

XML DATA ENCODING SPECIFICATION FOR INFORMATION SECURITY MARKING METADATA VERSION 5

ICTechSpec 500.D.2-V5

An Intelligence Community Technical Specification
Prepared by the
Intelligence Community Chief Information Officer

6 December 2010



Table of Contents

| | |
|--|-----------|
| Table of Contents | i |
| List of Tables | ii |
| Chapter 1 – Introduction | 1 |
| 1.1 Purpose | 1 |
| 1.2 Needs and Requirements | 1 |
| 1.3 Audience and Applicability | 2 |
| 1.4 Utility | 2 |
| 1.5 Version Information | 2 |
| 1.6 Components of this DES | 3 |
| 1.7 Normative and Informative Components | 3 |
| 1.8 Technical Encoding Dependencies | 4 |
| 1.9 Typographic conventions | 4 |
| Chapter 2 – Development Guidance | 5 |
| 2.1 Mapping of Abstract Data Elements to Physical XML Elements | 5 |
| 2.2 Additional Guidance | 11 |
| 2.2.1 <i>Physical XML Attribute Groups</i> | 11 |
| 2.2.2 <i>Notices</i> | 12 |
| Chapter 3 – Guides | 13 |
| 3.1 Schema Guide | 13 |
| 3.2 Schematron Guide | 14 |
| Chapter 4 – Data Validation Constraint Rules | 15 |
| 4.1 Basics | 15 |
| 4.1.1 <i>Schematron</i> | 15 |
| 4.1.2 <i>"Living" Constraint Rules</i> | 16 |
| 4.1.3 <i>Classified or Controlled Constraint Rules</i> | 16 |
| 4.1.4 <i>Rule Identifiers</i> | 17 |
| 4.1.5 <i>Errors and Warnings</i> | 17 |
| 4.1.6 <i>DES Constraints</i> | 17 |
| 4.2 Validation Against CVEs | 17 |
| 4.3 Obsolete rule numbers | 18 |
| Appendix A IC CIO Approval Memo | 20 |
| Appendix B Acronyms | 21 |
| Appendix C Glossary | 23 |
| Appendix D Bibliography | 24 |
| Appendix E Points of Contact | 27 |
| Appendix F Change History | 28 |
| F.1 V5 Change Summary | 29 |
| F.2 V4 Change Summary | 34 |
| F.3 V3 Change Summary | 35 |
| F.4 V2 Change Summary | 39 |

| | | |
|-------------------|---|-----------|
| Appendix G | Configuration Management | 43 |
| Appendix H | Controlled Vocabulary Enumerations | 44 |

List of Tables

| | |
|--|----|
| Table 1. Mapping of Abstract Data Element to Physical XML Elements | 6 |
| Table 2. Mapping of Abstract Data Element Refinements to Physical XML Attributes | 8 |
| Table 3. DES Version Identifier History | 28 |
| Table 4. Data Encoding Specification V5 Change Summary | 29 |
| Table 5. Data Encoding Specification V4 Change Summary | 34 |
| Table 6. Data Encoding Specification V3 Change Summary | 35 |
| Table 7. Data Encoding Specification V2 Change Summary | 39 |
| Table 8. CVE Definitions | 44 |

Chapter 1 – Introduction

1.1 Purpose

This *XML Data Encoding Specification for Information Security Marking Metadata* (ISM.XML) defines detailed specifications for using Extensible Markup Language (XML) to encode information security marking metadata in compliance with the *Intelligence Community Abstract Data Definition (IC.ADD)*. 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 Needs and Requirements

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 when necessary. 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 today being performed by human beings.

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 (EO) 13526, ICD 710, Classification and Control Marking System, and implemented by the CAPCO Register and accompanying Implementation Manual, 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

1.3 Audience and Applicability

DESs are intended primarily to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described. The applicability and conditions for when the DES should be used will be found in the Intelligence Community Enterprise Standards Baseline and referenced in IC policy guidance.

1.4 Utility

A DES specifies how to implement the abstract data elements in the IC.ADD in a particular physical encoding (e.g., data or file format). For example:

- DESs for textual markup formats, such as XML and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.
- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.
- DESs for application-specific formats, such as Microsoft Word, define document properties, styles, fields, cardinalities, processing requirements, and use.

