



# **Intelligence Community Technical Specification**

---

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

**Version 11**

10 April 2013

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
1.7 - Dependencies .....	4
1.7.1 - Dependencies required to download for Standalone Package .....	4
1.8 - Conformance .....	4
Chapter 2 - Development Guidance .....	6
2.1 - Relationship to Abstract Data Definition and other encodings .....	6
2.2 - Additional Guidance .....	6
2.2.1 - Physical XML Attribute Groups .....	6
2.2.2 - Notices .....	7
2.2.2.1 - US-Person .....	8
2.2.2.2 - Point Of Contact Requirements .....	8
2.2.2.3 - pre13526ORCON .....	8
Chapter 3 - Data Constraint Rules .....	10
3.1 - Constraint Rule Types .....	10
3.2 - "Living" Constraint Rules .....	10
3.3 - Classified or Controlled Constraint Rules .....	10
3.4 - Terminology .....	10
3.5 - Errors and Warnings .....	11
3.6 - Rule Identifiers .....	11
3.7 - Data Validation Constraint Rules .....	11
3.7.1 - Purpose .....	11
3.7.2 - Schematron .....	11
3.7.3 - Non-null Constraints .....	12
3.7.4 - Value Enumeration Constraints .....	12
3.7.5 - Additional Constraints .....	12
3.7.5.1 - DES Constraints .....	12
3.7.6 - Constraint Rules .....	13
3.8 - Data Rendering Constraint Rules .....	13
3.8.1 - Purpose .....	13
3.8.2 - Rendering Constraint Rules .....	13
Chapter 4 - Conformance Validation .....	14
4.1 - Business Rule Validation .....	14
Chapter 5 - Generated Guides .....	15
5.1 - Schema Guide .....	15
5.2 - Schematron Guide .....	16
Appendix A - Feature Summary .....	17
A.1 - ISM Feature Summary .....	17
Appendix B - Change History .....	23
B.1 - V11 Change Summary .....	23
B.2 - V10 Change Summary .....	25

---

B.3 - V9 Change Summary .....	33
B.4 - V8 Change Summary .....	36
B.5 - V7 Change Summary .....	39
B.6 - V6 Change Summary .....	42
B.6.1 - V6 Change Errata .....	47
B.7 - V5 Change Summary .....	47
B.7.1 - V5 Change Errata .....	54
B.8 - V4 Change Summary .....	54
B.9 - V3 Change Summary .....	56
B.10 - V2 Change Summary .....	61
Appendix C - Acronyms .....	65
Appendix D - Bibliography .....	70
Appendix E - Points of Contact .....	74
Appendix F - IC CIO Approval Memo .....	75

## List of Tables

Table 1 - Dependencies .....	4
Table 2 - Constraint Rules .....	13
Table 3 - Feature Summary Legend .....	17
Table 4 - ISM Feature comparison .....	17
Table 5 - DES Version Identifier History .....	23
Table 6 - Data Encoding Specification V11 Change Summary .....	24
Table 7 - Data Encoding Specification V10 Change Summary .....	26
Table 8 - Data Encoding Specification V9 Change Summary .....	33
Table 9 - Data Encoding Specification V8 Change Summary .....	36
Table 10 - Data Encoding Specification V7 Change Summary .....	40
Table 11 - Data Encoding Specification V6 Change Summary .....	42
Table 12 - Data Encoding Specification V6 Change Errata .....	47
Table 13 - Data Encoding Specification V5 Change Summary .....	48
Table 14 - Data Encoding Specification V5 Change Errata .....	54
Table 15 - Data Encoding Specification V4 Change Summary .....	55
Table 16 - Data Encoding Specification V3 Change Summary .....	56
Table 17 - Data Encoding Specification V2 Change Summary .....	62
Table 18 - Acronyms .....	65

## 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 is applicable 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 IC 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>[11]</sup> grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, 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 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 ICS 500-21, <sup>[17]</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 achieving the IC's data discovery, data sharing, and interoperability goals.

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 Extensible Markup Language (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, for e.g. Microsoft Word, define document properties; styles; fields; cardinalities; processing requirements; and use.

