



Intelligence Community Technical Specification

XML Data Encoding Specification for Information Security Markings

Version 7

9 August 2011

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	2
1.6 - Conventions	3
1.7 - Conformance	3
1.8 - Dependencies	4
Chapter 2 - Development Guidance	5
2.1 - Mapping of Abstract Data Elements to Physical XML Elements	5
2.1.1 - Subject Metadata	5
2.1.2 - Attribute Metadata	9
2.2 - Additional Guidance	14
2.2.1 - Physical XML Attribute Groups	14
2.2.2 - Notices	15
2.2.2.1 - US-Person	16
2.2.2.2 - Point Of Contact Requirements	16
2.2.2.3 - pre13526ORCON	17
Chapter 3 - Data Validation Constraint Rules	18
3.1 - Basics	18
3.1.1 - Schematron	18
3.1.2 - "Living" Constraint Rules	18
3.1.3 - Classified or Controlled Constraint Rules	19
3.1.4 - Terminology	19
3.1.5 - Rule Identifiers	19
3.1.6 - Errors and Warnings	19
3.2 - Non-null Constraints	20
3.3 - Value Enumeration Constraints	20
3.4 - Additional Constraints	20
3.4.1 - DES Constraints	20
3.5 - Constraint Rules	20
3.6 - Obsolete rule numbers	21
Chapter 4 - Data Rendering Constraint Rules	23
4.1 - Basics	23
4.1.1 - "Living" Constraint Rules	23
4.1.2 - Classified or Controlled Constraint Rules	23
4.1.3 - Rule Identifiers	23
4.1.4 - Errors and Warnings	23
4.2 - Constraint Rules	24
4.3 - Obsolete Constraint Rules	24
Chapter 5 - Generated Guides	25
5.1 - Schema Guide	25
5.2 - Schematron Guide	26
Appendix A - Change History	27
A.1 - V7 Change Summary	27

A.2 - V6 Change Summary	30
A.3 - V5 Change Summary	34
A.4 - V4 Change Summary	40
A.5 - V3 Change Summary	41
A.6 - V2 Change Summary	46
Appendix B - Acronyms	49
Appendix C - Bibliography	51
Appendix D - Points of Contact	54
Appendix E - IC CIO Approval Memo	55

List of Tables

Table 1 - Dependencies	4
Table 2 - Mapping of Abstract Data Element to Physical XML Elements	5
Table 3 - Mapping of Abstract Data Element Refinements to Physical XML Attributes	9
Table 4 - Obsolete Rules	21
Table 5 - Constraint Rules	24
Table 6 - Obsolete Rules	24
Table 7 - DES Version Identifier History	27
Table 8 - Data Encoding Specification V7 Change Summary	27
Table 9 - Data Encoding Specification V6 Change Summary	30
Table 10 - Data Encoding Specification V5 Change Summary	34
Table 11 - Data Encoding Specification V4 Change Summary	40
Table 12 - Data Encoding Specification V3 Change Summary	41
Table 13 - Data Encoding Specification V2 Change Summary	46
Table 14 - Acronyms	49

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification* for Information Security Markings (ISM.XML) defines detailed specifications for using Extensible Markup Language (XML) to encode Information Security Markings (ISM) data in compliance with the *Intelligence Community Abstract Data Definition* (IC.ADD). This Data Encoding Specification (DES) defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing security marking concepts using XML.

1.2 - 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 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.

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

Early in the intelligence life cycle, intelligence producers need:

- User interfaces that help reliably assign and manipulate information security markings
- Automated formatting of the IC's classification and control marking system as defined by Executive Order (EO) 13526, ICD 710, Classification and Control Marking System, and implemented by the CAPCO Register and accompanying Implementation Manual, this includes portion marks, security banners, the classification authority block, and other security control markings
- Cross-domain discovery, access, and dissemination capabilities

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

- Secure collaboration
- Content management
- Content and portion-level filtering of discovery results
- Cross-security domain content transfers

1.5 - 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 and applicability for this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*, 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 [RFC 2119]. 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 - 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, CVE values from the XML CVE files, and the Schematron code version of the constraint rules are normative for this DES. The rest of this document, the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files are informative. Additionally, the use of keywords defined in IETF RFC 2119 is considered normative within the scope of the sentence. All other parts of this document are informative.