1.5 Version Information

This is **Version 5** of this DES. This version number must be specified in the **DESVersion** attribute within any XML instance document claiming to be valid against this version. A separate **DESVersion** attribute must be specified for each DES against which an instance document is claiming

compliance. These attributes must be in the namespace specified by each DES.

For descriptions of the changes made in this and prior versions see Appendix F.

1.6 Components of this DES

This document is the primary documentary component of the DES. This document contains:

- **Chapter 1 – Introduction.** The introduction describes high-level background information for this document. It defines the purpose and scope of this document.
- **Chapter 2 – Development Guidance.** This chapter covers two primary topics: 1) mappings of the XML element and attributes defined within this DES to appropriate IC.ADD data elements, and 2) descriptions of how particular encoding situations should be handled using the features provided by this DES.
- **Chapter 3 – XML Schema Guide.** Highlights the availability of an interactive presentation of the ISM.XML schema as well as an implementation-specific data element dictionary.
- **Chapter 4 – Data Validation Constraint Rules.** The constraint rules in this chapter define data validation constraints for ISM.XML beyond those in the XML Schema.

This DES consists of a number of additional technical components to include: the interactive *XML Schema Guide* referenced in Chapter 3, XML schema files, Controlled Vocabulary Enumerations (CVE) files, and Extensible Stylesheet Language Transformation (XSLT) files for rendering ISM marks.

1.7 Normative and Informative Components

The XML schemas, CVE values from the XML CVE files, and the Schematron code version of the constraint rules are normative for this DES. The rest of this document, the descriptive content referenced within the *XML Schema Guide*, the XSL transformations, the SchematronGuide, and HTML CVE value files are informative.

1.8 Technical Encoding Dependencies

This DES serves a critical role in bridging the text-based security marking instructions and business rules established by the Office of the Director of National Intelligence (ODNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO) Register and Implementation Manual, Information Security Oversight Office (ISOO) Directive 1, E.O. 13526, and E.O. 12829, as amended; with the technical implementation of marking concepts within local and enterprise systems. It is important to recognize that this DES relies on the CAPCO Register and Implementation Manual as the authoritative sources for the controlled values, marking relationships, and presentation formats. This DES pertains to the technical implementation of a data model for information security markings and in no way attempts to replace or assume authority for text-based security marking instructions, controlled values, or business rules.

The particular value enumerations from the CAPCO Register and other authoritative sources of values used by this DES are described in the CVEs.

This DES is based in part on:

- CAPCO Register (4.1)
- CAPCO Implementation Manual (4.1)
- ISO Schematron implementation by Rick Jelliffe (2010-04-14)

1.9 Typographic conventions

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.

Chapter 2 – Development Guidance

This chapter covers two primary topics:

- 1) Mappings of the XML element and attributes defined within this DES to appropriate IC.ADD data elements
- 2) Descriptions of how particular encoding situations should be handled using the features provided by this DES.

2.1 Mapping of Abstract Data Elements to Physical XML Elements

The mapping of abstract data elements from the IC.ADD to the corresponding physical XML structures defined by this DES is shown in the following tables, which reflect the groupings in the IC.ADD. These mappings are provided for reference only. The complete set of DES artifacts, both normative and informative, should be consulted.

This mapping and additional mappings in other DESs provide a starting point for the development of automated transformations between formats defined by the DESs. However, it should be noted that when these transformations are used between formats with different levels of detail, there might be some data loss.

