



# **Intelligence Community Technical Specification**

---

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

**Version 2016-SEPr2017-JUL**

July 21, 2017

Distribution Notice:

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

# Table of Contents

Chapter 1 - Introduction .....	1
1.1 - Purpose .....	1
1.2 - Scope .....	1
1.3 - Background .....	1
1.4 - Enterprise Need .....	2
1.5 - Audience and Applicability .....	3
1.6 - Conventions .....	3
1.6.1 - Language .....	3
1.6.2 - Typography .....	4
1.6.3 - Terminology .....	4
1.6.4 - XML Namespaces .....	4
1.7 - Dependencies .....	4
1.7.1 - Types of Dependencies .....	4
1.7.2 - Specification Dependencies .....	5
1.7.3 - Standalone and Convenience Packages .....	7
1.7.4 - Inverse Dependencies .....	8
1.8 - Conformance .....	8
1.9 - Version Policies .....	9
1.9.1 - XML Namespace Policy .....	9
1.9.2 - Version Numbering .....	9
Chapter 2 - Development Guidance .....	11
2.1 - Understanding Access Control .....	11
2.2 - Relationship to Abstract Data Definition and other encodings .....	12
2.3 - ISM and Access Control .....	12
2.4 - Additional Guidance .....	13
2.4.1 - Document Compliance and Exemptions .....	13
2.4.2 - Physical XML Attribute Groups .....	13
2.4.3 - Notices .....	14
2.4.3.1 - US-Person .....	15
2.4.3.2 - Point Of Contact Requirements .....	15
2.4.3.3 - pre13526ORCON .....	16
2.4.4 - Originator Controlled Assets .....	16
2.4.5 - Section and Portion Style Marking Limitations .....	17
2.4.6 - NATO NAC Markings .....	17
2.4.7 - ISM Types .....	18
2.4.8 - ISM Attributes .....	18
2.4.9 - ISM Attribute Groups .....	28
2.5 - CSV Notes .....	32
2.6 - JSON Notes .....	33
Chapter 3 - Definitions, Interfaces, and Constraints .....	34
3.1 - Constraint Rule Types .....	34
3.2 - "Living" Constraint Rules .....	34
3.3 - Classified or Controlled Constraint Rules .....	34
3.4 - Constraint Terminology .....	34
3.5 - Errors and Warnings .....	35
3.6 - Rule Identifiers .....	35

3.7 - Data Validation Constraint Rules .....	35
3.7.1 - Purpose .....	35
3.7.2 - Schematron .....	36
3.7.3 - Non-null Constraints .....	36
3.7.4 - Value Enumeration Constraints .....	36
3.7.5 - Additional Constraints .....	37
3.7.5.1 - DES Constraints .....	37
3.7.5.2 - Revision Constraints .....	37
3.7.6 - Constraint Rules .....	39
3.8 - Data Rendering Constraint Rules .....	39
3.8.1 - Purpose .....	39
3.8.2 - Rendering Constraint Rules .....	39
Chapter 4 - Conformance Validation .....	40
4.1 - Schema Validation .....	40
4.2 - Business Rule Validation .....	40
Chapter 5 - Generated Guides .....	41
5.1 - Schema Guide .....	41
5.2 - Schematron Guide .....	42
Appendix A - Feature Summary .....	43
A.1 - ISM Feature Summary .....	43
Appendix B - Change History .....	50
B.1 - V2016-SEPr2017-JUL Change Summary .....	51
B.2 - V2016-SEP Change Summary .....	55
B.3 - V2015-AUG Change Summary .....	59
B.4 - V2014-DEC Change Summary .....	61
B.5 - V13 Change Summary .....	64
B.6 - V12 Change Summary .....	65
B.7 - V11 Change Summary .....	69
B.8 - V10 Change Summary .....	71
B.9 - V9 Change Summary .....	79
B.10 - V8 Change Summary .....	82
B.11 - V7 Change Summary .....	85
B.12 - V6 Change Summary .....	88
B.12.1 - V6 Change Errata .....	93
B.13 - V5 Change Summary .....	93
B.13.1 - V5 Change Errata .....	100
B.14 - V4 Change Summary .....	100
B.15 - V3 Change Summary .....	102
B.16 - V2 Change Summary .....	107
Appendix C - List of Abbreviations .....	111
Appendix D - Bibliography .....	114
Appendix E - Points of Contact .....	122
Appendix F - IC CIO Approval Memo .....	123

## List of Figures

Figure 1 - Related Specifications .....	7
Figure 2 - Inverse Dependency Specifications .....	8
Figure 3 - Three-legged Stool of Access Decisions .....	11

## List of Tables

Table 1 - XML Namepaces .....	4
Table 2 - Dependencies .....	5
Table 3 - NAC Conversions .....	17
Table 4 - ISM Simple Types .....	18
Table 5 - ISM Complex Types .....	18
Table 6 - ISM Attributes .....	18
Table 7 - ISMNoticeBaseAttributeGroup .....	29
Table 8 - ISMNoticeAttributeGroup .....	29
Table 9 - ISMNoticeExternalAttributeGroup .....	29
Table 10 - ISMResourceAttributeGroup .....	29
Table 11 - ISMResourceAttributeOptionGroup .....	29
Table 12 - ISMRootNodeAttributeGroup .....	30
Table 13 - ISMRootNodeAttributeOptionGroup .....	30
Table 14 - NoticeAttributeGroup .....	30
Table 15 - NoticeAttributesOptionGroup .....	30
Table 16 - NoticeExternalAttributesGroup .....	30
Table 17 - NoticeExternalAttributesOptionGroup .....	30
Table 18 - POCAAttributeGroup .....	30
Table 19 - ResourceNodeAttributeGroup .....	31
Table 20 - ResourceNodeAttributeOptionGroup .....	31
Table 21 - SecurityAttributeGroup .....	31
Table 22 - SecurityAttributesOptionGroup .....	32
Table 23 - Numerical Rule Identifier Ranges .....	35
Table 24 - Revision Constraints table .....	38
Table 25 - Constraint Rules .....	39
Table 26 - ISM Dependency over Time .....	43
Table 27 - Feature Summary Legend .....	43
Table 28 - ISM Feature Comparison .....	43
Table 29 - DES Version Identifier History .....	50
Table 30 - Data Encoding Specification 2016-SEPr2017-JUL Change Summary .....	51
Table 31 - Data Encoding Specification 2016-SEP Change Summary .....	55
Table 32 - Data Encoding Specification 2015-AUG Change Summary .....	59
Table 33 - Data Encoding Specification 2014-DEC Change Summary .....	62
Table 34 - Data Encoding Specification V13 Change Summary .....	65
Table 35 - Data Encoding Specification V12 Change Summary .....	66
Table 36 - Data Encoding Specification V11 Change Summary .....	70
Table 37 - Data Encoding Specification V10 Change Summary .....	72
Table 38 - Data Encoding Specification V9 Change Summary .....	79
Table 39 - Data Encoding Specification V8 Change Summary .....	82
Table 40 - Data Encoding Specification V7 Change Summary .....	86
Table 41 - Data Encoding Specification V6 Change Summary .....	88
Table 42 - Data Encoding Specification V6 Change Errata .....	93
Table 43 - Data Encoding Specification V5 Change Summary .....	94
Table 44 - Data Encoding Specification V5 Change Errata .....	100
Table 45 - Data Encoding Specification V4 Change Summary .....	101
Table 46 - Data Encoding Specification V3 Change Summary .....	102

Table 47 - Data Encoding Specification V2 Change Summary .....	108
--	-----

## 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) 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 marking concepts using XML.

### 1.2 - Scope

This specification applies to the Intelligence Community (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 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* <sup>[31]</sup> grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common Information Technology (IT) standards, protocols, and interfaces, to establish uniform information security standards, and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* <sup>[38]</sup> the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* <sup>[2]</sup>. Many IC encoding specifications are based on XML,

but other technologies are possible. For example, IC-ID<sup>[28]</sup> defines a plain-text format for IC Identifiers as well as an associated XML structure.

## 1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata (including information security markings) to allow 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.

Early in the intelligence life cycle, intelligence producers need:

- User interfaces that help reliably assign and manipulate information security markings.
- Automated formatting of the IC’s classification and control marking system as defined by Executive Order (E.O.) 13526, *Classified National Security Information*, <sup>[20]</sup> ICD 710 Classification and Control Marking System,<sup>[33]</sup> and implemented by the IC Markings System Register and Manual.<sup>[22]</sup> This includes portion marks, security banners, the classification authority block, and other security control markings.
- Cross-domain discovery, access, and dissemination capabilities.

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

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan<sup>[21]</sup>
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer<sup>[31]</sup>
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC<sup>[32]</sup>

- Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information<sup>[38]</sup>
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility<sup>[29]</sup>
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination<sup>[30]</sup>
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide<sup>[36]</sup>
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System<sup>[33]</sup>
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control<sup>[34]</sup>
  - Intelligence Community Policy Guidance (ICPG) 710.2, Application of Dissemination Controls: Foreign Disclosure and Release Markings<sup>[35]</sup>

## 1.5 - Audience and Applicability

This is a data encoding specification. It defines the structure and related business rules for encoding the described data type. A DES is intended for those developing tools and services that create, modify, store, exchange, search, display, or further process the type of data being described.

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,<sup>[37]</sup> defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,<sup>[16]</sup> requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

## 1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

### 1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in IETF RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels."<sup>[39]</sup> When these words appear in regular case, they are meant in their natural-language sense.

## 1.6.2 - Typography

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

## 1.6.3 - Terminology

For an implementation to conform to this specification, it **MUST** adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

## 1.6.4 - 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

## 1.7 - Dependencies

### 1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

Dependency	Directly or transitively influenced by.  Examples:  1. A is influenced by B therefore B is a dependency of A.  2. A is influenced by B and B is influenced by C; therefore C is a dependency of A.
Direct Dependency	Explicit influence.  Example: A influences B.