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

1.8 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in the following table. The documents listed below may or may not be referenced in this Data Encoding Specification, and may or may not be considered normative or informative.

Table 1 - Dependencies

Name
CAPCO Register (4.2)
CAPCO Implementation Manual (4.2)
ISO Schematron implementation by Rick Jelliffe (2010-04-14)
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this DES.

Chapter 2 - Development Guidance

This chapter covers two primary topics:

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

2.1 - Mapping of Abstract Data Elements to Physical XML Elements

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

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

2.1.1 - Subject Metadata

Table 2 - Mapping of Abstract Data Element to Physical XML Elements

Abstract Data Element	Definition	XPath and XML implementation notes
Notice	A statement about an information resource designed to inform those accessing the resource. The statement may provide information about handling or protecting the resource, additional information about interpreting the content, use of the resource, etc.	<p>The following elements are used to represent Notices.</p> <p>NoticeList</p> <p>Notice</p> <p>NoticeText</p> <p>The following attributes are used to classify Notices.</p> <p>@noticeType</p> <p>@noticeDate</p>

Abstract Data Element	Definition	XPath and XML implementation notes
		@noticeReason @pocType @unregisteredNoticeType

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

Abstract Data Element	Definition	XPath and XML implementation notes
Resource Classification Declassification Mark	<p>Classification information and declassification instructions associated with a classified resource based on either an original or derivative classification decision(s).</p> <p>These values are prominently presented with specific labels and formatting on the first page of a document.</p>	<p>The physical structures representing the conceptual refinements for the Resource Classification Declassification Mark are intended to be associated with the entire resource being encoded by the presence of @resourceElement="true" on the element that represents the Resource Security metadata.</p> <p>Note: This is the same element that holds the Resource Security Mark.</p> <p>Note: @compilationReason is used to identify documents intentionally having classification and/or control markings more restrictive than any of the portions in the document.</p> <p>The following attributes represent the Resource Classification Declassification Mark Group.</p> <p>@classificationReason</p> <p>@classifiedBy</p> <p>@compilationReason</p> <p>@declassDate</p> <p>@declassEvent</p> <p>@declassException</p> <p>@derivativelyClassifiedBy</p> <p>@derivedFrom</p>

Abstract Data Element	Definition	XPath and XML implementation notes
Portion Security Mark	<p>The security classification carried by an individual portion or block of narrative or media, such as a title, paragraph, table, list, media, or caption.</p> <p>These values are prominently presented at the beginning of the respective portion, are enclosed in parentheses, and utilize the same separators as the overall classification markings of the information resource.</p>	<p>The following attributes represent the Portion Security Mark.</p> <p>@atomicEnergyMarkings</p> <p>@classification</p> <p>@displayOnlyTo</p> <p>@disseminationControls</p> <p>@FGIsourceOpen</p> <p>@FGIsourceProtected</p> <p>@nonICmarkings</p> <p>@nonUSControls</p> <p>@ownerProducer</p> <p>@releasableTo</p> <p>@SARIdentifier</p> <p>@SCIcontrols</p>

2.1.2 - Attribute Metadata

Table 3 - Mapping of Abstract Data Element Refinements to Physical XML Attributes

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
Applicable Ruleset	The rule sets that a document asserts compliance with.	@compliesWith
Atomic Energy Markings	One or more indicators identifying information controlled under the Atomic Energy Act.	@atomicEnergyMarkings
Classification	A single indicator of the highest level of classification applicable to an information resource or portion within the domain of classified national security information. The Classification element is always used in conjunction with the Owner Producer element.	<p>@classification</p> <p>@compilationReason</p>