Table 1. Mapping of Abstract Data Element to Physical XML Elements

| Abstract Data Element | Definition | XPath and XML implementation notes |
|------------------------|--|--|
| Resource Security Mark | <p>The overall security classification and security handling instructions carried by the resource.</p> <p>These values are prominently presented, in the case of publications, at the top and bottom of every page and in other specified locations.</p> | <p>The physical structures representing the conceptual refinements for the Resource Security Mark are intended to be associated with the entire resource being encoded by the presence of @resourceElement="true" on the element that represents the Resource Security metadata.</p> <p>Note: This is the same element that holds the Resource Classification Declassification Mark.</p> <p>The following attributes represent the Resource Security Mark.</p> <p>@classification @compilationReason @disseminationControls @FGISourceOpen @FGISourceProtected @nonICmarkings @ownerProducer @releasableTo @SARIdentifier @SCIcontrols @notice</p> |

| Abstract Data Element | Definition | XPath and XML implementation notes |
|---|--|---|
| Resource Classification Declassification Mark | <p>Classification information and declassification instructions associated with a classified resource based on either an original or derivative classification decision(s).</p> <p>These values are prominently presented with specific labels and formatting on the first page of a document.</p> | <p>The physical structures representing the conceptual refinements for the Resource Classification Declassification Mark are intended to be associated with the entire resource being encoded by the presence of @resourceElement="true" on the element that represents the Resource Security metadata.</p> <p>Note: This is the same element that holds the Resource Security Mark.</p> <p>Note: @compilationReason is used to identify documents intentionally having classification and/or control markings more restrictive than any of the portions in the document.</p> <p>The following attributes represent the Resource Classification Declassification Mark Group.</p> <p>@classificationReason @classifiedBy @compilationReason @declassDate @declassEvent @declassException @derivativelyClassifiedBy @derivedFrom</p> |
| Portion Security Mark | <p>The security classification carried by an individual portion or block of narrative or media, such as a title, paragraph, table, list, media, or caption.</p> <p>These values are prominently presented at the beginning of the respective portion, are enclosed in parentheses, and utilize the same separators as the overall classification markings of the information resource.</p> | <p>The following attributes represent the Portion Security Mark.</p> <p>@classification @disseminationControls @FGISourceOpen @FGISourceProtected @nonICmarkings @ownerProducer @releasableTo @SARIdentifier @SCIcontrols</p> |

Table 2. Mapping of Abstract Data Element Refinements to Physical XML Attributes

| Abstract Data Element Refinement | Definition | XPath and XML implementation notes |
|---|---|---|
| Classification | A single indicator of the highest level of classification applicable to an information resource or portion within the domain of classified national security information. The Classification element is always used in conjunction with the Owner Producer element. Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint). | @classification @compilationReason |
| Classification Reason | One or more reason indicators or explanatory text describing the basis for an original classification decision. | @classificationReason @compilationReason |
| Classified By | The identity, by name or personal identifier, and position title of the original classification authority for a resource. | @classifiedBy @compilationReason |
| Declassification Date | A specific year, month, and day upon which the information shall be automatically declassified if not properly exempted from automatic declassification. | @compilationReason @declassDate |
| Declassification Event | A description of an event upon which the information shall be automatically declassified if not properly exempted from automatic declassification. | @compilationReason @declassEvent |
| Declassification Exemption | A single indicator describing an exemption to the nominal 25-year point for automatic declassification. This element may be used in conjunction with the Declassification Date or Declassification Event. | @compilationReason @declassException |
| Derivatively Classified By | The identity, by name or personal identifier, of the derivative classification authority. | @compilationReason @derivativelyClassifiedBy |
| Derived From | A citation of the authoritative source(s) or reference to "Multiple Sources" of the classification markings used in a classified resource. | @compilationReason @derivedFrom |
| Dissemination Controls | One or more indicators identifying the expansion or limitation on the distribution of information. | @compilationReason @disseminationControls |

| Abstract Data Element Refinement | Definition | XPath and XML implementation notes |
|-------------------------------------|--|--|
| FGI Source Open | One or more indicators identifying information, which qualifies as foreign government information, for which the source(s) of the information is not concealed. | @FGISourceOpen |
| FGI Source Protected | <p>A single indicator that information qualifies as foreign government information for which the source(s) of the information must be concealed.</p> <p>Within protected internal organizational spaces this element may be used to maintain a record of the one or more indicators identifying information, which qualifies as foreign government information for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.</p> | @FGISourceProtected |
| Non-Intelligence Community Markings | One or more indicators of the expansion or limitation on the distribution of an information resource or portion within the domain of information originating from non-intelligence components. | @compilationReason @nonICmarkings |
| Owner Producer | <p>One or more indicators identifying the national government or international organization that have purview over the classification marking of an information resource or portion therein. This element is always used in conjunction with the Classification element. Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint).</p> <p>Within protected internal organizational spaces this element may include one or more indicators identifying information, which qualifies as foreign government information, for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.</p> | @ownerProducer |