## 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 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 (E.O.) 13526,<sup>[7]</sup> ICD 710 Classification and Control Marking System,<sup>[13]</sup> and implemented by the CAPCO Register and Manual,<sup>[1]</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>[8]</sup>

- 500 Series:
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC<sup>[12]</sup>
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information<sup>[17]</sup>
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility<sup>[9]</sup>
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination<sup>[10]</sup>
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide<sup>[15]</sup>
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System<sup>[13]</sup>
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control<sup>[14]</sup>

## 1.5 - Audience and Applicability

DESS are primarily intended 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 conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,<sup>[16]</sup> defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

## 1.6 - Conventions

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

The keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this technical specification are to be interpreted as described in the IETF RFC 2119.<sup>[18]</sup> These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of

implementations. When these words are not capitalized, they are meant in their natural-language sense.

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

## 1.7 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in the following table. The documents listed below are referenced in this Data Encoding Specification, and are normative or informative as indicated in the dependencies table.

**Table 1 - Dependencies**

Name	Dependency Description
CAPCO Register and Manual (6.0) <sup>[1]</sup>	Policy Driver
DoD Manual 5200.1 February 2012 <sup>[4]</sup>	Policy Driver
ISO Schematron <sup>[28]</sup> implementation by Rick Jelliffe (2010-04-14)	Specification uses Schematron to encode IC business rules for this specification. Conformance to the logic of the business rules is normative, whereas use of the schematron language to encode them is informative.
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.

### 1.7.1 - Dependencies required to download for Standalone Package

ISM does not depend on any specification that would have to be downloaded separately.

## 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 or enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron<sup>[28]</sup> code version of the constraint rules are normative for this DES. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119<sup>[18]</sup> is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs<sup>[30]</sup>. For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of `ism:DESVersion='9'` to `ism:DESVersion='10'` in the `xsd:schema` statement. The ability to import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications, such as ISM CVE updates. The decoupling of dependency versions is not retroactive, see the dependency table for allowed dependency versions.

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

## Chapter 2 - Development Guidance

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

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

The mappings in the IC.ADD 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.

### 2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is not clearly a single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers of this DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

#### 2.2.1 - 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 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.<sup>[13]</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 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 rollup 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 TS even though the data extracted was U and the document the source citation is U.

## 2.2.2 - Notices

The **ISMNoticeAttributesGroup** can be used on an element to signify that it contains notice information concerning a "well-defined" security notice such as 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 CAPCO Register and Manual<sup>[1]</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 CAPCO Register and Manual<sup>[1]</sup> and/or whose values 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 CAPCO.

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 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.

### 2.2.2.1 - 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 in the CVE provides a standard implementation for all producing agencies.

### 2.2.2.2 - 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.

### 2.2.2.3 - 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 EO 13526, classified ORCON documents created prior to the effective date of the order 29 December 2009 should be handled according to EO 12958, as amended, and documents