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
	Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint).	
Classification Reason	One or more reason indicators or explanatory text describing the basis for an original classification decision.	@classificationReason @compilationReason
Classified By	The identity, by name or personal identifier, and position title of the original classification authority for a resource.	@classifiedBy @compilationReason
Compilation Reason	The reason that a portion or resource is marked with a higher and/or more restrictive mark than its components would indicate. For example this would document why 3 Unclassified bullet items form a Secret List. Without this reason being noted the above-described document would be considered to be mismarked and over-classified.	@compilationReason
Declassification Date	A specific year, month, and day upon which the information shall be automatically declassified if not properly exempted from automatic declassification.	@compilationReason @declassDate
Declassification Event	A description of an event upon which the information shall be automatically declassified if not properly exempted from automatic declassification.	@compilationReason @declassEvent
Declassification Exemption	A single indicator describing an exemption to the nominal 25-year point for automatic declassification. This element may be used in conjunction with the Declassification Date or Declassification Event.	@compilationReason @declassException
Derivatively Classified By	The identity, by name or personal identifier, of the derivative classification authority.	@compilationReason @derivativelyClassifiedBy

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
Derived From	A citation of the authoritative source(s) or reference to "Multiple Sources" of the classification markings used in a classified resource.	@compilationReason @derivedFrom
Display Only To	One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be displayed based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element.	@displayOnlyTo
Dissemination Controls	One or more indicators identifying the expansion or limitation on the distribution of information.	@compilationReason @disseminationControls
FGI Source Open	One or more indicators identifying information, which qualifies as foreign government information, for which the source(s) of the information is not concealed.	@FGIsourceOpen
FGI Source Protected	<p>A single indicator that information qualifies as foreign government information for which the source(s) of the information must be concealed.</p> <p>Within protected internal organizational spaces this element may be used to maintain a record of the one or more indicators identifying information, which qualifies as foreign government information for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.</p>	@FGIsourceProtected

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
Non-Intelligence Community Markings	One or more indicators of the expansion or limitation on the distribution of an information resource or portion within the domain of information originating from non-intelligence components.	@compilationReason @nonICmarkings
Non-US Controls	One or more indicators of the expansion or limitation on the distribution of an information resource or portion within the domain of information originating from non-US components.	@compilationReason @nonUSConrols
Notice	An indicator identifying and categorizing a well-defined security-related notice, such as those described in the CAPCO Register, as well as additional formally-recognized security notice types described in other directives, such as US-Person and DoD Distribution.	@noticeType
Notice Date	The date associated with the notice, such as the date it was issued.	@noticeDate
Notice Reason	Specifies the reason the notice was issued.	@noticeReason

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
Owner Producer	<p>One or more indicators identifying the national government or international organization that have purview over the classification marking of an information resource or portion therein. This element is always used in conjunction with the Classification element. Taken together, the two elements specify the classification category and the type of classification (US, non-US, or Joint).</p> <p>Within protected internal organizational spaces this element may include one or more indicators identifying information, which qualifies as foreign government information, for which the source(s) of the information must be concealed. Measures must be taken prior to dissemination of the information to conceal the source(s) of the foreign government information.</p>	@ownerProducer
Point of Contact	An indicator identifying the entity contains a name and/or contact method for a specific point-of-contact requirement in a document.	@pocType
Releasable To	One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be released based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element.	@releasableTo
Special-Access-Required Program Identifier	One or more indicators identifying the defense or intelligence programs for which special access is required.	@SARIdentifier
SCI Controls	One or more indicators identifying sensitive compartmented information control system(s).	@SCIcontrols

Abstract Data Element Refinement	Definition	XPath and XML implementation notes
Unregistered Notice Type	For use on security notices that are of a category that is not sufficiently defined or widely recognized. This attribute can be used by specifications that import ISM to represent a wider variety of security-related notices.	@unregisteredNoticeType

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 be referenced by other DESs (e.g., Information Resource Metadata or Intelligence Publications) to incorporate the information security marking attributes as needed.

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

- **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.

@excludeFromRollup is an attribute not in any group but should be added to any elements in an implementing schema that may require their attributes to be excluded from rollup logic impacting the resource security element. A classic example of this would be a bibliographic source citation where the desire is to indicate that the classification of the referenced source is TS even though the data extracted was U and the document the source citation is 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, IMCON, FRD, 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, 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/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, an 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** is not required according to the CAPCO Implementation Manual or Register; however, several producing agencies have varying implementations to support notices associated with US-Person information. The inclusion of this value in the CVE provides a standard implementation for all producing agencies.