| Abstract Data Element Refinement | Definition | XPath and XML implementation notes |
|--|---|------------------------------------|
| Releasable To | One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be released based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element. | @releasableTo |
| DisplayOnlyTo (provisional) | One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be displayed based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element. | @displayOnlyTo |
| Special-Access-Required Program Identifier | One or more indicators identifying the defense or intelligence programs for which special access is required. | @SARIdentifier |
| SCI Controls | One or more indicators identifying sensitive compartmented information control system(s). | @SCIcontrols |
| Compilation Reason (provisional) | The reason that a portion or resource is marked with a higher and/or more restrictive mark than its components would indicate. For example this would document why 3 Unclassified bullet items form a Secret List. Without this reason being noted the above-described document would be considered to be miss-marked and overclassified. | @compilationReason |
| Applicable Ruleset (provisional) | The rulesets that a document asserts compliance with. | @compliesWith |
| Atomic Energy Markings | One or more indicators identifying information controlled under the Atomic Energy Act. | @atomicEnergyMarkings |

2.2 Additional Guidance

2.2.1 Physical XML Attribute Groups

The ISM.XML schema defines several attribute groups. These attribute groups are intended 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 it includes **SecurityAttributesGroup**. The resource node is the element in an implementing schema that represents the security attributes for the entire resource; it would be used to generate the "banner" mark for the resource. The Resource Node also specifies rule sets the resource is claiming compliance with such as ICD-710.
- **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 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.

excludeFromRollup is an attribute not in any group but should be added to any elements in an implementing schema that may require their attributes to be excluded from rollup logic impacting 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 TS even though the data extracted was U and the document the source citation is in is U.

2.2.2 Notices

The **NoticeAttributesGroup** and the **NoticeAttributesOptionGroup** can be used on an element to signify that it contains notice information concerning a "well defined" notice such as RD, IMCON, FRD, FISA; the value of the **ism:notice** attribute is used to indicate which notice is contained in the element.

An implementing schema could use the same element to capture both the notices codified using this attribute as well as other notices, warnings, notes, etc. It is a best practice to limit the content of a single element, used for notice information, to a single type of notice. For example if a document is to contain both a FISA notice and notice about languages used, two separate elements should be used, one with an **ism:notice** attribute with a value of "FISA" and one without any **ism:notice** attribute.

DoD Distro statements are slightly more complex; a single document may have multiple DoD Distro 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.

Applying the **ism:notice** attribute with the value of FISA or any other notice does NOT remove the obligation to put the appropriate required text in the notice element. For example, only placing the **ism:notice** attribute with the value of RD would not constitute a valid RD notice.

2.2.2.1 US-Person

The value US-Person in **ism:notice** is not required according to the CAPCO Implementation Manual or Register; however, several producing agencies have varying implementations to support notices associated with US-Person information. The inclusion of this value in the CVE provides a standard implementation for all producing agencies.

Chapter 3 – Guides

3.1 Schema Guide

The detailed description and reference documentation for the ISM.XML schema can be found in a separate document entitled *ISM.XML Schema Guide*. This guide 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®*, 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
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

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

3.2 Schematron Guide

The detailed description and reference documentation for the ISM.XML schema can be found in a separate document inside the SchematronGuide directory, Rules.pdf. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Chapter 4 – Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for ISM-XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded, especially for criteria that exceed the constraints implemented in the XML Schema. These rules are in separate files, one per rule or constraint written in the Schematron in plain English phrases; however, knowledge of the ISM-XML schemas and Schematron is required to understand the rules. Complex constraint rules may be followed by text labeled **Human Readable**. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement as defined by the formal Schematron language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved.

4.1 Basics

This DES pertains to the technical implementation of a data model for information security markings and in no way attempts to replace or assume authority for text-based security marking instructions, controlled values, or business rules.