Inverse Dependency      Directly or transitively influences.

Example: B influences A.

## 1.7.2 - Specification Dependencies

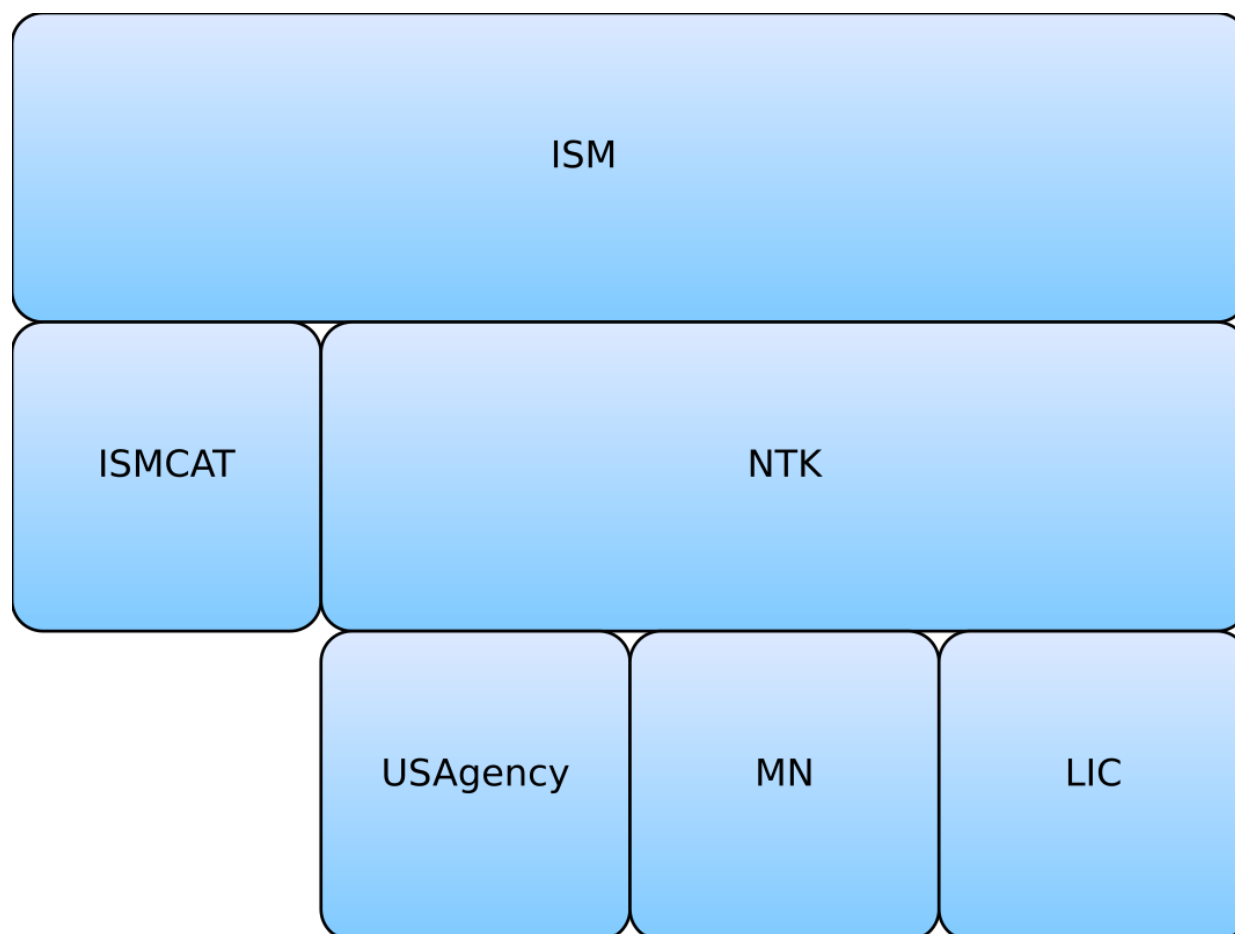
This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g. Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the IC CIO specifications related to this specification. The graphic depicts direct dependencies (see [Direct Dependency](#)). 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 specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all direct dependencies.

**Table 2 - Dependencies**

Name	Dependency Description
December 2016 IC Markings System Register and Manual <sup>[24]</sup>	Policy Driver
DoD Manual 5200.1 February 2012 <sup>[17]</sup>	Policy Driver
<i>XML Data Encoding Specification for Need-To-Know Metadata</i> (NTK.XML.V2015-AUG+) <sup>[49]</sup>	The specification does not depend on a specific version of Need To Know (NTK.XML); NTK.XML versions later than version 2015-AUG MAY be used. The minimum version was based on a technical dependency; The structural changes in NTK.
<i>CVE Encoding Specification for ISM Country Codes and Tetragraphs</i> (ISMCAT.CES.V2017-JUL+) <sup>[40]</sup>	The specification does not depend on a specific version of ISM Country Codes and Tetragraphs (ISMCAT.CES); ISMCAT.CES versions later than version 2017-JUL MAY be used. The minimum version was based on a technical dependency; The use of the decomposed tetragraph CVE.

Name	Dependency Description
Schematron <sup>[52]</sup>	<p>Schematron — ISO/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 <b>MUST</b> 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 <b>MAY</b> 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 XSLT 2.0<sup>[57]</sup> query binding.</p>
<p>XSLT 2.0<sup>[57]</sup> implementation of Schematron<sup>[52]</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 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 <b>MAY</b> use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator <b>MUST</b> 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>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the ISM CVEs is normative.



**Figure 1 : Related Specifications**

### 1.7.3 - Standalone and Convenience Packages

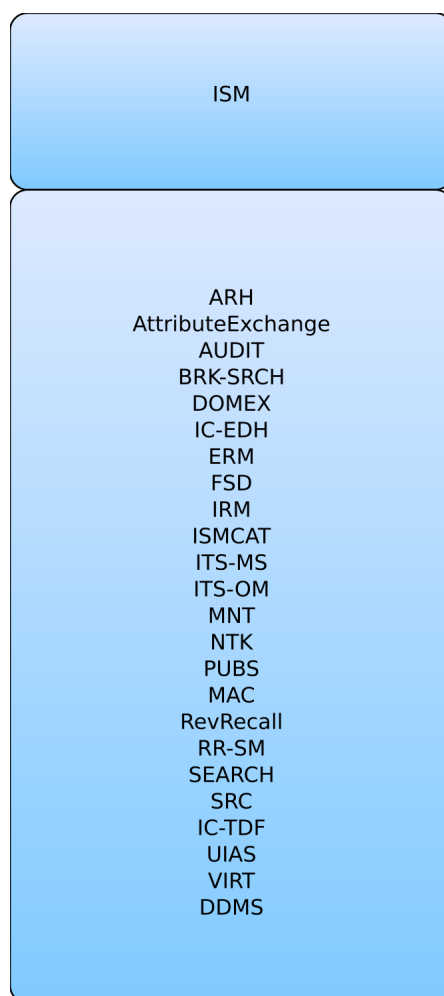
The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all direct dependent (see [Direct Dependency](#)) specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

Convenience packages convey all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

## 1.7.4 - Inverse Dependencies

Generally, it is only necessary to think of the *direct dependencies* (see [Direct Dependency](#)) in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies* (see [Inverse Dependency](#)), 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.

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 dependency relationships and how changes in a specification may impact others. This diagram is representative of dependencies at the time of the release of this specification, but are subject to change over time.



**Figure 2 : Inverse Dependency Specifications**

## 1.8 - Conformance

For an implementation to conform to this specification, it **MUST** adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

The CVE values from the XML CVE files, the XSL transformations behavior, and the Schematron<sup>[52]</sup> rules are normative for this specification. The rest of this document and the rest of this package, including the XML Schema, the SchemaGuide, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119<sup>[39]</sup> is considered normative within the scope of the sentence. All other parts of this document are informative.

Additional guidance that is either classified or has handling controls can be found in separate annexes distributed to the appropriate networks and environments as necessary. Systems and services operating in those environments **MUST** consult the appropriate annexes.

## 1.9 - Version Policies

### 1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from “The Disposition of Names in an XML Namespace.”<sup>[53]</sup> This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 “Versioning and XML namespace policy” of “Architecture of the World Wide Web, Volume One.”<sup>[54]</sup>

There is a version attribute (e.g. **@DESVersion**, **@CESVersion**, **@TESVersion**, **@version**) for each namespace defined in an IC CIO specification. Version attributes are used to capture the specification version number the specification author intends an instance to conform to. Namespaces do not change, so the version attribute is required to fully understand an instance document.

As changes to the specification are released, the version number captured in the “version” attribute increments. See [Section 1.9.2 - Version Numbering](#) for information on the numbering scheme.

This XML namespace policy only applies to the namespaces defined in this specification, any namespaces that are included by reference should define their own namespace policy.