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 is required. 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.

Example:

```
<Notice classification="U" ownerProducer="USA" noticeType="POC">
  <NoticeText classification="U" ownerProducer="USA"
    pocType="ICD-710 DoD-Dist-C">
    John Smith, AgencyX, 888-555-5555, jsmith@agencyx.gov
  </NoticeText>
</Notice>
```

By using the attributes in the **POCAttributeGroup**, an importing schema could use the **@pocType** attribute to indicate that its own element structures contain the contact information for a point-of-contact requirement for further granularity.

Example:

```
<AuthorInfo ism:pocType="ORCON">
  <Surname>Smith</Surname>
  <GivenName>John</GivenName>
  <PhoneNumber>888-555-5555</PhoneNumber>
  <Affiliation>AgencyX</Affiliation>
  <EmailAddress>jsmith@agencyx.gov</EmailAddress>
</AuthorInfo>
```

2.2.2.3 - pre13526ORCON

The ORCON Memo signed March 11, 2011 provides guidance on the dissemination of ORCON data. According to this memo, ORCON documents created prior to June 28, 2010 should be handled according to E.O. 12958, and documents created after this date should be handled according to E.O. 13526. However, derived products that include ORCON data produced prior to June 28, 2010 must include a statement that it should be handled according to the previous E.O. 12958; this statement is marked with the **@noticeType** attribute value [pre13526ORCON]. The attribute indicates that the document contains ORCON information that predates E.O. 13526, 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. With questions, contact John Smith, AgencyX,
    888-555-5555, jsmith@agencyx.gov.
  </NoticeText>
</Notice>
```

Chapter 3 - Data Validation Constraint Rules

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

3.1 - Basics

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.

This Data Encoding Specification pertains to the technical implementation of a data model for sharing security markings data from collaborative systems.

3.1.1 - Schematron

Schematron was selected as the language in which to encode these additional rules. The provided Schematron is used to define the constraint rules; it is NOT a required implementation. 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*® or the XSLT2 implementation of ISO Schematron provided by Rick Jelliffe at <http://schematron.com/>. Constraint rules are dependent on XPath 2.0 and XSLT 2.0 features. According to Mr. Jelliffe, the editor of Schematron for ISO:

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

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

3.1.2 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as

defined by ICD 710 implemented in the Register and Implementation Manual, ISOO Directive 1, Executive Order (E.O.) 13526, and E.O. 12829, as amended. These rules will be expanded and modified as the model matures, the CAPCO Register is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

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

3.1.3 - Classified or Controlled Constraint Rules

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

3.1.4 - 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.

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

3.1.6 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an "Error" or a "Warning." An "Error" is naturally more severe and is indicative of a clear violation of an ISM.XML constraint rule, which would be likely to have a significant impact on the quality of a document. A "Warning" is less severe although noteworthy, and may not necessarily have any impact on

the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

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

3.2 - 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. If an element, defined in this Specification, used in an XML instance is required (or conditional in certain cases), and that element may possibly contain only text content, then the element must have content in order to be Constraint Rules Valid.

3.3 - 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.

3.4 - Additional Constraints

This section provides additional constraints.

3.4.1 - DES Constraints

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

3.5 - 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.

3.6 - Obsolete rule numbers

The following table contains the information for the ISM.XML rules that have been removed or replaced by other rules.

Table 4 - Obsolete Rules

Rule Number	Removed/ Replaced	Version
ISM-ID-00050	Removed	V2
ISM-ID-00051	Removed	V2
ISM-ID-00052	Removed	V2
ISM-ID-00053	Removed	V2
ISM-ID-00054	Removed	V2
ISM-ID-00055	Removed	V2
ISM-ID-00101	Removed	V2
ISM-ID-00022	Removed	V3
ISM-ID-00076	Removed	V3
ISM-ID-00023	Removed	V4
ISM-ID-00089	Removed	V4
ISM-ID-00120	Removed	V4
ISM-ID-00144	Removed	V4
ISM-ID-00003	Removed	V5
ISM-ID-00004	Removed	V5
ISM-ID-00007	Removed	V5
ISM-ID-00009	Removed	V5
ISM-ID-00010	Removed	V5
ISM-ID-00011	Removed	V5
ISM-ID-00024	Removed	V5
ISM-ID-00025	Removed	V5
ISM-ID-00027	Removed	V5
ISM-ID-00029	Removed	V5
ISM-ID-00039	Removed	V5
ISM-ID-00069	Removed	V5
ISM-ID-00091	Removed	V5
ISM-ID-00092	Removed	V5

Rule Number	Removed/ Replaced	Version
ISM-ID-00093	Removed	V5
ISM-ID-00106	Removed	V5
ISM-ID-00114	Removed	V5
ISM-ID-00115	Removed	V5
ISM-ID-00117	Removed	V5
ISM-ID-00131	Removed	V5
ISM-ID-00172	Removed	V6
