISM-ID-00136 ISM-ID-00137 ISM-ID-00138 ISM-ID-00139 ISM-ID-00150 ISM-ID-00151 ISM-ID-00152 ISM-ID-00153	FISA, RD, FRD, IMCON, LIMDIS, LES, and LES-NF Data created under previous releases WILL not be valid under this release without adding the appropriate notice.
13	Clarify use of 25X1-human.	ISM-ID-00133	25X1-human data created under previous releases may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
14	Add check that RELIDO is required on all portions to appear in banner.	ISM-ID-00132	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
15	Add check that NF is not allowed on U portions.	ISM-ID-00140	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
16	Enforce E.O. 13526 <sup>[24]</sup> requirements for Authority block.	ISM-ID-00141 ISM-ID-00017 ISM-ID-00142 ISM-ID-00143	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
17	Incorporate LES and LES-NF markings.	ISM-ID-00066 ISM-ID-00145 ISM-ID-00146 ISM-ID-00147 ISM-ID-00148 ISM-ID-00149 ISM-ID-00150 ISM-ID-00151 ISM-ID-00152 ISM-ID-00153	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release.
18	Add rule for For Official Use Only (FOUO) compilation reason.	ISM-ID-00154	Data generation systems that correctly implement CAPCO guidance <sup>[7]</sup> and follow E.O. 13526 <sup>[24]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

## B.25 - V2 Change Summary

Significant drivers for Version 2 include:

- Executive Order 12958, as amended<sup>[23]</sup>(compilationReason)
- *Authorized Classification and Control Markings Register* v2.1<sup>[9]</sup>
- ISOO 32 CFR Parts 2001 and 2004 (Guidance on Type of Exempted Source [as of September 22, 2003])<sup>[52]</sup>

The following table summarizes the changes made to V1 in developing V2.

**Table 72 - Data Encoding Specification V2 Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Updated ISM.XML XSL rendering stylesheet to include new CAPCO changes such as removal of declass dates from banner.	Stylesheet	Data rendered using provided stylesheets will render differently.
2	Removed version number from file names.	Schema	Systems need to be updated to use the new file names.
3	Added ability for instance documents to specify DES versions used.	Constraint Rules Schema	Data generation systems need to be updated to include DES version(s) in output. Ingestion systems need to be updated to properly handle the new data. Schemas and/or DESs using ISM.XML need to implement the attribute appropriately.
4	Added <code>@ism:compilationReason</code> to indicate compilation and provide a reason that the element has an aggregate classification higher than its parts or a control marking has been applied that is not in the individual parts.	Schema	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
5	Expanded constraint rules to identify previously unrecognized data errors in accordance with the <i>Authorized Classification and Control Markings Register</i> v2.1 <sup>[9]</sup> .	Constraint Rules	Data generation systems that correctly implement CAPCO guidance <sup>[9]</sup> and follow E.O. 12958, as amended <sup>[23]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
6	Changed ISM.XML vocab warnings to errors, based on identification of specific CVE.	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance <sup>[9]</sup> and follow E.O. 12958, as amended <sup>[23]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
7	Updated constraint rules and schema documentation to specify data values for: <code>@ism:ownerProducer</code> , <code>@ism:SCIcontrols</code> , <code>@ism:SARIdentifier</code> , <code>@ism:disseminationControls</code> , <code>@ism:FGISourceOpen</code> , <code>@ism:FGISourceProtected</code> , <code>@ism:releasableTo</code> , <code>@ism:nonICmarkings</code> , <code>@ism:declassException</code> , <code>@ism:typeOfExemptedSource</code> .	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance <sup>[9]</sup> and follow E.O. 12958, as amended <sup>[23]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
8	Removed <code>@ism:declassManualReview</code> .	Constraint Rules ADD Mapping Table	Data generation systems should be updated to prohibit <code>@ism:declassManualReview</code> on new data. Ingestion systems need to be updated to reject <code>@ism:declassManualReview</code> on new data, or else they will accept invalid data. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