### 1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-**MMM**). This provides a temporal representation of when the specification was released. Revisions to a version of the specification also use a year-month structure (e.g., YYYY-**MMM**). When the version number is used in the version attribute, the expression follows the Augmented Backus-Naur Form<sup>[1]</sup> below:

## Version Format when used in the version attribute:

- [1] Version ::= [Year Month](#)["." [Revision](#) ] ["-" [CustomizationSuffix](#) ]
- [2] VersionYear ::= 4( DIGIT )
- [3] VersionMonth ::= 2( DIGIT )
- [4] Customization ::= 1\*23(ALPHA / DIGIT / "\_" )  
Suffix
- [5] RevisionYear ::= 4( DIGIT )
- [6] RevisionMonth ::= 2( DIGIT )  
h
- [7] Revision ::= [Year Month](#)

## Version in XML Lexicon

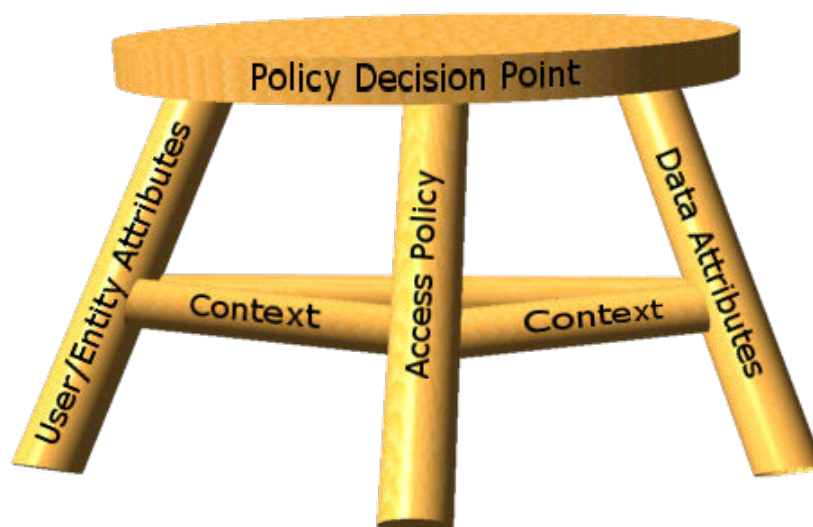
The following vocabulary helps explain the meaning of terms used in the version documentation, and it may further constrain the set of allowable values:

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version/revision being referenced.
VersionYear	The four digit year from the version of the specification being referenced.
VersionMonth	The 2 digit month from the version of the specification being referenced.
CustomizationSuffix	An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.
RevisionYear	The four digit year from the revision of the specification being referenced.
RevisionMonth	The 2 digit month from the revision of the specification being referenced.
Revision	The Year and Month from the revision of the specification being referenced. Revisions are modifications to Versions.

## Chapter 2 - Development Guidance

### 2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions are based upon three components (data attributes, user attributes, and access control policies) and are held together by the context in which the access control decision is made. The context itself includes various elements, such as the environment, temporal state, and method of access, that together provide the Where, When, and How details of the access request. The context, together with the user making the request and the data/repository/application being requested (the Who and What respectively), make up the framework that supports an access control decision. Access Policy **SHOULD** be constrained to use data attributes, user attributes, and context information. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. An entity **MUST** meet all criteria in the framework to be granted access. The concept of the access control decision framework is depicted in [Figure 3](#).



**Figure 3 : Three-legged Stool of Access Decisions**

All of these parts come together to create a tri-legged stool of access control. When a stool is missing one of the components of its frame, it is unable to function properly. The same is true of access control. Without each component of the framework, access control falls apart. Each component is crucial to make accurate, reliable, and automated access control decisions. Each IC CIO document will address a piece of the framework of access control decisions.

This specification addresses matters dealing with data and it falls into the data attributes leg of the access control framework. Data attribute specifications include: Access Rights and Handling

(ARH), Information Security Marking (ISM), CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT), and Need-To-Know Metadata (NTK), (which includes, but is not limited to, profiles for Intelligence Community Only, Originator Control, and Proprietary Information).

## 2.2 - Relationship to Abstract Data Definition and other encodings

The relationship of the XML structures defined in this encoding specification to the abstract terms defined in the ADD are described using a mapping table in the ADD. The mapping tables generally show the mapping to the encoding specification where a structure is defined, not where it is used. These mappings are provided for reference only. The complete set of encoding specification artifacts, both normative and informative, should be consulted in order to gain a complete understanding of this encoding specification.

The mappings in the ADD provide a starting point for the development of automated transformations between formats defined by the encoding specifications. However, it should be noted that when these transformations are used between formats with different levels of detail there might be some data loss.

## 2.3 - ISM and Access Control

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

1. Markings about the resource such as classification:

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

NTK represents additional rules that may or may not require additional data.

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

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) is an example of a specification of markings about Persons and NPEs.

3. Rules or policy for granting access based on the markings (ISM-ACES, NTK Policies):

The ACES associated with ISM is the Access Control Encoding Specification for ISM (ISM-ACES).

A resource could additionally have Need To Know (NTK) associated with it, and this would add additional ACES constraints on access to the resource. See the NTK DES for details on how to interpret from the NTK markings which additional ACES are required in order to satisfy requirements for resource access.

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

## 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 - Document Compliance and Exemptions

ISM documents claim compliance with rule sets using the **@compliesWith** attribute on the resource node of a document; **@compliesWith** MUST be specified. This is a multi-valued attribute, and the acceptable values are U.S. Government ("USGov"), U.S. IC ("USIC"), U.S. Department of Defense ("USDOD"), 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 USA produced documents must comply with. All documents that contain [USA] in the <b>@ism:ownerProducer</b> field of the resource node MUST contain USGov in <b>@ism:compliesWith</b> .
USIC	The rule set for documents that comply with US Intelligence Community policies. Documents that assert USIC MUST assert USGov.
USDOD	The rule set for documents that comply with US DOD policies. Documents that assert USDOD MUST assert USGov.
OtherAuthority	The rule set for documents that comply with policies not covered by USGov, USIC, or USDOD. Currently, there are no rules in the Other Authority 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 and Release (FD&R), and a USDOD document may claim exemption from DoD 5230.24 using **@exemptFrom** on the resource node. The acceptable values are IC\_710\_MANDATORY\_FDR and DOD\_DISTRO\_STATEMENT.

### 2.4.2 - Physical XML Attribute Groups

The ISM.XML schema defines several attribute groups. These attribute groups are intended to be referenced by other DESs (e.g., Information Resource Metadata or Intelligence Publications) to incorporate the information security marking attributes as needed.

- **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.
- **SecurityAttributesGroup** lists the attributes **@classification** and **@ownerProducer** as required. It is the "normal" group to apply to a portion or resource mark element where classification is required.

- **ResourceNodeAttributeGroup** is used on the resource node of an implementing schema and includes **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>[33]</sup>
- **ISMRootNodeAttributeGroup** is used on the root node of the implementing schema to ensure the DES version is specified.
- **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.
- **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.
- **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 **@pocType** attribute.

The attribute **@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 unclassified (U) and the document with the source citation is U.

## 2.4.3 - Notices

The **ISMNoticeAttributesGroup** 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 **NoticeAttributesGroup** and the **NoticeAttributesOptionGroup** contain all of the attributes in the **ISMNoticeAttributesGroup** as well as the security marking attributes defined in the **SecurityAttributesGroup** and the **SecurityAttributesOptionGroup**, respectively. The **ISMNoticeAttributesGroup** is comprised of the following attributes:

- The attribute **@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 System Register and Manual,<sup>[22]</sup> as well as additional well-defined and formally recognized security notice types described in other directives, such as US-Person and DoD Distribution. The permissible values for this attribute are defined in the Controlled Value Enumeration (CVE) CVEnumISMNotice.xml.
- The attribute **@noticeDate** specifies the date associated with the notice, such as the date it was issued.
- The attribute **@noticeReason** specifies the reason a notice was issued.

- The attribute **@unregisteredNoticeType** is used to represent notices that are not categorized according to the IC Markings System Register and Manual<sup>[22]</sup> and/or notices with values that do not appear in CVEnumISMNotice.xml. This attribute can be used to designate specification-specific security notices that may not be sufficiently defined to be recognized by SMP.

ISM provides constraint checking for the **@noticeType** attribute, requiring that there be a matching 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, ISM includes elements that can represent a set of notices. The element **NoticeList** is comprised of one or more **Notice** elements, which use the **NoticeAttributesGroup** to provide additional information about each notice. The actual contents of a notice message is contained within the **Notice** sub-element **NoticeText**. The **POCAttributeGroup** included on **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 to benefit from the constraint checking that ISM 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 **@noticeType** attribute with a value of "FISA" and one with the **@unregisteredNoticeType** attribute with some appropriate string value, such as "Language."

Applying the **@noticeType** attribute does not remove the obligation to put the appropriate required text in the notice element. For example, only placing the **@noticeType** attribute with the value of RD, without including RD data in **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.

### 2.4.3.1 - US-Person

The value [US-Person] in the **@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.