ISM-ID-00212	Removed	V6
ISM-ID-00216	Removed	V6
ISM-ID-00218	Removed	V6

Chapter 4 - Data Rendering Constraint Rules

The constraint rules in this chapter define constraints on the rendering 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.

4.1 - Basics

4.1.1 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710 implemented in the Register and Implementation Manual, ISOO Directive 1, Executive Order (E.O.) 13526, and E.O. 12829, as amended. These rules will be expanded and modified as the model matures, the CAPCO Register is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

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

4.1.2 - Classified or Controlled Constraint Rules

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

4.1.3 - 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 rendering constrain rule IDs are prefixed with "ISM-RENDER-"

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

4.1.4 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an "Error" or a "Warning" and is indicated in brackets preceding each constraint rule description. 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 system. A "Warning" is less severe although noteworthy, and may not necessarily have any impact on the quality of a system.

Each system responsible for rendering documents must be evaluated based on its use. Those evaluating the system must make a mission-appropriate decision about the system's suitability for use.

4.2 - Constraint Rules

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

Table 5 - Constraint Rules

Rule Number	Severity	Description	Human Readable Description

4.3 - Obsolete Constraint Rules

The following table contains the information for the ISM.XML data rendering rules that have been removed or replaced by other rules.

Table 6 - Obsolete Rules

Rule Number	Removed/ Replaced	Version

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®*, produced by SyncRO Soft.

The guide provides an interactive index to:

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

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of 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 Change History

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

Table 7 - DES Version Identifier History

Version	Date	Purpose
1.0	August 2008	Initial Release
2	24 December 2009	Routine revision to technical specification. For details of changes, see Section A.6 - V2 Change Summary
3	4 June 2010	Routine revision to technical specification. For details of changes, see Section A.5 - V3 Change Summary
4	7 September 2010	Routine revision to technical specification. For details of changes, see Section A.4 - V4 Change Summary
5	6 December 2010	Routine revision to technical specification. For details of changes, see Section A.3 - V5 Change Summary
6	11 April 2011	Routine revision to technical specification. For details of changes, see Section A.2 - V6 Change Summary
7	9 August 2011	Routine revision to technical specification. For details of changes, see Section A.1 - V7 Change Summary

A.1 - V7 Change Summary

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

Table 8 - 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 Notice , NoticeText and NoticeList to represent valid ISM notices, as well as the attribute @unregisteredNoticeType to represent other notices.	Schema CVCEnumISMElements Added CVCEnumISMAttributes Changed ISM-ID-00223 Added ISM-ID-00226 Added	Data generation and ingestion systems need to be updated to use the new values.
Added ISMNoticeAttributeGroup to ResourceNodeAttributeGroup	Schema	Schema developers need to update to use the corrected

Change	Artifacts changed	Compatibility Notes
and ResourceNodeOptional-AttributeGroup		attribute group. Instance documents are not impacted.
Added new @pocType attribute and POCAttributeGroup to support indicators for a security-related point-of-contact, including ORCON, ICD-710 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 @ism:unregisteredNoticeType 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.
Removed @ism:ACCM and moved its values to @ism:nonICmarkings .	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 @notice to @noticeType and replaced @noticePOC with @pocType="DoD-Dist" .	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 @declassException .	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.

Change	Artifacts changed	Compatibility Notes
Added @ism:declassException="50X1-HUM" and @ism:declassException="50X2-WMD" 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 @ism:noticeType and @ism:unregisteredNoticeType 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 @ism:noticeType 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.
As tetragraphs [MIFH], [EUDA] and [EFOR] were removed from the CAPCO register, their deprecation dates were added to the CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and Ingestion systems need to be updated to remove these tokens before their deprecation dates.
Removed deprecation dates for @declassException tokens [25X1-human], and [AEA].	CVEnumISM25X1	Should not affect data.
Added country code for South Sudan to the ISO-3166 CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and Ingestion systems need to be updated to properly use the new values.

A.2 - V6 Change Summary

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