#	Change	Artifacts changed	Compatibility Notes
9	Changed definition of <b>@ism:declassException</b> and <b>@ism:typeOfExemptedSource</b> from NMTOKENS to NMTOKEN – single value instead of multiple values.	Schema	No changes to authoring/ generation or ingestion systems that correctly limit the attributes to single values. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
10	Added attributes to enable defining of the roles that ISM.XML attributes play in a document.  <b>@ism:resourceElement</b> , <b>@ism:excludeFromRollup</b>	Schema  Constraint Rules	Data generation systems need to be updated to include these attributes in output. Ingestion systems need to be updated to properly handle the new data. Schemas and/or DESs using ISM.XML need to implement these attributes appropriately.
11	Added attribute to enable ISM.XML date based rules.  <b>@ism:createDate</b>	Schema  Constraint Rules	Data generation systems need to be updated to include this attribute in output. Ingestion systems need to be updated to properly handle the new data. Schemas and/or DESs using ISM.XML need to implement this attribute appropriately.

## Appendix C List of Abbreviations

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

ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ACES	Access Control Encoding Specification
AEA	Atomic Energy Act
AG	Attorney General
ARH	Access Rights and Handling
CAD	Cryptologic Agencies Domain
CAPCO	Controlled Access Program Coordination Office
CES	Controlled Vocabulary Enumeration Encoding Specification
CFR	Code of Federal Regulations
CMIWG	Classification Marking Implementation Working Group
CNSI	Classified National Security Information
CNWDI	Critical Nuclear Weapons Design Information
CUI	Controlled Unclassified Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DHS	Department of Homeland Security
DN	Distinguished Name
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOS	U.S. Department of State
E.O.	Executive Order
ESB	Enterprise Standards Baseline
EXDIS	Exclusive Distribution



FBI	Federal Bureau of Investigation
FD&R	Foreign Disclosure & Release
FGI	Foreign Government Information
FOUO	For Official Use Only
GENC	Geopolitical Entities, Names, and Codes
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICO	Intelligence Community Only
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISCAP	Interagency Security Classification Appeals Panel
ISM	Information Security Markings
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
ISSM	Information Systems Security Manager
MIME	Media Type
MN	Mission Need Profile
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NITF	National Imagery Transmission Format
No Distribution	Data Encoding Specification for No Distribution Need-To-Know

NPE	Non-Person Entity
NTK	Need-To-Know Metadata
OC	Originator Controlled
OC-NTK	Originator Controlled Need-to-Know
OLA	Office of Legislative Affairs
ORCON	Originator Controlled
PE	Person Entity
PKI	Public Key Infrastructure
POC	Point of Contact
PROPIN	Proprietary Information
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SCI	Sensitive Compartmented Information
SMP	Security Markings Program
TS	Top Secret
U	Unclassified
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
USA	United States of America
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

## Appendix D Bibliography

[1] AUTHCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Authority Category (AUTHCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/JIMIYN5> (case sensitive – Juliet India Mike lima Yankee November 5 )

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

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

[2] CAPCO Register and Manual V6.0 AU

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 6.0 Administrative Update. 05 April 2013.

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

[3] CAPCO Register and Manual V6.0

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 6.0. 28 February 2013.

Available online on Interlink-U at: <https://w3id.org/ic/standards/policy/icmarkings> or [https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/CAPCO/CAPCO\\_Register%20and%20Manual%20v6.0\\_28%20Feb13\\_FOUO.pdf#search=CAPCO%20Register%20and%20Manual%20V6%2E0](https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/CAPCO/CAPCO_Register%20and%20Manual%20v6.0_28%20Feb13_FOUO.pdf#search=CAPCO%20Register%20and%20Manual%20V6%2E0)

[4] CAPCO Register and Manual V5.1

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 5.1. 30 December 2011.

[5] CAPCO Register and Manual V4.2

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register*. Version 4.2. 31 May 2011.

[6] CAPCO Register and Manual V4.1

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 4.1. 12 December 2012.