### 2.4.3.2 - 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 **@noticeType** value of [POC] to indicate that the contents of a **Notice** are used to provide contact information. The

**@pocType** attribute indicates that the text of the **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.

### 2.4.3.3 - pre13526ORCON

Executive Order 13526, 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, classified ORCON documents created prior to the effective date of the order 25 June 2010 should be handled according to E.O. 12958, as amended, and documents created after this date should be handled according to E.O. 13526. 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>[19]</sup> as amended, and this statement MUST be marked with the **@noticeType** attribute value [pre13526ORCON]. The attribute indicates that the document contains ORCON information that predates E.O. 13526,<sup>[20]</sup> and the text of the **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>
```

### 2.4.4 - 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 for NTK which provides a defined structure for indicating the approved for dissemination agencies and organizations.

[OC-USGOV] may have 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.

## 2.4.5 - Section and Portion Style Marking Limitations

There are limitations to consider specific to ISM 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 Schematron cannot determine the difference between a **Section** and a **Portion** marked with ISM 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.

## 2.4.6 - NATO NAC Markings

North Atlantic Council (NAC) Activities are represented in ISM as an NMToken created from the activity name. To create an NMToken from an activity name:

1. Replace the slash following 'NATO' with a colon
2. Replace spaces with underscores

The following ABNF rules explicitly define the content of NAC and are used to provide a formal description independent of any particular technology. It is important to note that ABNF strings are case-insensitive, therefore all components of the NAC attribute are case-insensitive. ALPHA is defined to be A-Z / a-z. The ABNF rules used to specify the format of (NAC) Activities are normative:

### NAC encoding Format

- [8] NATO/NAC : : = "NATO:" [NAC](#)  
 [9] NAC : : = 1\*256(ALPHA / DIGIT / "\_" )

Example conversions:

**Table 3 - NAC Conversions**

NAC	Converted for use in ISM
NATO/Partnership for Peace	NATO:Partnership_for_Peace
NATO/KFOR	NATO:KFOR
NATO/PFP	NATO:PFP

## 2.4.7 - ISM Types

ISM 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 ISM, the complex types are used primarily to add ISM attributes in addition to the basic value field simple type.

**Table 4 - ISM Simple Types**

Name	Type
<b>@ism:LongStringType</b>	xsd:string maxLength 32000
<b>@ism:ShortStringType</b>	xsd:string maxLength 256

**Table 5 - ISM Complex Types**

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

## 2.4.8 - ISM Attributes

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

**Table 6 - ISM Attributes**

Attribute	Type	Description
<b>@ism:atomicEnergyMarkings</b>	xsd:tokens	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

Attribute	Type	Description
<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:tokens	The ISM rule sets a document complies with
<b>@ism:createDate</b>	xsd:date	The date when ISM metadata was added or updated  This date is used by some constraint rules to determine if ISM markings are valid. For example, this date is used to check deprecation of some marks.

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:derivativelyClassified By</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
<b>@ism:derivedFrom</b>	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 style="padding-left: 40px;">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>
<b>@ism:DESVersion</b>	xsd:string conforming to regular expression: ^201508(\-{1,23})?\$	<p>The version number of the DES</p> <p>If there are multiple <b>@ism:DESVersion</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:displayOnlyTo</b>	xsd:tokens	<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:tokens	Applicable dissemination control markings for a document or portion
<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:tokens	<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>

Attribute	Type	Description
<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>
<b>@ism:FGIsourceOpen</b>	xsd:tokens	<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:tokens	<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:ISMATCESVersion</b>	xsd:string conforming to regular expression: ^201505(\-{1,23})?\$	<p>The version number of the ISMCAT CES 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>
<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

Attribute	Type	Description
<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:tokens	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:tokens	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:noticeReason</b>	xsd:string maxLength 2048	A reason associated with a notice (for example, the DoD Distribution reason)
<b>@ism:noticeType</b>	xsd:tokens	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 Intelligence Community Markings System Register and Manual, as well as additional well-defined and formally recognized security notice types described in other directives, such as US-Person and DoD Distribution.

Attribute	Type	Description
<b>@ism:ownerProducer</b>	xsd:tokens	<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>@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:tokens	<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 purposes would have the <b>@ism:pocType</b> value of "ICD-710".</p>
<b>@ism:releasableTo</b>	xsd:tokens	<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>

Attribute	Type	Description
<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.</p>
<b>@ism:SARIdentifier</b>	xsd:tokens	The set of applicable SAR identifiers for the containing document or portion
<b>@ism:SCIcontrols</b>	xsd:tokens	The set of applicable SCI controls for the containing document or portion
<b>@ism:unregisteredNoticeType</b>	xsd:string maxLength 2048	<p>A notice that is of a category not described in the IC Markings System Register and Manual and/or is not sufficiently defined to be represented in the Controlled Value Enumeration CValueEnumISMNotice.xml</p> <p>This attribute can be used by specifications that import ISM to represent a wider variety of security-related notices.</p>

## 2.4.9 - ISM Attribute Groups

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

**Table 7 - ISMNoticeBaseAttributeGroup**

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

**Table 8 - ISMNoticeAttributeGroup**

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

**Table 9 - ISMNoticeExternalAttributeGroup**

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

**Table 10 - ISMResourceAttributeGroup**

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

**Table 11 - 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 - ISMRootNodeAttributeGroup**

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

**Table 13 - ISMRootNodeAttributeOptionGroup**

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

**Table 14 - NoticeAttributeGroup**

Attribute	Required
<a href="#">ISMNoticeAttributeGroup</a>	Not Required
<a href="#">SecurityAttributeGroup</a>	Not Required

**Table 15 - NoticeAttributesOptionGroup**

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

**Table 16 - NoticeExternalAttributesGroup**

Attribute	Required
<a href="#">ISMNoticeExternalAttributeGroup</a>	Not Required
<a href="#">SecurityAttributeGroup</a>	Not Required

**Table 17 - NoticeExternalAttributesOptionGroup**

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

**Table 18 - POCAAttributeGroup**

Attribute	Required
@ism:pocType	Not Required

**Table 19 - ResourceNodeAttributeGroup**

Attribute	Required
<a href="#">ISMResourceAttributeGroup</a>	Not Required
<a href="#">SecurityAttributeGroup</a>	Not Required
<a href="#">ISMNoticeAttributeGroup</a>	Not Required

**Table 20 - ResourceNodeAttributeOptionGroup**

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

**Table 21 - SecurityAttributeGroup**

Attribute	Required
@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

**Table 22 - SecurityAttributesOptionGroup**

Attribute	Required
@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

## 2.5 - CSV Notes

There are Comma Separated Value files provided for all of the CVEs. They are in the CVE folder with the XML and JSON versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence.



### Important

The CSV files on many systems will open “automatically” in Microsoft Excel; the default opening however, will not correctly read UTF-8 special characters. These are found in some country names such as “Republic of Côte d’Ivoire”. If you need to use a CVE that contains such special characters, or you think may contain such characters in Excel, you should:

- Open Excel to a blank sheet
- Under the Data menu choose to get external data from a text file
- Choose UTF-8 as the file origin
- Choose delimited as the format
- Choose next
- Change from tab to Comma as the delimiter
- Finish import to get the data in with the UTF-8 Characters properly encoded in Excel.

## 2.6 - JSON Notes

There are JSON format files provided for all of the CVEs. They are in the CVE folder with the XML and CSV versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence. The JSON files are formatted using JSON-LD based on a proposed method for JSON in NIEM.

## Chapter 3 - Definitions, Interfaces, and Constraints

### 3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

### 3.2 - "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>[33]</sup> implemented in the IC Markings System Register and Manual,<sup>[22]</sup> ISOO 32 CFR Parts 2001 and 2004 (as of September 22, 2003),<sup>[43]</sup> E.O. 13526, as amended,<sup>[20]</sup> and E.O. 12829, as amended.<sup>[18]</sup> These rules will be expanded and modified as the model matures, the IC Markings System Register and Manual<sup>[22]</sup> 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.

### 3.3 - Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the encoding specification artifacts wherever they are located.

### 3.4 - Constraint Terminology

For the purposes of this document, the following statements apply:

- The term "is specified" indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term "must be specified" indicates that an attribute **MUST** be applied to an element and the attribute **MUST** have a non-null value.

- The term “is not specified” indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.
- The term “must not be specified” indicates that an attribute MUST NOT be applied to an element.

## 3.5 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is more severe and is indicative of a clear violation of a constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

Each system responsible for processing a document (e.g., create, modify, transform, or exchange) MUST make a mission-appropriate decision about using a document with errors or warnings based on mission needs.

## 3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. ISM.XML data validation constraint rule identifiers are prefixed with “ISM-ID-” and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in [Table 23](#). As the constraint rules are managed over time, IDs from deleted rules will not be reused.

**Table 23 - Numerical Rule Identifier Ranges**

Rule Identifier Range		Description
Start	End	
00001	09999	Reserved for Unclassified constraint rules
10001	19999	Reserved for Unclassified but For Official Use Only (FOUO) constraint rules
20001	20999	Reserved for constraint rules classified at the “Secret//REL USA, FVEY” level
21001	21999	Reserved for constraint rules classified at the “Secret//NF” level
22001	29999	Reserved for constraint rules classified at the “Secret//TBD” level
30001 and above		Reserved for constraint rules classified with other classifications

## 3.7 - Data Validation Constraint Rules

### 3.7.1 - Purpose

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.

### 3.7.2 - Schematron

Schematron<sup>[52]</sup> is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document **MUST** meet, 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, and 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 *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

For better understanding, the Schematron<sup>[52]</sup> rules for this specification may be executed in *Oxygen*<sup>[51]</sup> or with an XSLT 2.0-compliant processor using the XSLT 2.0<sup>[57]</sup> transforms in the Schematron implementation from Rick Jelliffe (see [XSLT 2.0 implementation of Schematron by Rick Jelliffe](#) in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0<sup>[56]</sup> and XSLT 2.0<sup>[57]</sup> features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:<sup>[48]</sup>

By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this.



#### Note

For convenience, the specification package provides the XSLT 2.0<sup>[57]</sup> implementation of Schematron<sup>[52]</sup> along with a compiled version of the rules.

### 3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) **MUST** have content, other than white space.<sup>1</sup> Elements, which are allowed to only have text content, **MUST** have text content specified.

### 3.7.4 - Value Enumeration Constraints

Several elements and attributes of the ISM.XML model use Controlled Vocabulary Enumerations (CVEs) to define the data allowed in the element or attribute. In some cases the specific CVE is

<sup>1</sup>“White space” is defined in XML 1.0<sup>[55]</sup> as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

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.