created after this date should be handled according to EO 13526. However, derived products that include ORCON data produced prior to 29 December 2009 must include a statement that it should be handled according to the previous E.O. 12958, as amended;<sup>[6]</sup> this statement is marked with the **@noticeType** attribute value [pre13526ORCON]. The attribute indicates that the document contains ORCON information that predates E.O. 13526,<sup>[7]</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. With questions, contact John Smith,
    AgencyX,
    888-555-5555, jsmith@agencyx.gov.
  </NoticeText>
</Notice>
```

## Chapter 3 - Data Constraint Rules

### 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 to be resolved. 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>[13]</sup> implemented in the CAPCO Register and Manual,<sup>[1]</sup> ISOO 32 CFR Parts 2001 and 2004 (as of September 22, 2003),<sup>[21]</sup> Executive Order (E.O.) 13526, as amended,<sup>[7]</sup> and E.O. 12829, as amended.<sup>[5]</sup> These rules will be expanded and modified as the model matures, the CAPCO Register and Manual <sup>[1]</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 DES artifacts wherever they are located.

### 3.4 - 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 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 constraint rule IDs are prefixed with “ISM-ID-”.

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

## 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>[28]</sup> was selected as the language in which to encode these additional rules. The provided Schematron<sup>[28]</sup> is used to define the constraint rules; it is NOT a required implementation. Implementers 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*<sup>[27]</sup> or the XML Stylesheet Language for Transformation (XSLT) 2.0<sup>[32]</sup>

implementation of International Organization for Standardization (ISO) Schematron<sup>[28]</sup> provided by Rick Jelliffe at <http://schematron.com/> [<http://schematron.com/>]. Constraint rules are dependent on XPath 2.0<sup>[31]</sup> and XSLT 2.0<sup>[32]</sup> features. According to Mr. Jelliffe, the editor of Schematron<sup>[28]</sup> 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<sup>[28]</sup> implementation and XSLT 2.0<sup>[32]</sup> files provided as a convenience 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 — which allows for empty (or null) content. 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 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.

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.

---

<sup>1</sup>"white space" is defined in XML 1.0<sup>[29]</sup> as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

## 3.7.6 - Constraint Rules

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

## 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 2 - Constraint Rules**

Rule Number	Severity	Description	Human Readable Description
There are no Data Rendering Constraint rules at this time.			

## **Chapter 4 - Conformance Validation**

An instance is considered conformant with the this specification if it passes all of the following normative validation steps. The following steps do not dictate how this validation strategy is implemented.

### **4.1 - Business Rule Validation**

As this specification has no normative schema the only necessary compliance validation step is to ensure that an instance document complies with the business rules expressed in this specification. It should be noted that while the business rules for this specification are expressed in Schematron, the Schematron is informative but the constraints they express are normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the Schematron included in this specification and its dependencies.

## 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>®</sup> [\[27\]](#), 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 SchematronGuide 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 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 CAPCO Register and Manual<sup>[1]</sup> the date is often one year after the date of Register and Manual. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

**Table 3 - Feature Summary Legend**

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can't comply)
N/A	Not Applicable. Feature is no longer required.

Cell Colors represent the same information as the Key value

### A.1. ISM Feature Summary

**Table 4 - ISM Feature comparison**

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
CAPCO Register and Manual 2.1	Declass Removed from Banner	N	F	F	F	F	F	F	F	F	F	F
January 22, 2009 (1 year after 2008 memo)												
E.O. 13526 <sup>[7]</sup>	Compilation Reason	N	F	F	F	F	F	F	F	F	F	F
December 29, 2009												
CAPCO Register and Manual 3.1	LES	P	N	F	F	F	F	F	F	F	F	F
May 7, 2010												
CAPCO Register and Manual 3.1	LES-NF	P	N	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
Pre 2008												
CAPCO Register and Manual 4.1	KDK	N	N	F	F	F	F	F	F	F	F	F
December 10, 2010												

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
ICD 710 <sup>[13]</sup> September 11, 2009	710 Foreign Disclosure or Release	P	P	F	F	F	F	F	F	F	F	F