[7] CAPCO Register and Manual V3.1

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 3.1. 7 May 2010.

[8] CAPCO Register and Manual V2.2

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 2.2. 25 September 2009.

[9] CAPCO Register and Manual V2.1

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *Intelligence Community Authorized Classification and Control Markings Register and Manual*. Version 2.1. 5 January 2009.

[10] CAPCO Register and Manual Appendix A V6.0

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *CAPCO Manual Appendix A: Non-US Markings*. Version 6. Effective: 28 February 2013.

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

[11] CAPCO Register and Manual Appendix B V6.0

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *CAPCO Manual Appendix B NATO Protective Markings*. Version 6.0. Effective: 28 February 2013.

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

[12] CAPCO Register Annex A V5.1

Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *CAPCO Register Annex A Tetragraphs*. Version 5.1. Effective: 30 December 2011.

[13] CUI Category Registry

National Archives and Records Agency. *CUI Category Registry*.

Available online at: <https://www.archives.gov/cui/registry/category-list>

[14] 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>

[15] 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>

[16] DoD Instruction 5230.24

Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. Change 3, October 15, 2018.

Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf>

[17] DoD Directive 5240.01

Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.

Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524001p.pdf>

[18] DoD Instruction 5230.24

Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 23 August 2012.

23 August 2012 edition replaced the March 18, 1987.

Available online at: <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf>

[19] DoD Manual 5200.01

Under Secretary of Defense for Intelligence. *DoD Information Security Program (Vol 1-3)*:. 5200.01. February 24, 2012.

Vol 1 Available online at: [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m\\_vol1.pdf](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol1.pdf)

Vol 2 Available online at: [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m\\_vol2.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol2.pdf)

Vol 3 Available online at: [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m\\_vol3.pdf](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol3.pdf)

Vol 4 was replaced by DoDI 5200.48

[20] DoD Instruction 5200.48

Office of the Under Secretary of Defense for Intelligence and Security. *Controlled Unclassified Information (CUI)*. 5200.48. 6 March 2020.

Cancels: DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended

Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF>

[21] 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>

[22] E.O. 12829

The White House. *Executive Order 12829 – National Industrial Security Program, as Amended*. Federal Register, Vol. 58, No. 240. 14 December 1993.

Available online at: <https://www.archives.gov/isoo/policy-documents/eo-12829-with-eo-13691-amendments.html>

[23] E.O. 12958

The White House. *Executive Order 12958 - Classified National Security Information, as Amended*. Federal Register, Vol. 68, No. 60. 25 March 2003.

Available online at: <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>

[24] 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>

## [25] 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>

## [26] FAC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Fine Access Control (FAC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/uZz5l7T> (case sensitive – uniform Zulu zulu 5 India 7 Tango )

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

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

## [27] 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.

## [28] 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>

## [29] IC Markings JUN 2016

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 30 Jun 2016.

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>

## [30] IC Markings DEC 2016

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2016.

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>

## [31] 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>

## [32] IC Markings DEC 2014

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2014.

- Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>
- [33] IC Markings DEC 2013  
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2013.  
Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>
- [34] 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>
- [35] 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](http://www.dni.gov/files/documents/ICD/icd_208.pdf)
- [36] 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>
- [37] 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](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)
- [38] 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](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)
- [39] 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](http://www.dni.gov/files/documents/ICD/ICD_710.pdf)
- [40] 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](http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf)

[41] 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>

[42] 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](http://www.dni.gov/files/documents/ICPG/ICPG710-2_403-5.pdf)

[43] 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>

[44] 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>

[45] 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>

[46] IRM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Resource Metadata (IRM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pOKLbmx> (case sensitive – papa Oscar Kilo Lima bravo mike xray )

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

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

[47] ISM.ACES



Office of the Director of National Intelligence. *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*.

Available online Intelink-TS at: <https://go.ic.gov/rOG2Bjt> (case sensitive – romeo Oscar Golf 2 Bravo juliet tango )

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

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

[48] ISM-Rollup.XML

Office of the Director of National Intelligence. *Rollup Guidance for ISM*.