## 3.7.5 - Additional Constraints

### 3.7.5.1 - DES Constraints

The DES version is specified through attributes on the root element. The schema constrains the values of these attributes. The **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.

### 3.7.5.2 - Revision Constraints

When validating an instance document against the validation rule sets and schema provided by the specification there is a certain philosophy that SHOULD be applied to both protect the data and the systems processing that data. This validation philosophy consists of the following seven basic rules that describe how the DESVersion matters to validation:

1. One MUST NOT validate with rules older than the integer version declared in an instance; this is an error.
2. One MAY validate with rules that are of a greater integer version than an instance.
3. When validating an instance with a lower integer version number than that of the validation rules, there MAY be a minimum integer version cutoff for a set of rules. If such a limit exists, this is an error.
4. Within an integer, validation MUST only occur with the newest decimal value implemented by the validator; that is a validator MUST only implement one signed validation rule set within an integer and it SHOULD be the latest.
5. When a validator detects an instance document claiming a version newer than what is implemented in the validator, a notice/log SHOULD be generated so a human can evaluate if the validator needs to be updated to the latest rule set, as passing the old rules MAY not comply with current law or policy.

6. A validator SHOULD document and communicate all versions and revisions it accepts, including the constraints (business/policy rules, allowed values, schema formats, etc.) in each of those versions.

The matrix of fictional generic examples in [Table 24](#) are provided to illustrate these validation concepts with the following assumptions:

- Version 11: Technically incompatible with newer versions
- Version 12: Technically compatible with newer versions, but retired from the Enterprise Standards Baseline
- Version 13: Oldest in the Enterprise Standards Baseline
- Version 13.201701: Revision to version 13
- Version 13.201804: Revision to version 13
- Version 201508: Standard release
- Version 201609: Latest version release

**Table 24 - Revision Constraints table**

Validation Rules Version	11	12	13	13.201701	13.201804	201508	201609
Instance Version							
11	Version Match	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)
12	Instance Too New	Version Match	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)
13	Instance Too New	Instance Too New	Version Match	Same Integer	Same Integer	Allowed	Allowed
13.201701	Instance Too New	Instance Too New	Same Integer	Version Match	Same Integer	Allowed	Allowed
13.201804	Instance Too New	Instance Too New	Same Integer	Same Integer	Version Match	Allowed	Allowed
201508	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match	Allowed
201609	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match

## 3.7.6 - Constraint Rules

The detailed constraint rules for the ISM.XML schema can be found in a separate document inside the Schematron/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.

## 3.8 - Data Rendering Constraint Rules

### 3.8.1 - 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; rather these rules should inform the evaluation of a system's capabilities and functionality.

### 3.8.2 - Rendering Constraint Rules

The following table contains the information for the ISM.XML data rendering constraint rules.

**Table 25 - Constraint Rules**

Rule Number	Severity	Description	Human Readable Description
ISM-RENDER-00001	Error	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.	SSI Warnings must be rendered at the bottom of every page of an asset.

## Chapter 4 - Conformance Validation

An instance document conforms with this specification if it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

### 4.1 - Schema Validation

This specification has no normative schema. The schema provided with this specification is an informative aid, and it **SHOULD NOT** be used for conformance validation.

### 4.2 - Business Rule Validation

Validation **MUST** ensure that instance documents comply with the business rules expressed in this specification.

An instance document **MUST** comply with the business rules expressed in this specification and those expressed in this specification's dependencies. The business rules in this specification are expressed in Schematron, but 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. To conform to this specification, a validator **MUST** find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

## Chapter 5 - Generated Guides

### 5.1 - Schema Guide

The detailed description and reference documentation for the ISM.XML schema can be found as a collection of HTML files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the ISM.XML schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen@*,<sup>[51]</sup> produced by SyncRO Soft.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

## 5.2 - Schematron Guide

The detailed description and reference documentation for the ISM.XML Schematron rules can be found in a separate document named *ISM\_Rules.pdf*, which is located inside the Schematron/ISM directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

The following table shows the version dependencies for ISM on other specifications. Direct dependencies are marked with an asterisk.

Table 26 - ISM Dependency over Time

Dependent Specification	V2016-SEP	V2016-SEPr2017-JUL
ARH	V3+	V3+
NTK*	V2015-AUG+	V2015-AUG+
USAgency	V2015-FEB+	V2015-FEB+
ISMCAT*	V2016-SEP+	V2017-JUL+
MN	V2015-AUG+	V2015-AUG+
LIC	V2015-AUG+	V2015-AUG+

The following table summarizes major features by version for ISM and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. For those changes driven by the IC Markings System Register and Manual, the date is often one year after the date of publication. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

Table 27 - 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

Table 28 - ISM Feature Comparison

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
CAPCO Register and Manual 2.1 <sup>[10]</sup>	Declass Removed from Banner	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
January 22, 2009 (1 year after 2008 memo)																		
E.O. 13526 <sup>[20]</sup>	Compilation Reason	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
December 29, 2009																		

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
CAPCO Register and Manual 3.1 <sup>[8]</sup>	LES	P	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
May 7, 2010																		
CAPCO Register and Manual 3.1 <sup>[8]</sup>	LES-NF	P	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
May 7, 2010																		
CAPCO Register and Manual All versions	Require Notices	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Pre 2008																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	KDK	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
December 10, 2010																		
ICD 710 <sup>[33]</sup>	710 Foreign Disclosure or Release	P	P	F	F	F	F	F	F	F	F	F	F	N/A	N/A	N/A	N/A	N/A
September 11, 2009																		
ICD 710 <sup>[33]</sup>	710 Foreign Disclosure or Release	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N	F	F	F	F	F
June 23, 2013																		
E.O. 13526 <sup>[20]</sup>	DeclassReasons/Dates	P	P	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
December 29, 2009																		
IC CIO enhance data quality	Schema validation of values	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F
See IC ESB																		
DoD Instruction 5230.24 <sup>[15]</sup>	DoD Distro Statements	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F
March 18, 1987																		
DoD Directive 5240.01 <sup>[14]</sup>	US Person Notice	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F	F	F
August 27, 2007																		
CAPCO Register and Manual 2.2 <sup>[9]</sup>	Remove SAMI	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F	F	F
September 25, 2010 (1 Year after 2.2)																		
ISOO Marking Booklet 2010 <sup>[44]</sup> / ISOO Notice 2009-13 <sup>[45]</sup>	Remove exempted source	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F	F	F

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
December 2010																		
E.O. 13526 <sup>[20]</sup>	derivativelyClassifiedBy	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F	F	F
December 29, 2009																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	Atomic Energy New banner location	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	Display Only	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)																		
IC CIO enhance data quality	Schematron <sup>[52]</sup> Implementation of rules	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F
See IC ESB																		
E.O. 13526 <sup>[20]</sup>	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F
December 29, 2009																		
DoD Manual 5200.1 <sup>[17]</sup>	DoD ACCM Markings	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F
January 1997																		
CAPCO Register and Manual 4.2 <sup>[6]</sup>	SSI	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F
May 31, 2011																		
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[42]</sup>	TFNI	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F	F
June 28, 2010																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	HCS SubCompartments	N	N	N	N	N	F	F	F	N	N	F	F	F	F	F	P	P
December 10, 2010																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	MCFI Remove	P	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F	F
November 16, 2010 (date disestablished)																		
CAPCO Register and Manual 4.2 <sup>[6]</sup>	MIFH, EUDA and EFOR removed	P	P	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F
May 31, 2011																		

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[42]</sup>	Multivalue declassException	F	N	N	N	N	N	F	F	F	N/A	N/A	N/A	N/A	N/A	F	F	F
June 28, 2010																		
IC CIO enhance data quality	SouthSudan	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F
See IC ESB																		
ICD 710 <sup>[33]</sup>	710 POC	N	N	N	N	N	N	F	F	F	F	F	F	N/A	N/A	F	F	F
September 11, 2009																		
DNI ORCON Memo <sup>[50]</sup>	ORCON POC	N	N	N	N	N	N	F	F	F	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
March 11, 2011																		
ISOO Marking Booklet <sup>[44]</sup>	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F
December 2010																		
IC CIO enhance data quality	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F
See IC ESB																		
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F
IC CIO enhance data quality	@ism:excludeFromRollup=true( ) allowed to not have an ICD-710 foreign release indicator	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F
See IC ESB																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	SINFO Remove	P	P	P	P	P	P	P	F	F	F	F	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)																		
CAPCO Register and Manual 4.1 <sup>[7]</sup>	SC Remove	P	P	P	P	P	P	P	F	F	F	F	F	F	F	F	F	F
December 10, 2011 (1 Year after 4.1)																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	RSV	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F	F
December 30, 2011																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Require using 50X1-HUM instead of 25X1-human	N	N	N	N	P	P	P	F	F	F	F	F	F	F	F	F	F

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
December 30, 2011																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Allow use of KDK compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
December 30, 2011																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Allow use of SI compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
December 30, 2011																		
CAPCO Register and Manual 5.1 Annex A <sup>[13]</sup>	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
December 30, 2011																		
IC CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
DoD Manual 5200.1-R <sup>[17]</sup>	COMSEC Notice	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
February 2012																		
DoD Manual 5200.1-R <sup>[17]</sup>	Support for NNPI	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
February 2012																		
Decouple ISM from the Schema	Informative Schema	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F
January 2013																		
Decouple ISM from the Schema	Normative Schematron rules and CVEs	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F
January 2013																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Add ENDSEAL system with compartments ECRU and NONBOOK	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F
December 2012																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Limit KDK system compartments to BLUEFISH, IDITAROD and KANDIK	N	N	N	N	N	N	N	N	P	F	F	F	F	F	F	F	F
December 2013																		
ISOO Notice 2013-01 <sup>[47]</sup> .	Support NATO exemptions to declass date	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F
November 2012																		

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
CAPCO Register and Manual 5.1 <sup>[5]</sup>	Support multiple non JOINT countries prior to the Classification	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