E.O. 13526 <sup>[7]</sup> December 29, 2009	DeclassReasons/Dates	P	P	F	F	F	F	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	schema validation of CVE values	N	N	N	F	F	F	F	F	F	F	F
DoD Instruction 5230.24 <sup>[3]</sup> March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F	F	F	F
DoD Directive 5240.01 <sup>[2]</sup> August 27, 2007	US Person Notice	P	P	P	P	F	F	F	F	F	F	F
CAPCO Register and Manual 2.2 September 25, 2010 (1 Year after 2.2)	Remove SAMI	P	P	P	P	F	F	F	F	F	F	F
ISOO Marking Booklet 2010 <sup>[22]</sup> / ISOO Notice 2009-13 <sup>[23]</sup> December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F	F	F
E.O. 13526 <sup>[7]</sup> December 29, 2009	derivativelyClassifiedBy	P	P	P	P	F	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Atomic Energy New banner location	N	N	N	N	F	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Display Only	N	N	N	N	F	F	F	F	F	F	F
IC-CIO enhance data quality See IC ESB	Schematron <sup>[28]</sup> Implementation of rules	N	N	N	N	F	F	F	F	F	F	F

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
E.O. 13526 <sup>[7]</sup> December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F	F	F
DoD Manual 5200.1 <sup>[4]</sup> January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[20]</sup> June 28, 2010	TFNI	N	N	N	N	N	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F	N	N	F
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	F	F	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	MIFH, EUDA and EFOR removed	P	P	P	P	P	P	F	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010) <sup>[20]</sup> June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F	N/A	N/A
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F	F	F
ICD 710 <sup>[13]</sup> September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F	F	F
DNI ORCON Memo <sup>[26]</sup> March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F	N/A	N/A

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
ISOO Marking Booklet <sup>[22]</sup> December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	F	F	F	F
IC-CIO enhance data quality See IC ESB December 30, 2012	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F	F	F	F
IC-CIO enhance data quality See IC ESB	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	F	F	F	F
IC-CIO enhance data quality See IC ESB	@ism:excludeFromRollup=true() allowed to not have an ICD-710 foreign release indicator	N	N	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SINFO Remove	P	P	P	P	P	P	P	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SC Remove	P	P	P	P	P	P	P	F	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Require using 50X1-HUM instead of 25X1-human	N	N	N	N	P	P	P	F	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of KDK compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of SI compartments and sub-compartments	N	N	N	N	N	N	N	N	F	F	F
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F	F	F

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F	F	F
DoD Manual 5200.1-R <sup>[4]</sup> February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F	F	F
DoD Manual 5200.1-R <sup>[4]</sup> February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F	F	F
Decouple ISM from the Schema January 2013	Schema is Informative, Schematron and CVEs are Normative.	N	N	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 December 2012	Add ENDSEAL system with compartments ECRU and NONBOOK	N	N	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 December 2013	Limit KDK system compartments to BLUEFISH, IDITAROD and KANDIK.	N	N	N	N	N	N	N	N	P	F	F
ISOO Notice 2013-01 <sup>[25]</sup> November 2012	Support NATO exemptions to declass date.	N	N	N	N	N	N	N	N	N	F	F
CAPCO Register and Manual 5.1 December 2013	Support multiple non JOINT countries prior to the Classification.	N	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 6.0 Feb 2014	Support ORCON-USGOV.	N	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 6.0 Feb 2014	Support RD precedence over FRD.	N	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 6.0 Feb 2014	Treat caveated UNCLASSIFIED as RELIDO unless explicitly specified.	N	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 6.0 Feb 2014	Allow commingling of SBU and SUB-NF with classified information in portions.	N	N	N	N	N	N	N	N	N	N	F

ISM Feature Comparison												
Driver	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11
Required date												
CAPCO Register and Manual 6.0, Appendix D Feb 2014	50X1 and 50X6	N	N	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 6.0, Appendix B, Section 4 Feb 2014	Allow newly registered NATO Dissemination Controls REL TO and NOFORN	P	P	P	P	P	P	P	P	P	P	P
CAPCO Register and Manual 6.0 Feb 2014	Allow JOINT classification markings with SCI, SAP, AEA, IC and non-IC Dissemination Control Markings (excluding NOFORN)	F	F	F	F	F	F	F	F	F	F	F
CAPCO Register and Manual 6.0, Appendix A, Enclosure 1 Feb 2014	Allow Non-US classification markings with US SCI, SAP, AEA, IC and non-IC Dissemination control markings (excluding NOFORN)	F	F	F	F	F	F	F	F	F	F	F

## Appendix B Change History

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

**Table 5 - 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.10 - V2 Change Summary</a>
3	4 June 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.9 - V3 Change Summary</a>