Table 9 - 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.
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.
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	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-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	
	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	

Change	Artifacts changed	Compatibility Notes
	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	
	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	

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

Change	Artifacts changed	Compatibility Notes
Added support for SSI	CVEs	Data generation and Ingestion systems need to be updated to properly use the new value.

A.3 - V5 Change Summary

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

Table 10 - 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 @typeOfExemptedSource and @dateOfExemptedSource since ISOO no longer supports that concept.	Documentation Schema ISM-ID-00014 Change ISM-ID-00016 Change ISM-ID-00018 Remove ISM-ID-00019 Remove ISM-ID-00020 Remove ISM-ID-00021 Remove	Data generation and Ingestion systems need to be updated to not use these values anymore and to properly enforce the new constraint rules.
Remove Appendix H Reading the Schematics	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.
ISM-ID-00037 and ISM-ID-00083 contradict each other when classified material is involved.	ISM-ID-00037 Change	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rules.

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

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

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

A.4 - V4 Change Summary

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

Table 11 - 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	Data generation and Ingestion systems need to be updated

Change	Artifacts changed	Compatibility Notes
	Controlled Value Enumerations ISM-ID-00163	to use the new structures and to properly enforce the new constraint rules
Use Schema to enforce DES version number	Schema ISM-ID-00102	Forces DES to match version shipped.
Enforce ICD 710 immediately	ISM-ID-00088 ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data Ingestion systems need to be updated to properly enforce the new constraint rules. Data generation systems compliant with ICD 710 need make no changes. Existing data may not be valid anymore.
Remove Duplicate or redundant rules.	ISM-ID-00144 ISM-ID-00023	Data validation systems may remove duplicate code.

A.5 - V3 Change Summary

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

Table 12 - Data Encoding Specification V3 Change Summary

Change	Artifacts changed	Compatibility Notes
Allow use of KDK	Controlled Value Enumerations Constraint Rules ISM-ID-00122 ISM-ID-00123	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules.
Require appropriate foreign disclosure or release marking on classified national intelligence per ICD 710.	Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
Update references to E.O. 12958 to refer to NSI-EO	Documentation Constraint Rules	Should not impact data. Will impact constraint checking

Change	Artifacts changed	Compatibility Notes
	ISM-ID-00013 ISM-ID-00014 ISM-ID-00017 ISM-ID-00018 ISM-ID-00019 ISM-ID-00020 ISM-ID-00021 ISM-ID-00023	systems since it changes the name of a condition.
Force ordering of SAR	Constraint Rules ISM-ID-00121	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
Update rules to exclude the resource element from being considered in rollup constraints.	Constraint Rules ISM-CONTRIBUTES	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

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 and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
Update ISM-ID-00040 to allow for R portions in a USA document	ISM-ID-00040	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release
Update ISM-ID-00028 to allow use of NF with any classification type (i.e., US, non-US, and JOINT).	ISM-ID-00028	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release
Update rules to prevent RELIDO on portions that do not have USA as one of the ownerProducers.	ISM-ID-00124	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

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

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

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 and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to no longer generate some errors as per the new rules. Note: Data could have been created that was <i>invalid</i> under previous releases that may be valid under this release
Add rule for FOUO compilation reason	ISM-ID-00154	Data generation systems that correctly implement CAPCO guidance and follow E.O. 13526 should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

A.6 - V2 Change Summary

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

Table 13 - 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

Change	Artifacts changed	Compatibility Notes
		systems need to be updated to properly handle the new data. Schemas and/or DESs using ISM.XML need to implement the attribute appropriately.
Added @compilationReason to indicate compilation and provide a reason that the element has an aggregate classification higher than its parts or a control marking has been applied that is not in the individual parts.	Schema	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