The ISM.XML schema defines the data elements, attributes, cardinalities, and parent-child relationships for which XML instances must comply. Validation of these syntactic 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 Intelligence Community (IC) policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

4.1.1 Schematron

Schematron was selected as the language in which to encode these additional rules. The provided Schematron is used to define the constraint rules; it is NOT a required implementation. Implementors can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either Oxygen or the XSLT2 implementation of ISO

schematron provided by Rick Jelliffe at <http://Schematron.com>. ISM rules are dependent on XPath 2.0 and XSLT 2.0 features. According to Mr. Jelliffe who is the editor of Schematron for ISO:

“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.”

Included in the package are the ISO schematron implementation XSLT files provided as a convenience along with a compiled version of the rules.

4.1.2 “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 implemented in the Register and Implementation Manual, ISOO Directive 1, Executive Order (E.O.) 13526, and E.O. 12829, as amended. These rules will be expanded and modified as the model matures, the CAPCO Register is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

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

4.1.3 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 DES artifacts wherever they are located.

4.1.4 Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are "for official use only" (FOUO). IDs from 20001 to 30000 are reserved for "Secret" rules and 30001 and above for more classified rules. ISM.XML data validation constrain rule IDs are prefixed with "ISM-ID-".

As the validation constraint rules are managed over time, IDs from deleted rules will not be reused.

4.1.5 Errors and Warnings

The severity of a constraint rule violation is categorized as either an "Error" or a "Warning." An "Error" is naturally more severe and is indicative of a clear violation of an ISM.XML 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.

4.1.6 DES Constraints

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

4.2 Validation Against CVEs

Several ISM attributes are explicitly associated with CVEs. There are constraint rules defining which CVE should be used to verify each such restricted attribute.

Developers of systems processing SCI or SAP from the unpublished register will need to contact the DES POC listed in Appendix E for guidance since those values are not in the CVE.

Validation engines must be aware that CVE may contain patterns in addition to explicit values.

4.3 Obsolete rule numbers

[ISM-ID-00050][] Removed in V2

[ISM-ID-00101][] Removed in V2

[ISM-ID-00051][] Removed in V2

[ISM-ID-00052][] Removed in V2

[ISM-ID-00053][] Removed in V2

[ISM-ID-00054][] Removed in V2

[ISM-ID-00055][] Removed in V2

[ISM-ID-00022][] Removed in V3

[ISM-ID-00076][] Removed in V3

[ISM-ID-00023][] Removed in V4

[ISM-ID-00089][] Removed in V4

[ISM-ID-00120][] Removed in V4

[ISM-ID-00144][] Removed in V4

[ISM-ID-00003][] Removed in V5

[ISM-ID-00004][] Removed in V5

[ISM-ID-00007][] Removed in V5

[ISM-ID-00009][] Removed in V5

[ISM-ID-00010][] Removed in V5

[ISM-ID-00011][] Removed in V5

[ISM-ID-00024][] Removed in V5

[ISM-ID-00025][] Removed in V5

[ISM-ID-00027][] Removed in V5

[ISM-ID-00029][] Removed in V5

[ISM-ID-00039][] Removed in V5

[ISM-ID-00069][] Removed in V5

[ISM-ID-00091][] Removed in V5

[ISM-ID-00092][] Removed in V5

[ISM-ID-00093][] Removed in V5

[ISM-ID-00106][] Removed in V5

[ISM-ID-00114][] Removed in V5

[ISM-ID-00115][] Removed in V5

[ISM-ID-00117][] Removed in V5

[ISM-ID-00131][] Removed in V5

Appendix A 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.

Appendix B Acronyms

This appendix lists all the acronyms referenced in this DES and lists other acronyms that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely acronyms that are not referenced in that particular DES.