4	7 September 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.8 - V4 Change Summary</a>
5	6 December 2010	Routine revision to technical specification. For details of changes, see <a href="#">Section B.7 - V5 Change Summary</a>
6	11 April 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.6 - V6 Change Summary</a>
7	9 August 2011	Routine revision to technical specification. For details of changes, see <a href="#">Section B.5 - V7 Change Summary</a>
8	27 February 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - V8 Change Summary</a>
9	17 July 2012	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V9 Change Summary</a>
10	21 January 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V10 Change Summary</a>
11	5 April 2013	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V11 Change Summary</a>

### B.1 - 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.)
- CAPCO Register and Manual 5.1

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

**Table 6 - 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 5.1 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 disseminControls and created schematron rules to enforce correct usage.	CVerenumISMDissem 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 or FRD 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.2 - V10 Change Summary

Significant drivers for Version 10 include:

- CAPCO Register and Manual 5.1 and approved Change Requests

- 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 7 - Data Encoding Specification V10 Change Summary**

Change	Artifacts changed	Compatibility Notes
Fixed a misspelled include of an abstract rule in the master ISM value.		
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  CVEnumISMReITo 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
<p>Clarified the description in the Schematron rules that deal with deprecated values in the CVE files [artf13026].</p>	<p>Schematron</p> <p>ISM-ID-00166 Changed</p> <p>ISM-ID-00170 Changed</p> <p>ISM-ID-00179 Changed</p> <p>ISM-ID-00180 Changed</p> <p>ISM-ID-00188 Changed</p> <p>ISM-ID-00189 Changed</p> <p>ISM-ID-00190 Changed</p> <p>ISM-ID-00191 Changed</p> <p>ISM-ID-00192 Changed</p> <p>ISM-ID-00193 Changed</p> <p>ISM-ID-00194 Changed</p> <p>ISM-ID-00195 Changed</p> <p>ISM-ID-00196 Changed</p> <p>ISM-ID-00197 Changed</p> <p>ISM-ID-00198 Changed</p> <p>ISM-ID-00199 Changed</p> <p>ISM-ID-00200 Changed</p> <p>ISM-ID-00201 Changed</p> <p>ISM-ID-00202 Changed</p> <p>ISM-ID-00203 Changed</p> <p>ISM-ID-00204 Changed</p> <p>ISM-ID-00205 Changed</p> <p>ISM-ID-00206 Changed</p> <p>ISM-ID-00207 Changed</p> <p>ISM-ID-00208 Changed</p>	<p>Should not impact data.</p>

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 DataHasCorresponding Notice 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>[25]</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 FD&R 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.3 - V9 Change Summary

Significant drivers for Version 9 include:

- CAPCO Register and Manual 5.1

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

**Table 8 - 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 intel products required the ICD710 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.4 - V8 Change Summary

Significant drivers for Version 8 include:

- CAPCO Register and Manual 5.1
- ISOO Guidance (ISOO Notice 2012-02)<sup>[24]</sup>
- ISO 3166-1<sup>[19]</sup>

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

**Table 9 - Data Encoding Specification V8 Change Summary**

Change	Artifacts changed	Compatibility Notes
Updated country code descriptions in the ISO 3166-1 <sup>[19]</sup> CVEs to reflect ISO newsletter changes.	schema Changed CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMReITo Changed	Data generation and Ingestion systems need to be updated to properly use the new values.
Allow use of RSV.	schema Changed CVEnum-ISMSCIControls 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>[13]</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.5 - V7 Change Summary

Significant drivers for Version 7 include:

- CAPCO Register and Manual 4.2
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)<sup>[20]</sup>
- ISO 3166-1<sup>[19]</sup>
- DNI ORCON Memo<sup>[26]</sup>
- ICD 710<sup>[13]</sup>

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

**Table 10 - 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 CVEnumISMElements Added CVEnumISMAttributes 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>[13]</sup> and DoD Distribution statements.	Schema CVEnumISMAttributes Changed CVEnumISMPocType-Added ISM-ID-00222 Added ISM-ID-00224 Added	Data generation and ingestion systems need to be updated to use the new values and comply with the new constraint rules.
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 CVEnumISMACCM 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 CVEnumISMAttributes 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> .	CVEnumISM25X 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 <sup>[1]</sup> , their deprecation dates were added to the CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMReITo 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>[19]</sup> CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMReITo Changed	Data generation and Ingestion systems need to be updated to properly use the new values.