Expanded constraint rules to identify previously unrecognized data errors in accordance with the IC Classification and Control Markings system	Constraint Rules	Data generation systems that correctly implement CAPCO guidance and follow E.O. 12958, as amended should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
Changed ISM vocab warnings to errors, based on identification of specific CVE.	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance and follow E.O. 12958, as amended should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.
Updated constraint rules and schema documentation to specify data values for: @ownerProducer , @SCIcontrols , @SARIdentifier , @disseminationControls , @FGIsourceOpen , @FGIsourceProtected , @releasableTo , @nonICmarkings , @declassException , @typeOfExemptedSource .	Constraint Rules Controlled Value Enumerations	Data generation systems that correctly implement CAPCO guidance and follow E.O. 12958, as amended should not be impacted. Ingestion systems need to be updated to generate errors as per the new rules. Note: Data could have been created that was valid under previous releases that may not be valid under this release.

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

Appendix B Acronyms

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

Table 14 - Acronyms

Name	Definition
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DNI	Director National Intelligence
E.O.	Executive Order
GNS	Geographic Names Server
HTML	HyperText Markup Language
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICS	Intelligence Community Standard
ISBN	International Standard Book Number
ISM	Information Security Marking Metadata
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Internet Media Types
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NSI	National Security Intelligence
ODNI	Office of the Director of National Intelligence
SSC	Special Security Center
TGN	Thesaurus of Geographic Names
URI	Uniform Resource Identifier

Name	Definition
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

Appendix C Bibliography

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

(CAPCO Implementation Guide)

Community Classification and Control Markings Implementation Manual. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Implementation%20Manual%20v4%202_MAY_31_2011_FOUO_datefixed.pdf.

(CAPCO Register)

Authorized Classification and Control Markings Register. Unclassified FOUO version. Volume 4, Edition 2 (Version 4.2). 31 May 2011. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register_FOUO_v4.2_MAY31_2011.pdf.

(DC MES)

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

(E.O. 12958, as amended)

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

(E.O. 12829, as amended)

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

(E.O. 13526)

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

(ICD 206)

Sourcing Requirements for Disseminated Intelligence Products. Intelligence Community Directive Number 206. 17 October 2007. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_206.pdf.

(ICD 500)

Intelligence Community Directive Number 500. Director of National Intelligence Chief Information Officer. 7 August 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 501)

Intelligence Community Directive Number 501. Director of National Intelligence Chief Information Officer. 21 January 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_501.pdf.

Classification and Control Markings System. Intelligence Community Directive Number 710. 11 September 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_710.pdf.

(ICD 500-27)

Intelligence Community Standard for Collection and Sharing of Audit Data for IC Information Resources by IC Elements Number 500-27. DRAFT. Office of the Director of National Intelligence.

(ISO 639-2)

Codes for the representation of names of languages – Part 2: Alpha-3 code ISO 639-2:1998. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4767.

(ISO 3166-1)

Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. ISO 3166-1:2006. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719.

(ISO 8601)

Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874.

(ISO 15836)

Information and documentation – The Dublin Core metadata element set. ISO 15836:2009. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142.

(ISO 19757-3:2006)

Information technology - Document Schema Definition Language (DSDL) - Part 3: Rule-based validation - Schematron. 19757-3:2006 International Organization for Standardization (ISO). <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

(ISOO Directive 1)

Classified National Security Information (Directive No. 1); Final Rule. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 68, No. 183. 22 September 2003. Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). <http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.pdf>.

(RFC 3066)

Tags for the Identification of Languages. January 2001. H. Alvestrand. Cisco Systems. <http://www.rfc-editor.org/rfc/rfc3066.txt>.

Marking Classified National Security Information. Information Security Oversight Office. December 2010. <http://www.archives.gov/isoo/training/marketing-booklet.pdf>

<http://www.schematron.com/>.

Appendix D 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.

Appendix E 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.