CAPCO – Controlled Access Program Coordination Office

CVE – Controlled Vocabulary Enumeration

DCMI – Dublin Core Metadata Initiative

DC MES – Dublin Core Metadata Element Set

DES – Data Encoding Specification

DOI – Digital Object Identifier

DNI – Director National Intelligence

E.O. – Executive Order

GNS – Geographic Names Server

HTML – HyperText Markup Language

IC.ADD – Intelligence Community Abstract Data Definition

IC CIO – Intelligence Community Chief Information Officer

ICD – Intelligence Community Directive

ICEA – Intelligence Community Enterprise Architecture

ICS – Intelligence Community Standard

ISBN – International Standard Book Number

ISM – Information Security Marking Metadata

ISO – International Organization for Standardization

ISOO – Information Security Oversight Office

KA – Knowledge Assertion

KOS – Knowledge Organization System

MIME – Internet Media Types

NARA – National Archives and Records Administration

NGA – National Geospatial Intelligence Agency

NSI – National Security Intelligence

ODNI – Office of the Director of National Intelligence

SSC – Special Security Center

TGN – Thesaurus of Geographic Names

URI – Uniform Resource Identifier

URL – Uniform Resource Locator

W3CDTF – World Wide Web Consortium Date Time Format

XML – Extensible Markup Language

Appendix C Glossary

No pertinent glossary items requiring further definition.

Appendix D Bibliography

This appendix lists all the sources referenced in this DES and lists other sources that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely sources that are not referenced in that particular DES.

(CAPCO Implementation Guide)

Intelligence Community Classification and Control Markings Implementation Manual. Unclassified FOUO version. Volume 3, Edition 1 (Version 3.1). 7 May 2010. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO).
[https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO Implementation%20Manual FOUO v3%2010 07%20May%202010%200.pdf](https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO%20Implementation%20Manual%20FOUO%20v3%2010%2007%20May%202010%200.pdf)

(CAPCO Register)

Authorized Classification and Control Markings Register. Unclassified FOUO version. Volume 3, Edition 1 (Version 3.1). 7 May 2010. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO).
[https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO Register FOUO v3%2010 07%20May%202010%200\(2\).pdf](https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO%20Register%20FOUO%20v3%2010%2007%20May%202010%200(2).pdf)

(DC MES)

Dublin Core Metadata Element Set. Version 1.1. 02 June 2003. Dublin Core Metadata Initiative. <http://dublincore.org/documents/dces/>.

(E.O. 12958, as amended)

Executive Order 12958 – Classified National Security Information, as Amended. Federal Register, Vol. 68, No. 60. 25 March 2003. The White House. <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>.

(E.O. 12829, as amended)

Executive Order 12829 – National Industrial Security Program, as Amended. Federal Register, Vol. 58, No. 240. 16 December 1993. The White House. <http://www.archives.gov/isoo/policy-documents/eo-12829.html>

(E.O. 13526)

Executive Order 13526 – Classified National Security Information 29 December 2009. The White House.
<http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>.

(ICD 206)

Sourcing Requirements for Disseminated Intelligence Products.

Intelligence Community Directive Number 206. 17 October 2007.

Office of the Director of National Intelligence.

http://www.dni.gov/electronic_reading_room/ICD_206.pdf.

(ICD 500)

Director of National Intelligence Chief Information Officer.

Intelligence Community Directive Number 500. 7 August 2008. Office of the Director of National Intelligence.

http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 710)

Classification and Control Markings System. Intelligence Community Directive Number 710. 11 September 2009. Office of the Director of National Intelligence.

http://www.dni.gov/electronic_reading_room/ICD_710.pdf

(ISO 639-2)

Codes for the representation of names of languages – Part 2: Alpha-3 code. ISO 639-2:1998. International Organization for Standardization (ISO).

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4767.

(ISO 3166-1)

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

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719.

(ISO 8601)

Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004. International Organization for Standardization (ISO).

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874.

(ISO 15836)

Information and documentation – The Dublin Core metadata element set. ISO 15836:2009. International Organization for Standardization (ISO).

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142.