Available online Intelink-TS at: <https://go.ic.gov/ZHc3EsX> (case sensitive – Zulu Hotel charlie 3 Echo sierra Xray )

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

[49] ISMCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/mLf5WA9> (case sensitive – mike Lima Foxtrot 5 Whiskey Alpha 9 )

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

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

[50] ISO 3166-1

International Organization for Standardization (ISO). *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*. ISO 3166-1:2006.

Available online at: [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39719](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719)

[51] 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>

[52] ISOO 32 CFR Parts 2001 and 2004

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information (Directive No. 1); Final Rule*. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 28, No. 183. 22 September 2003.

Available online at: <https://www.gpo.gov/fdsys/pkg/FR-2003-09-22/pdf/03-24047.pdf>

[53] 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>

[54] ISOO 32 CFR Part 2002 Clarification Memo

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO 32 CFR Part 2002 Clarification Memo*. 4 June 2019.

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

[55] 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>

[56] 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>

[57] 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>

[58] ISOO Marking Booklet

Information Security Oversight Office. *Marking Classified National Security Information*. December 2010.

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

[59] ISOO Notice 2009-13

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2009-13: Prohibited Use of X1-X8 Markings*.

Available online at: <https://www.archives.gov/files/isoo/notices/notice-2009-13.pdf>

[60] ISOO Notice 2012-02

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2012-02: Classification Marking Instructions on the Use of "50X1-HUM" vs "25X1-human" as a Declassification Instruction*.

Available online at: <http://www.archives.gov/isoo/notices/notice-2012-02.pdf>

[61] ISOO Notice 2013-01

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2013-01: Further Marking Guidance on Commingling North Atlantic Treaty Organization (NATO) and Classified National Security Information (NSI)*.

Available online at: <http://www.archives.gov/isoo/notices/notice-2013-01.pdf>

[62] LIC.CES

Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/IsHgQxJ> (case sensitive – India sierra Hotel golf Quebec xray Juliet )

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

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

[63] MN.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Mission Need (MN.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/ndd7V1R> (case sensitive – november delta delta 7 Victor 1 Romeo )

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

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

[64] ORCON Memo

Director of National Intelligence. *Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities*. 29 March 2011.

ICPG 710.1 signed July 2012, rescinded the ORCON Memo.

Available online at: [https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings\\_ES%2000045.pdf](https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf)

Attachment A: <https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20A.pdf>

Attachment B: <https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20B.pdf>

Attachment C: <https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20C.pdf>

[65] PE-Portal

*ODNI/Partner Engagement Tetragraph Portal*. Office of the Director of National Intelligence

Available online Intelink-TS at: <https://intellipedia.intelink.ic.gov/wiki/Portal:Tetragraphs>

Available online Intelink-S at: <https://intellipedia.intelink.sgov.gov/wiki/Portal:Tetragraphs>

[66] 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>

[67] RegularExpressions

Michael Fitzgerald. O'Reilly Media, Inc.. *Introducing Regular Expressions*.

Available online at: <https://www.oreilly.com/library/view/introducing-regular-expressions/9781449338879/ch01.html>

[68] ROLE.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Role (ROLE.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/GknYELv> (case sensitive – Golf kilo november Yankee Echo Lima victor )

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

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

[69] 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/>

[70] UIAS.XML

Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1 )

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

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

[71] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/wmyIRCV> (case sensitive – whiskey mike yankee India Romeo Charlie Victor )

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

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

[72] XPath2

World Wide Web Consortium (W3C). *XML Path Language (XPath) 2.0 (Second Edition)*. W3C Recommendation 14 December 2010 (Link errors corrected 3 January 2011).

Available online at: <http://www.w3.org/TR/xpath20/>

[73] 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/>

## Appendix E 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 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](mailto:ic-standards-support@odni.gov).

## Appendix F IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC ESB as defined in ICS 500-20<sup>[44]</sup>.