## B.6 - V6 Change Summary

Significant drivers for Version 6 include:

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

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

**Table 11 - 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 ISM-ID-00014 Changed ISM-ID-00056 Changed ISM-ID-00057 Changed ISM-ID-00058 Changed ISM-ID-00059 Changed ISM-ID-00060 Changed ISM-ID-00061 Changed ISM-ID-00062 Changed ISM-ID-00063 Changed ISM-ID-00064 Changed ISM-ID-00065 Changed ISM-ID-00066 Changed ISM-ID-00067 Changed ISM-ID-00068 Changed ISM-ID-00069 Changed ISM-ID-00070 Changed ISM-ID-00071 Changed ISM-ID-00072 Changed ISM-ID-00073 Changed ISM-ID-00074 Changed ISM-ID-00075 Changed ISM-ID-00077 Changed ISM-ID-00078 Changed ISM-ID-00079 Changed ISM-ID-00080 Changed	Now is compliant with intent of ISM check for resourceElement. Only considers the first resourceElement=true() a resource element.

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

Change	Artifacts changed	Compatibility Notes
	ISM-ID-00146 Changed ISM-ID-00147 Changed ISM-ID-00149 Changed ISM-ID-00150 Changed ISM-ID-00151 Changed ISM-ID-00152 Changed ISM-ID-00153 Changed ISM-ID-00154 Changed ISM-ID-00155 Changed ISM-ID-00160 Changed ISM-ID-00161 Changed ISM-ID-00162 Changed ISM-ID-00165 Changed	
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 FGIsorceProtected 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 FGIsorceOpen 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 FGIsorceProtected 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 SClcontrols.	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.6.1 - V6 Change Errata

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

**Table 12 - 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.7 - V5 Change Summary

Significant drivers for Version 5 include:

- CAPCO Register and Manual 4.1

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

**Table 13 - 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.	<p>ISM-ID-00166 – classification deprecation warning</p> <p>ISM-ID-00170 – classification deprecation error</p> <p>ISM-ID-00179 – disseminationControls deprecation warning</p> <p>ISM-ID-00180 – disseminationControls deprecation error</p> <p>ISM-ID-00188 – FGIsourcesOpen deprecation warning</p> <p>ISM-ID-00189 – FGIsourcesOpen deprecation error</p> <p>ISM-ID-00190 – FGIsourcesProtected deprecation warning</p> <p>ISM-ID-00191 – FGIsourcesProtected deprecation error</p> <p>ISM-ID-00192 – nonICmarkings deprecation warning</p> <p>ISM-ID-00193 – nonICmarkings deprecation error</p> <p>ISM-ID-00194 – notice deprecation warning</p> <p>ISM-ID-00195 – notice deprecation error</p> <p>ISM-ID-00196 – ownerProducer deprecation warning</p>	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.7.1 - V5 Change Errata

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

**Table 14 - Data Encoding Specification V5 Change Errata**

Change	Artifacts changed	Compatibility Notes
Add 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.8 - V4 Change Summary

Significant drivers for Version 4 include:

- DoD Directive 5230.24<sup>[3]</sup>
- ICD 710<sup>[13]</sup> (enforce immediately no grace)

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

**Table 15 - 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>[13]</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>[13]</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.9 - V3 Change Summary

Significant drivers for Version 3 include:

- Executive Order 13526<sup>[7]</sup> (enforce requirements for Authority block)
- CAPCO Register and Manual 3.1
- ICD 710<sup>[13]</sup>

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

**Table 16 - 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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[13]</sup>	Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data generation systems that correctly implement CAPCO guidance <sup>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[6]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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.

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 <sup>[1]</sup> and follow E.O. 13526 <sup>[7]</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.
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.

Change	Artifacts changed	Compatibility Notes
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 <sup>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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>[1]</sup> and follow E.O. 13526 <sup>[7]</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.10 - V2 Change Summary

Significant drivers for Version 2 include:

- Executive Order 12958, as amended <sup>[6]</sup>(`compilationReason`)
- CAPCO Register and Manual 2.1
- ISOO 32 CFR Parts 2001 and 2004 (Guidance on Type of Exempted Source [as of September 22, 2003])<sup>[21]</sup>

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