(ISO 19757-3:2006)

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

-
- <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
(ISOO Directive 1)
Classified National Security Information (Directive No. 1); Final Rule.
32 CFR Parts 2001 and 2004. Federal Register, Vol. 68, No. 183. 22
September 2003. Information Security Oversight Office (ISOO),
National Archives and Records Administration (NARA).
[http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-
directive.pdf](http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.pdf).
- (RFC 3066)
Tags for the Identification of Languages. January 2001. H.
Alvestrand. Cisco Systems. <http://www.rfc-editor.org/rfc/rfc3066.txt>.
- (Schematron Implementation)
<http://www.schematron.com/>

Appendix E Points of Contact

This technical specification is managed by the Office of the Intelligence Community Chief Information Officer (IC CIO). As of this writing, the IC CIO/IC Enterprise Architecture (ICEA) Directorate facilitates the IC data collaboration and coordination forums responsible for the selection or development of common IC technical data specifications. Direct all inquiries about this IC technical specification to IC CIO/ICEA, the IC's data collaboration and coordination forum, or IC element representatives involved in those forums.

Appendix F Change History

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

Table 3. DES Version Identifier History

| Version | Identifier | Date | Purpose |
|---------|--------------------------|---------------------|---|
| 1.0 | | August 2008 | Initial Release |
| 2 | ICTechSpec 500.D.2-V2 | 24 December 2009 | Routine revision to technical specification. For details of changes, see appendix F.4 |
| 3 | ICTechSpec 500.D.2-V3 | 4 June 2010 | Routine revision to technical specification. For details of changes, see appendix F.3 |
| 4 | ICTechSpec 500.D.2-V4 | 7 September 2010 | Routine revision to technical specification. For details of changes, see appendix F.2 |
| 5 | ICTechSpec 500.D.2-V4 | 6 December 2010 | Routine revision to technical specification. For details of changes, see appendix F.1 |

F.1 V5 Change Summary

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

Table 4. 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 ISM-ID-00160 Change | Data generation and Ingestion systems need to be updated to use the new structures and to properly enforce the new constraint rules |
| 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 @typeOfExemptedSource and @dateOfExemptedSource 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. |
| 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 – FGIsorceOpen deprecation warning ISM-ID-00189 – FGIsorceOpen deprecation error ISM-ID-00190 – FGIsorceProtected 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-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 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 | |

| Change | Artifacts changed | Compatibility Notes |
|--------|--|---------------------|
| | ISM-ID-00208 – atomicEnergyMarkings deprecation warning ISM-ID-00209 – atomicEnergyMarkings deprecation error ISM-ID-00210 – nonUSControls deprecation warning ISM-ID-00211 – nonUSControls deprecation error | |

F.2 V4 Change Summary

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

Table 5. Data Encoding Specification V4 Change Summary

| Change | Artifacts changed | Compatibility Notes |
|--|--|--|
| Add support for DoD Distro 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 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 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. |

F.3 V3 Change Summary

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

Table 6. 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 and follow E.O. 13526 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. | Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089 | Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 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 references to E.O. 12958 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 and follow E.O. 13526 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 rules to exclude the resource element from being considered in rollup constraints. | Constraint Rules ISM- CONTRIBUTES | Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 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 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 and follow E.O. 13526 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 and follow E.O. 13526 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 and follow E.O. 13526 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 |

| Change | Artifacts changed | Compatibility Notes |
|---|--|---|
| 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 and follow E.O. 13526 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. |
| 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. |
| Add check that RELIDO is required on all portions to appear in banner | ISM-ID-00132 | Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 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 |
|---|--|--|
| Add check that NF is not allowed on U portions. | ISM-ID-00140 | Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 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 requirements for Authority block | ISM-ID-00141 ISM-ID-00017 ISM-ID-00142 ISM-ID-00143 | Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 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. |
| 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 and follow E.O. 13526 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 and follow E.O. 13526 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. |

F.4 V2 Change Summary

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

Table 7. 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 @compilationReason 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. |

| Change | Artifacts changed | Compatibility Notes |
|---|---|---|
| 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 and follow E.O. 12958, as amended 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. |
| 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 and follow E.O. 12958, as amended 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: @ownerProducer, @SCIcontrols, @SARIdentifier, @disseminationControls, @FGISourceOpen, @FGISourceProtected, @releasableTo, @nonICmarkings, @declassException, @typeOfExemptedSource. | Constraint Rules Controlled Value Enumerations | Data generation systems that correctly implement CAPCO guidance and follow E.O. 12958, as amended 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 |
|---|---------------------------------------|---|
| Removed @declassManualReview | Constraint Rules ADD Mapping Table | Data generation systems should be updated to prohibit @declassManualReview on new data. Ingestion systems need to be updated to reject @declassManualReview 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 @declassException and @typeOfExemptedSource 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. |
| Added attributes to enable defining of the roles that ISM attributes play in a document. @resourceElement, @excludeFromRollup | 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. @createDate | 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 |

| Change | Artifacts changed | Compatibility Notes |
|---------------|--------------------------|---|
| | | data. Schemas and/or DESs using ISM.XML need to implement this attribute appropriately. |