December 2013																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	Support ORCON-USGOV	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	Support RD precedence over FRD	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	Treat caveated UNCLASSIFIED as RELIDO unless explicitly specified	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	Allow commingling of SBU and SUB-NF with classified information in portions	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	50X1 and 50X6	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0, Appendix B, Section 4 <sup>[12]</sup>	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	N	N	N	N	N	N	N	N	N	N	P	P	P	P	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	Allow JOINT classification markings with SCI, SAP, AEA, IC and non-IC Dissemination Control Markings (excluding NOFORN)	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0, Appendix A, Enclosure 1 <sup>[11]</sup>	Allow Non-US classification markings with US SCI, SAP, AEA, IC and non-IC Dissemination control markings (excluding NOFORN)	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
Feb 2014																		
CAPCO Register and Manual 6.0 <sup>[4]</sup>	ORCON and ORCON-USGOV may not be used with RELIDO	N	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F
Feb 2014																		

ISM Feature Comparison																		
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	2014-DEC	2015-AUG	2016-SEP	2016-SEPr2017-JUL
Required Date																		
IC Marking System Register and Manual 31 December 2013 <sup>[27]</sup>	Required compliesWith to support ICD 710 Foreign Disclosure and Release changes	N	N	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F
Feb 2014																		
IC Marking System Register and Manual 31 December 2013 <sup>[27]</sup>	Support for NATO NACs	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	F	F
Feb 2014																		
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[42]</sup>	50X2, 50X3, 50X4, 50X5, 50X7, 50X8, and 50X9	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F	F
December 2010																		
	Use Tetragraph taxonomy to validate tetragraph classification does not violate document classification	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
	Support for approximate markings	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
	Support indicator of absence of aggregation	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
IC Marking System Register and Manual 24 December 2015 <sup>[25]</sup>	Remove support for HCS-O subcomparments	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
Dec 2016																		
IC Marking System Register and Manual 30 June 2016 <sup>[23]</sup>	Alignment with June 2016 IC Markings System Register and Manual	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
June 2017																		
	Use of fully decomposed tetragraph taxonomy	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F

## Appendix B Change History

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

**Table 29 - DES Version Identifier History**

Version	Date	Purpose
1	August 2008	Initial Release
2	24 December 2009	Routine revision to technical specification. For details of changes, see <a href="#">Section B.16 - V2 Change Summary</a>
3	4 June 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.15 - V3 Change Summary</a>
4	7 September 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.14 - V4 Change Summary</a>
5	6 December 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.13 - V5 Change Summary</a>
6	11 April 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.12 - V6 Change Summary</a>
7	9 August 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.11 - V7 Change Summary</a>
8	27 February 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.10 - V8 Change Summary</a>
9	17 July 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.9 - V9 Change Summary</a>
10	21 January 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.8 - V10 Change Summary</a>
11	5 April 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.7 - V11 Change Summary</a>
12	16 August 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.6 - V12 Change Summary</a>
13	14 March 2014	Routine revision to technical specification. For details of changes, see <a href="#">Section B.5 - V13 Change Summary</a>
2014-DEC	4 December 2014	Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - V2014-DEC Change Summary</a>
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V2015-AUG Change Summary</a>
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V2016-SEP Change Summary</a>
2016-SEPr2017-JUL	21 July 2017	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2016-SEPr2017-JUL Change Summary</a>

## B.1 - V2016-SEPr2017-JUL Change Summary

Significant drivers for Version 2016-SEPr2017-JUL include:

- Community Change Requests
- Alignment with December 2016 IC Marking System Register and Manual<sup>[24]</sup>
- Alignment with DoD Manual 5200.1<sup>[17]</sup>

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

**Table 30 - Data Encoding Specification 2016-SEPr2017-JUL Change Summary**

#	Change	Artifacts changed	Compatibility Notes
1	Moving ECRU and NONBOOK as sub-compartments 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.

#	Change	Artifacts changed	Compatibility Notes
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.
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.

#	Change	Artifacts changed	Compatibility Notes
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.
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.

#	Change	Artifacts changed	Compatibility Notes
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.
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 IC Markings System Register and Manual. (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.

#	Change	Artifacts changed	Compatibility Notes
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.2 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests
- Alignment with December 2015 IC Marking System Register and Manual<sup>[25]</sup>

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

**Table 31 - Data Encoding Specification 2016-SEP Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
Added new attribute <b>@hasApproximateMarkings</b> (CR-2015-050)	DES Schema CVEnumISMAttributes Schematron ISM-ID-00361 added	Data generation and ingestion systems need to be updated to enforce the new rule.

Change	Artifacts changed	Compatibility Notes
Added new attribute <b>@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.
Added RSEN to CVEnumISMNotice so that it can be used with the <b>@noticeType</b> attribute. (CR-2016-059)	CVEnumISMNotice	None
Removed Schematron rules related to HCS-O subcompartments (CR-2016-059)	DES Schematron ISM-ID-00334 removed	None
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
Updated schematron rules to exclude checks if the only ISM content is the use of @ism:ISMCACTCESVersion 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.
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.
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.
Added attribute Usage Info in ISM CVE descriptive information. (CR-2016-019)	CVE	No impact to systems.
Update rendering for nonUScontrols to align with IC Markings Register and Manual. (CR-2014-092)	IC-ISM-PortionMark.xsl IC-ISM-SecurityBanner.xsl	Rendering systems need to be updated.

Change	Artifacts changed	Compatibility Notes
Removed KDK and moved KDK subcompartments under TK to align with IC Markings Register and Manual. (CR-2016-024)	CVE CVEEnumISMSCIControls 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.
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.3 - 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>[26]</sup>

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

**Table 32 - Data Encoding Specification 2015-AUG Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.
Updated to use the new URIs for the NTK ProfileDes and AccessPolicy.	Schematron ISM-ID-00326 modified	Data generation and ingestion systems need to be updated to use the new URI.
Updated code descriptions to improve readability.	Schematron	No impact to data generation and ingestion systems.
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.
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.
Make @ism:ISMCATCESVersion optional in ISMRootNodeAttributeOptionGroup	Schema	No impact to data generation and ingestion systems. Impacts systems designing new schema using ISM.
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.
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.
Updated util:recursivelyCheckDisplayTo for correctness (CR-2015-011)	Schematron ISM_XML.sch	Data generation and ingestion systems need to be updated.

## B.4 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- December 2014 IC Marking System Register and Manual<sup>[26]</sup>

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

**Table 33 - Data Encoding Specification 2014-DEC Change Summary**

Change	Artifacts changed	Compatibility Notes
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.xml IC-ISM-SecurityBanner.xml IC-ISM-PortionMark.xml	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.
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.
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.
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.
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 CVE file.
Updated Banner and Portion StyleSheets for NATO NAC rendering issues.	IC-ISM-PortionMark.xml updated IC-ISM-SecurityBanner.xml updated	Data rendering systems should update their stylesheets.
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.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.
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.
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.
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
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.
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.5 - V13 Change Summary

Significant drivers for Version 13 include:

- IC Marking System Register and Manual 31 December 2013<sup>[27]</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 34 - Data Encoding Specification V13 Change Summary**

Change	Artifacts changed	Compatibility Notes
<p>Attribute <code>ism:compliesWith</code> now must be specified on all resource (<code>ism:resourceElement="true"</code>) nodes within a document. Allowed values for <code>ism:compliesWith</code> are <code>USGov</code>, <code>USDOD</code>, <code>USIC</code>, and <code>OtherAuthority</code>. <code>USDOD</code> and <code>USIC</code> require <code>USGov</code>. Note that <code>ism:compliesWith</code> MUST contain <code>USGov</code> when the <code>ism:ownerProducer</code> attribute for the containing resource node contains <code>USA</code>.</p> <p>Specific exemptions within a rule set - for example exemption from ICD 710 FD&amp;R requirements, must be declared in the <code>ism:exemptFrom</code> attribute (also on the resource node).</p>	<p><code>CVEnum-ISMExemptFrom</code> added</p> <p>Schematron</p> <p>All of the ISM rules were updated in accordance with the new ISM 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 <code>compliesWith</code> 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>
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.
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.6 - V12 Change Summary

Significant drivers for Version 12 include:

- Added a dependency on the *XML Encoding CVE Specification for ISM Country Codes and Tetragraphs* [\[40\]](#)
- CAPCO Register and Manual 6.0 Administrative Update [\[3\]](#)
- 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 35 - Data Encoding Specification V12 Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
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.
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.
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.
Added rule to require presence of NTK with an OC-NTKOC-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
Decoupled the Country Code and Tetragraph CVEs from ISM 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.	<p>Schema</p> <p>CVEnumISMFGIOpen</p> <p>CVEnum-ISMFGIProtected</p> <p>CVEnum-ISMOwnerProducer</p> <p>CVEnumISMRelTo</p> <p>Schematron</p> <p>ISM_ID_00100.sch updated</p> <p>ISM_ID_00166.sch updated</p> <p>ISM_ID_00170.sch updated</p> <p>ISM_ID_00179.sch updated</p> <p>ISM_ID_00180.sch updated</p> <p>ISM_ID_00188.sch updated</p> <p>ISM_ID_00189.sch updated</p> <p>ISM_ID_00190.sch updated</p> <p>ISM_ID_00191.sch updated</p> <p>ISM_ID_00192.sch updated</p> <p>ISM_ID_00193.sch updated</p> <p>ISM_ID_00194.sch updated</p>	Data generation and ingestion systems need to be updated to handle the new ISMCAT dependency, the removal of the ISM 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	
Added a schematron rule to enforce an ISM 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.
Added reference to Access Control Encoding Specifications (ACES).	Documentation	Access control systems using ISM need to review ACES to ensure compliance.
<p>HCS compartments and sub-compartments are no longer designated For Official Use Only. Rules relating to these values have been moved into the Unclassified rule number range.</p> <div>  <p><b>Note</b></p> <p>This change is ahead of the CAPCO Register and Manual.</p> </div>	Schematron  ISM_ID_00330.sch added  ISM_ID_00331.sch added  ISM_ID_00332.sch added  ISM_ID_00333.sch added  ISM_ID_00334.sch added  ISM_ID_00335.sch added  ISM_ID_00336.sch added	Data generation and ingestion systems may need to be updated to properly handle this change.

## B.7 - 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>[4]</sup>
- CAPCO Register and Manual 5.1<sup>[5]</sup>

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

**Table 36 - Data Encoding Specification V11 Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
Added ORCON-USGOV as a value for dissemControls 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.
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.
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.
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