**Table 17 - 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>[1]</sup> and follow E.O. 12958, as amended <sup>[6]</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>[1]</sup> and follow E.O. 12958, as amended <sup>[6]</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>@FGIsorceOpen</b> , <b>@FGIsorceProtected</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>[1]</sup> and follow E.O. 12958, as amended <sup>[6]</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
<p>Added attributes to enable defining of the roles that ISM attributes play in a document.</p> <p><b>@resourceElement,</b> <b>@excludeFromRollup</b></p>	<p>Schema</p> <p>Constraint Rules</p>	<p>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.</p>
<p>Added attribute to enable ISM date based rules.</p> <p><b>@createDate</b></p>	<p>Schema</p> <p>Constraint Rules</p>	<p>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.</p>

## Appendix C 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.

**Table 18 - Acronyms**

Name	Definition
A&A	Authorization and Accreditation
ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ADD	Abstract Data Definition
API	Applications Programming Interface
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BBOX	Bounding Box
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CAT	Catalog Services Interface Standard
CDR	Content Discovery and Retrieval
CF-NetCDF	Climate and Forecast - Network Common Data Format
CMS	Cryptographic Message Syntax
COMET	Completely Open Mapping Environment
CONOPS	Concept of Operations
CORBA	Common Object Request Broker Architecture
CQL	Common Catalog Query Language (CQL)
CRL	Certificate Revocation List
CSW	Catalog Service for Web
CVE	Controlled Vocabulary Enumeration
D & R	Discovery and Retrieval
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DIA	Defense Intelligence Agency

Name	Definition
DISR	DoD Information Technology Standards and Profile Registry
DNS	Domain Name System
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
EBNF	Extended Backus-Naur Form
EDH	Enterprise Data Header
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
EPR	Endpoint Reference
FOUO	For Official Use Only
FTP	File Transfer Protocol
GENC	Geopolitical Entities, Names, and Codes
GeoRSS	Geographic Really Simple Syndication
GeoTIFF	Geographic Tagged Image File Format
GIF	Graphics Interchange Format
GIS	Geospatial Information System
GML	Geography Markup Language
GNS	Geographic Names Server
GUIDE	Globally Unique Identifiers for Everything
GVS	GEOINT Visualization Services
HDF-EOS	Hierarchical Data Format - Earth Observing System
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I2	Information Integration
IC	Intelligence Community
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
IC EA	IC Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard

Name	Definition
ICSR	Intelligence Community Standards Registry
IdAM	Identity and Access Management
IDM	Interface Data Model
IDMView	Interface Data Model View
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability
IP	Internet Protocol
IPT	Integrated Project Team
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JPEG	Joint Photographic Experts Group
JPIP	JPEG 2000 Interactive Protocol
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWICS	Joint Worldwide Intelligence Communications System
JWT	JSON Web Token
KA	Knowledge Assertion
KML	Keyhole Markup Language
KOS	Knowledge Organization System
KVP	Key Value Pair
LIMDIS	Limited Distribution
LNI	Library of National Intelligence
MAC	Multi Audience Collection
MCG&GIL	Mapping, Charting, and Geodesy Information Library
MCGView	Mapping, Charting, and Geodesy View
MIME	Multipurpose Internet Mail Extensions
MTOM	Message Transmission Optimization Mechanism
NARA	National Archives and Records Administration
NCES	Net-Centric Enterprise Services
NGA	National Geospatial Intelligence Agency
NGDS	Net-Centric GEOINT Discovery Services
NGT	Next Generation Trident

Name	Definition
NIPR	Non-Classified Internet Protocol Router Network
NITF	National Imagery Transmission Format
NPE	Non-Person Entity
NRO	National Reconnaissance Office
NSG	National System for Geospatial Intelligence
NSI	National Security Information
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
OGC	Open Geospatial Consortium
OGCA	Open Geospatial Consortium Australia
OGCE	Open Geospatial Consortium Europe
OWS	OGC Web Services
PAP	Policy Administration Point
PAYL	Payload
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
PUBS	Intelligence Publications
PURL	Persistent Uniform Resource Locator
RA	Reference Architecture
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SIPR	Secret Internet Protocol Router Network
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSD	Special Security Directorate
SSL	Secure Sockets Layer
STIL	Saint Louis Information Library

Name	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TIFF	Tagged Image File Format
TIN	Triangulated Irregular Network
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universal Unique Identifier
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WARP	Web Based Access and Retrieval Portal
WCS	Web Coverage Service
WFS	Web Feature Service
WMS	Web Map Service
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XPath	XML Path Language
XPointer	XML Pointer Language
Xquery	XML Query
XSLT	XML Stylesheet Language for Transformations

## Appendix D Bibliography

### Bibliography

[1] CAPCO Register and Manual

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*. Unclassified FOUO version. Volume 6. (Version 6.0). Effective: 28 February 2013.