Appendix G Configuration Management

The selection or development of technical data specifications of common interest to the IC are collaborated and coordinated currently within governance forums managed by the IC CIO. Change requests for this technical data specification should be directed to the office identified in **Appendix E – Points of Contact**.

Appendix H Controlled Vocabulary Enumerations

The Controlled Vocabulary Enumerations (CVEs) used in this DES are as follows:

Table 8. CVE Definitions

| CVE File name | Definition | Attribute and Rules Cross reference |
|------------------------|---|---|
| CVEnumISMSCIControls | All currently valid SCI controls from the published register | @SCIcontrols ISM-ID-00042 ISM-ID-00204 ISM-ID-00205 Schema |
| CVEnumISMSAR | All currently valid SAR controls from the published register | @SARIdentifier ISM-ID-00202 ISM-ID-00203 ISM-ID-00121 Schema |
| CVEnumISMRelTo | USA followed by all currently valid ISO Trigraphs except USA in alphabetical order by Trigraph, followed by all currently valid CAPCO Coalition tetragraphs in alphabetical order by tetragraph | @releasableTo ISM-ID-00041 ISM-ID-00167 ISM-ID-00198 Schema |
| CVEnumISMOwnerProducer | FGI followed by all currently valid ISO Trigraphs in alphabetical order by Trigraph, followed by all currently valid CAPCO Coalition tetragraphs in alphabetical order by tetragraph | @ownerProducer ISM-ID-00100 ISM-ID-00196 ISM-ID-00197 Schema |
| CVEnumISMNonIC | All currently valid Non-IC markings from the published register | @nonICmarkings ISM-ID-00035 ISM-ID-00192 ISM-ID-00193 Schema |
| CVEnumISM25X | All currently authorized 25X values | @declassException ISM-ID-00206 ISM-ID-00207 Schema |
| CVEnumISMFGIProtected | FGI followed by all currently valid ISO Trigraphs except USA in alphabetical order by Trigraph, followed by all currently valid CAPCO Coalition tetragraphs in alphabetical order by tetragraph | @FGISourceProtected ISM-ID-00096 ISM-ID-00190 ISM-ID-00191 Schema |

| CVE File name | Definition | Attribute and Rules Cross reference |
|--------------------------------|---|--|
| CVEnumISMFGIOpen | UNKNOWN followed by all currently valid ISO Trigraphs except USA in alphabetical order by Trigraph, followed by all currently valid CAPCO Coalition tetragraphs in alphabetical order by tetragraph | @FGISourceOpen ISM-ID-00095 ISM-ID-00188 ISM-ID-00189 Schema |
| CVEnumISMDissem | All currently valid Dissemination controls from the published register | @disseminationControls ISM-ID-00026 ISM-ID-00179 ISM-ID-00180 Schema |
| CVEnumISMClassificationUS | All currently valid US classification marks | @classification ISM-ID-00040 |
| CVEnumISMClassificationAll | All currently valid classification marks | @classification Schema |
| CVEnumISMAutomicEnergyMarkings | All currently valid Atomic Energy information markings from the published register | @atomicEnergyMarkings ISM-ID-00178 ISM-ID-00208 ISM-ID-00209 |
| CVEnumISMAttributes | All currently authorized ISM attribute names | ISM-ID-00125 |
| CVEnumISMCompliesWith | Current rule set names that documents may comply with | @compliesWith Schema |
| CVEnumISMNonUSControls, | NonUS Control markings supported by ISM | @nonUSControls ISM-ID-00210 ISM-ID-00211 Schema |
| CVEnumISMNotice | All currently authorized Notice values | @notice Schema |