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.
Removed obsolete rule ISM-ID-00126.	Schematron ISM-ID-00126 Removed	Data generation and ingestion systems should be aware of the rule removal.
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.
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.
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.
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.
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.8 - V10 Change Summary

Significant drivers for Version 10 include:

- CAPCO Register and Manual 5.1 and approved Change Requests<sup>[5]</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 from other specifications

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

**Table 37 - Data Encoding Specification V10 Change Summary**

Change	Artifacts changed	Compatibility Notes
Added a rule to verify that the DESVersion of ISM is 10.	Schematron ISM_XML.sch	Data generation and ingestion systems need to ensure they are including the abstract rule.
Replaced ISO 3166 with GENC Standard for country trigraph codes based on CAPCO CR CR-2012-010.	CVE 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
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.
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.
Added a rule to ensure that an element with a declassException of AEA contains atomicEnergyMarkings.	Schematron ISM-ID-00299 Added	Data generation and ingestion systems need to be updated to properly use the new rule.
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.
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
Created schematron rules to validate ISM 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 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
Clarified the description in the Schematron rules that deal with deprecated values in the CVE files [artf13026].	Schematron	Should not impact data.
	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	

Change	Artifacts changed	Compatibility Notes
	ISM-ID-00209 Changed ISM-ID-00210 Changed ISM-ID-00211 Changed	
Created schematron rules to check that the value(s) of an ISM 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 CVE values instead of using the schema.
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.
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
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.
Corrected typo of duplicate "[" in error message.	ISM-ID-00242 Changed	No change in logic.
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.
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.
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.
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.
Add NATO declass exemption to potential exemptions, based on ISOO Notice 2013-01 <sup>[47]</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
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.
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.
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.
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.
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.9 - V9 Change Summary

Significant drivers for Version 9 include:

- CAPCO Register and Manual 5.1<sup>[5]</sup>

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

**Table 38 - Data Encoding Specification V9 Change Summary**

Change	Artifacts changed	Compatibility Notes
Added support for alphanumeric <b>@DESVersion</b> identifiers [artf12167].	Schema	Should not impact data but ingestion systems may need to account for it.
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.
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
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
Remove support for HCS sub-compartments.	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.
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 CVEnum-ISMCompliesWith.xml Changed	Data generation and ingestion systems need to be updated to no longer use these values.
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.
Added OSTY Open Skies Treaty.	CVEnum-ISMOwnerProducer.xml Changed CVEnum-ISMFGIProtected.xml Changed CVEnumISMRelTo.xml Changed CVEnum-ISMFGIOpen.xml Changed	Data generation and ingestion systems need to be updated to properly use the new value.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.10 - V8 Change Summary

Significant drivers for Version 8 include:

- CAPCO Register and Manual 5.1<sup>[5]</sup>
- ISOO Guidance (ISOO Notice 2012-02)<sup>[46]</sup>
- ISO 3166-1<sup>[41]</sup>

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

**Table 39 - Data Encoding Specification V8 Change Summary**

Change	Artifacts changed	Compatibility Notes
Updated country code descriptions in the ISO 3166-1 <sup>[41]</sup> CVEs to reflect ISO newsletter changes.	schema Changed CVCEnumISMFGIOpen Changed CVCEnum-ISMFGIProtected Changed CVCEnum-ISMOwnerProducer Changed CVCEnumISMRelTo Changed	Data generation and ingestion systems need to be updated to properly use the new values.
Allow use of RSV.	schema Changed CVCEnumISMSCIControls Changed	Data generation and ingestion systems need to be updated to properly use the new values.

Change	Artifacts changed	Compatibility Notes
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.
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.
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.
Added unique namespaces to generated CVE schema fragments. Moved schema fragment imports to the base schema.	Schema CVEs	Should not affect data.
Added attributeFormDefault="qualified" to make the attributes explicitly require the being namespace prefixed.	Schema	Should not affect data.
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.
Allow portions with @ism:excludeFromRollup=true() to not have an ICD 710 <sup>[33]</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.

Change	Artifacts changed	Compatibility Notes
Enforce illegal value duplications in ISM attributes.	ISM-ID-00236 Added	Data generation and ingestion systems need to be updated to handle these data changes.
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.
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.
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.
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.
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.
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.
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.
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.
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.

Change	Artifacts changed	Compatibility Notes
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.
All attributes in the ISM 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.
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.
Removes \$ISM_CAPCO_RESOURCE from rules enforcing attributes and elements in the ISM namespace.	ISM-ID-00125 Changed ISM-ID-00223 Changed	Data generation and ingestion systems need to be updated to handle these rule changes.
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.
Added new hierarchy structure to SAR Identifiers.	CVE Changed	Data generation and ingestion systems need to be updated to handle these changes.
Added requirement for 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.11 - V7 Change Summary

Significant drivers for Version 7 include:

- CAPCO Register and Manual 4.2<sup>[6]</sup>
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)<sup>[42]</sup>
- ISO 3166-1<sup>[41]</sup>
- DNI ORCON Memo<sup>[50]</sup>
- ICD 710<sup>[33]</sup>

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

**Table 40 - Data Encoding Specification V7 Change Summary**

Change	Artifacts changed	Compatibility Notes
Resolved attribute composability issue by separating ISM notice attributes from the security attributes.	Schema	Should not affect data.
Added elements <b>Notice</b> , <b>NoticeText</b> and <b>NoticeList</b> to represent valid ISM notices, as well as the attribute <b>@unregisteredNoticeType</b> to represent other notices.	Schema CVCEnumISMElements Added CVCEnumISMAAttributes Changed ISM-ID-00223 Added ISM-ID-00226 Added	Data generation and ingestion systems need to be updated to use the new values.
Added <b>ISMNoticeAttributeGroup</b> to <b>ResourceNodeAttributeGroup</b> and <b>ResourceNodeOptionalAttributeGroup</b> .	Schema	Schema developers need to update to use the corrected attribute group. Instance documents are not impacted.
Added new <b>@pocType</b> attribute and <b>POCAttributeGroup</b> to support indicators for a security-related point-of-contact, including ORCON, ICD 710 <sup>[33]</sup> and DoD Distribution statements.	Schema CVCEnumISMAAttributes Changed CVCEnumISMPocType-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.
Added notice attributes to ISM resource node.	Schema	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
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.
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 data, addition is necessary to prevent unintended changes to IRM. Data generation and ingestion systems will need to be updated to reflect the change.

Change	Artifacts changed	Compatibility Notes
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.
Renamed <b>@notice</b> to <b>@noticeType</b> and replaced <b>@noticePOC</b> with <b>@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.
Allowed for multiple values to be specified for <b>@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.
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.
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.
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
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.
Removed deprecation dates for <b>@declassException</b> tokens [25X1-human], and [AEA].	CVEnumISM25X1	Should not affect data.
Added country code for South Sudan to the ISO 3166-1 <sup>[41]</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.12 - V6 Change Summary

Significant drivers for Version 6 include:

- CAPCO Register and Manual 4.1 (HCS Sub Cats missed in V5)<sup>[7]</sup>
- Executive Order 13526<sup>[20]</sup>
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)<sup>[42]</sup>

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

**Table 41 - Data Encoding Specification V6 Change Summary**

Change	Artifacts changed	Compatibility Notes
Removed ISM-ID-00212.	ISM-ID-00212 Remove	ISM-ID-00212 was a duplicate of ISM-ID-103.

Change	Artifacts changed	Compatibility Notes
Cleaned up English text of ISM-ID-00124.	ISM-ID-00124 Changed	Corrected an error in text. No change to Schematron.
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
Modified check for resourceElement to be more accurate only applying to the first occurrence of resourceElement=true().	ISM-ID-00013 Changed	Now is compliant with intent of ISM check for resourceElement. Only considers the first resourceElement=true() a resource element.
	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	

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	
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.
Improved checking for null attributes.	ISM-ID-00002 Changed	Does not affect anything except that the check for null-valued attributes is more accurate.
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.
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.
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
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.
Tetragraph [MCFI] removed from CVEs.	CVEs	Data generation and ingestion systems need to be updated to no longer use the obsolete value.
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.
Added support for TFNI.	CVEs	Data generation and ingestion systems need to be updated to properly use the new value.
Added support for SSI.	CVEs	Data generation and ingestion systems need to be updated to properly use the new value.

## B.12.1 - V6 Change Errata

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

**Table 42 - Data Encoding Specification V6 Change Errata**

Change	Artifacts changed	Compatibility Notes
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.13 - V5 Change Summary

Significant drivers for Version 5 include:

- CAPCO Register and Manual 4.1<sup>[7]</sup>

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

**Table 43 - Data Encoding Specification V5 Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
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.
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.
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
Support Atomic Energy Act (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	
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.
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.
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
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.
Remove <b>@typeOfExemptedSource</b> and <b>@dateOfExemptedSource</b> 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.
Remove Appendix H Reading the Schematics.	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.
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
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.13.1 - V5 Change Errata

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

**Table 44 - Data Encoding Specification V5 Change Errata**

Change	Artifacts changed	Compatibility Notes
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.14 - V4 Change Summary

Significant drivers for Version 4 include:

- DoD Directive 5230.24<sup>[15]</sup>
- ICD 710<sup>[33]</sup> (enforce immediately no grace)

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

**Table 45 - Data Encoding Specification V4 Change Summary**

Change	Artifacts changed	Compatibility Notes
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.
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.