Available online IntelLinkU at: [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)

[2] DoD Directive 5240.01

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

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/524001p.pdf>

[3] 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.dtic.mil/whs/directives/corres/pdf/523024p.pdf>

[4] DoD Manual 5200.1

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

Vol 1 Available online at: [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol1.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf)

Vol 2 Available online at: [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol2.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf)

Vol 3 Available online at: [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol3.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf)

Vol 4 Available online at: [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol4.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf)

[5] 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>

[6] 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>

[7] 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>

[8] 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 JWICS at: <http://go.ic.gov/HvBHBmY>

[9] 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)

[10] 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\\_209\\_Tearline\\_Production\\_and\\_Dissemination.pdf](http://www.dni.gov/files/documents/ICD/ICD_209_Tearline_Production_and_Dissemination.pdf)

[11] ICD 500

Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_500.pdf](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

[12] ICD 501

Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_501.pdf](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

[13] ICD 710

Director of National Intelligence Chief Information Officer. *Classification and Control Markings System*. Intelligence Community Directive 710. 11 September 2009.  
Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_710.pdf](http://www.dni.gov/files/documents/ICD/ICD_710.pdf)

[14] ICPG 710.1

Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.  
Available online JWICS at: <http://go.ic.gov/fU3HML>

[15] ICPM 2007-200-2

Assistant Director of National Intelligence for . *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>

[16] 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 IntelLinkU at: [https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500\\_20\\_signed\\_16DEC2010.pdf](https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf)

- [17] 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 IntelLinkU at: [https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS\\_500-21\\_SIGNED\\_20110128.pdf](https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf)
- [18] 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>
- [19] 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)
- [20] 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>
- [21] 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: <http://edocket.access.gpo.gov/2003/pdf/03-24047.pdf>
- [22] 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>
- [23] 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/notice-2009-13.pdf>
- [24] 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>
- [25] ISOO Notice 2013-01  
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *ISOO Notice 2013-01: Further Marking Guidance on*

*Commingleing North Atlantic Treaty Organization (NATO) and Classified National Security Information (NSI).*

Available online at: [www.archives.gov/isoo/notices/notice-2013-01.pdf](http://www.archives.gov/isoo/notices/notice-2013-01.pdf)

[26] 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>[14]</sup>, rescinded the ORCON Memo.

Available online at: [https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings\\_ES%2000045.pdf](https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf)

Attachment A: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf>

Attachment B: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf>

Attachment C: <https://intelshare.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf>

[27] Oxygen

SyncRO Soft. <oXygen/> XML Editor. version 14.1.

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

[28] Schematron

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

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

[29] 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>

[30] XML Catalogs

The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs.* Committee Specification 06 Aug 2001.

Available online at: <https://www.oasis-open.org/committees/entity/spec-2001-08-06.html>

[31] 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/>

[32] XSLT2

World Wide Web Consortium (W3C) . *XSL Transformations (XSLT) Version 2.0.* W3C Recommendation 23 January 2007.

Available online at: <http://www.w3.org/TR/xslt20/>

## 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 DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Public Website: <http://purl.org/ic/standards/public>

E-mail: <[datastandardssupport@ugov.gov](mailto:datastandardssupport@ugov.gov)> or  
<[ic-standards-support@intelink.gov](mailto:ic-standards-support@intelink.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>[16]</sup>