Use schema to enforce DES version number.	Schema ISM-ID-00102	Forces DES to match version shipped.
Enforce ICD 710 <sup>[33]</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>[33]</sup> need make no changes. Existing data may not be valid anymore.
Remove Duplicate or redundant rules.	ISM-ID-00144 ISM-ID-00023	Data validation systems may remove duplicate code.

## B.15 - V3 Change Summary

Significant drivers for Version 3 include:

- Executive Order 13526<sup>[20]</sup> (enforce requirements for Authority block)
- CAPCO Register and Manual 3.1<sup>[8]</sup>
- ICD 710<sup>[33]</sup>

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

**Table 46 - Data Encoding Specification V3 Change Summary**

Change	Artifacts changed	Compatibility Notes
Allow use of KDK.	Controlled Value Enumerations Constraint Rules ISM-ID-00122 ISM-ID-00123	Data generation systems that correctly implement CAPCO guidance <sup>[8]</sup> and follow E.O. 13526 <sup>[20]</sup> should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules.
Require appropriate foreign disclosure or release marking on classified national intelligence per ICD 710. <sup>[33]</sup>	Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data generation systems that correctly implement CAPCO guidance <sup>[8]</sup> and follow E.O. 13526 <sup>[20]</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
Update references to E.O. 12958, as amended <sup>[19]</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.
Force ordering of SAR.	Constraint Rules ISM-ID-00121	Data generation systems that correctly implement CAPCO guidance <sup>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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
Remove ISM-ID-00022.	ISM-ID-00022	No impact rule was effectively a duplicate of ISM-ID-00011 due to CVE change in V1.
Reduce risk of using ISM 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.
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.
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
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
Add check that NF is not allowed on U portions.	ISM-ID-00140	Data generation systems that correctly implement CAPCO guidance <sup>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
Enforce E.O. 13526 <sup>[20]</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>[8]</sup> and follow E.O. 13526 <sup>[20]</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
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>[8]</sup> and follow E.O. 13526 <sup>[20]</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.
Add rule for FOUO compilation reason.	ISM-ID-00154	Data generation systems that correctly implement CAPCO guidance <sup>[8]</sup> and follow E.O. 13526 <sup>[20]</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.16 - V2 Change Summary

Significant drivers for Version 2 include:

- Executive Order 12958, as amended <sup>[19]</sup>(compilationReason)
- CAPCO Register and Manual 2.1<sup>[10]</sup>
- ISOO 32 CFR Parts 2001 and 2004 (Guidance on Type of Exempted Source [as of September 22, 2003])<sup>[43]</sup>

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

**Table 47 - Data Encoding Specification V2 Change Summary**

Change	Artifacts changed	Compatibility Notes
Updated ISM 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.
Removed version number from file names.	Schema	Systems need to be updated to use the new file names.
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.
Added <b>@compilationReason</b> 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.
Expanded constraint rules to identify previously unrecognized data errors in accordance with the IC Classification and Control Markings system.	Constraint Rules	Data generation systems that correctly implement CAPCO guidance <sup>[10]</sup> and follow E.O. 12958, as amended <sup>[19]</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
Changed ISM vocab warnings to errors, based on identification of specific CVE.	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance <sup>[10]</sup> and follow E.O. 12958, as amended <sup>[19]</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.
Updated constraint rules and schema documentation to specify data values for: <b>@ownerProducer</b> , <b>@SCIcontrols</b> , <b>@SARIdentifier</b> , <b>@disseminationControls</b> , <b>@FGIsourceOpen</b> , <b>@FGIsourceProtected</b> , <b>@releasableTo</b> , <b>@nonICmarkings</b> , <b>@declassException</b> , <b>@typeOfExemptedSource</b> .	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance <sup>[10]</sup> and follow E.O. 12958, as amended <sup>[19]</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.
Removed <b>@declassManualReview</b> .	Constraint Rules ADD Mapping Table	Data generation systems should be updated to prohibit <b>@declassManualReview</b> on new data. Ingestion systems need to be updated to reject <b>@declassManualReview</b> 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.
Changed definition of <b>@declassException</b> and <b>@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.

Change	Artifacts changed	Compatibility Notes
Added attributes to enable defining of the roles that ISM attributes play in a document.  <b>@resourceElement,</b> <b>@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.
Added attribute to enable ISM date based rules.  <b>@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.

ABNF	Augmented Backus-Naur Form
ACES	Access Control Encoding Specification
ADD	Abstract Data Definition
AEA	Atomic Energy Act
ARH	Access Rights and Handling
CAPCO	Controlled Access Program Coordination Office
CES	Controlled Vocabulary Enumeration Encoding Specification
CFR	Code of Federal Regulations
CNWDI	Critical Nuclear Weapons Design Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
E.O.	Executive Order
FD&R	Foreign Disclosure & Release
FOUO	For Official Use Only
GENC	Geopolitical Entities, Names, and Codes
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance

ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISM-ACES	Access Control Encoding Specification for Information Security Marking
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LIC	License
MN	Mission Need Profile
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NIEM	National Information Exchange Model
NPE	Non-Person Entity
NTK	Need-To-Know Metadata
OC	Originator Controlled
OCIO	Office of the Intelligence Community Chief Information Officer
OC-NTK	Originator Controlled Need-to-Know
ODNI	Office of the Director of National Intelligence
OLA	Office of Legislative Affairs
ORCON	See OC.
PDP	Policy Decision Point

POC	Point of Contact
RFC	Request for Comments
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SMP	Security Markings Program
TS	Top Secret
U	Unclassified
UIAS	Unified Identity Attribute Set
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URL	Uniform Resource Locator
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

### Bibliography

[1] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*. Available online at: <http://tools.ietf.org/html/std68>  
Also known as: <http://www.ietf.org/rfc/rfc5234.txt>

[2] ADD

Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*. Available online Intelink-TS at: <http://go.ic.gov/soSC6M8>  
Available online Intelink-U at: <https://w3id.org/ic/standards/ADD>  
Available online at: <https://w3id.org/ic/standards/public>

[3] 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/capco>

[4] 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/capco> or [https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO\\_Register%20and%20Manual%20v6.0\\_28%20Feb13\\_FOUO.pdf](https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register%20and%20Manual%20v6.0_28%20Feb13_FOUO.pdf)

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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/capco>

[12] 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/capco>

[13] 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.

[14] DoD Directive 5240.01

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

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

[15] 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>

[16] DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.

Available online at: <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf>

[17] DoD Manual 5200.1

Under Secretary of Defense for Intelligence. *DoD Information Security Program (Vol 1-4):* . 5200.1. February 24, 2012.

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

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

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

Vol 4 Available online at: [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001\\_vol4.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001_vol4.pdf)

[18] E.O. 12829

The White House. *Executive Order 12829 – National Industrial Security Program, as Amended*. Federal Register, Vol. 58, No. 240. 16 December 1993.

Available online at: <http://www.archives.gov/isoo/policy-documents/eo-12829.html>

[19] 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>

[20] 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>

[21] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

Available online Intelink-TS at: <http://go.ic.gov/4X6TOc1>

[22] 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: <http://go.ic.gov/5DjqgWz>

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

[23] 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: <http://go.ic.gov/PXJoxCz>

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

[24] 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-U at: <https://w3id.org/ic/standards/policy/icmarkings> [https://w3id.org/ic/standards/policy/icmarkings ]
- [25] 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> [https://w3id.org/ic/standards/policy/icmarkings ]
- [26] 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>
- [27] 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>
- [28] IC-ID.XML  
Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.  
Available online Intelink-TS at: <http://go.ic.gov/mQ4IUDk>  
Available online Intelink-U at: <https://w3id.org/ic/standards/IC-ID>  
Available online at: <https://w3id.org/ic/standards/public>
- [29] 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)
- [30] 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>
- [31] 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: <http://go.ic.gov/5Ot5sbK>  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_500.pdf](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)
- [32] 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: <http://go.ic.gov/GG61roi>

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_501.pdf](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

[33] ICD 710

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

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_710.pdf](http://www.dni.gov/files/documents/ICD/ICD_710.pdf)

[34] 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: <http://go.ic.gov/0d147Ee>

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

[35] 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)

[36] 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>

[37] 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: <http://go.ic.gov/sLKNq3N>

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

[38] 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: <http://go.ic.gov/cWYv9nw>

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

[39] IETF-RFC 2119

Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.

Available online at: <http://tools.ietf.org/html/rfc2119>

[40] ISMCAT.CES

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

Available online Intelink-TS at: <http://go.ic.gov/xhPflI3>

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

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

[41] 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)

[42] 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>

[43] 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>

[44] 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>

[45] 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: <http://www.archives.gov/isoo/notices/>

[46] 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>

[47] 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>

[48] Jelliffe

Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.

Available online at: <http://www.schematron.com>

## [49] NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/YLXsYUX>

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

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

## [50] 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<sup>[34]</sup>, 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>

## [51] Oxygen

SyncRO Soft. *<oXygen/> XML Editor*.

Available online at: <http://www.oxygenxml.com/>

## [52] 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/>

## [53] TAG-9-Jan-2006

W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace*. 9 January 2006.

Available online at: <http://www.w3.org/2001/tag/doc/namespaceState.html>

## [54] WEBARCH-15-Dec-2004

W3C. *Architecture of the World Wide Web, Volume One*. 15 December 2004.

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

## [55] XML 1.0

World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.

Available online at: <http://www.w3.org/TR/2000/REC-xml-20001006>

[56] 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/>

[57] 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@iarpa.gov](mailto:ic-standards-support@iarpa.gov).

## Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO 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 OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO 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 Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.<sup>[37]</sup>