Intelligence Community Technical Specification

XML Data Encoding Specification for Information Security Markings

Version 9

17 July 2012

Table of Contents

List of Tables

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* [8] 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,[11] 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,[7] ICD 710 Classification and Control Marking System,[9] and implemented by the CAPCO Register and Manual,[1] 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 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,[10] 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.[12] 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[21] 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[12] 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 and Manual (5.1)[1]
DoD Directive 5200.1 February 2012[2]
ISO Schematron[21] 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

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.[9]
- **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, 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 and Manual[1], 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[1] 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 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 29, 2011[19] 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, as amended,[6] and documents created after this date should be handled according to E.O. 13526.[7] 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, as amended;[6] this statement is marked with the **@noticeType** attribute value [pre13526ORCON]. The attribute indicates that the document contains ORCON information that predates E.O. 13526,[7] 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 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[21] was selected as the language in which to encode these additional rules. The provided Schematron[21] 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*® [20] or the XSLT 2.0[24] implementation of ISO Schematron[21] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[23] and XSLT 2.0[24] features. According to Mr. Jelliffe, the editor of Schematron[21] 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[21] implementation and XSLT 2.0[24] 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[9] implemented in the CAPCO Register and Manual,[1] ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010),[14] E.O. 13526,[7] and E.O. 12829, as amended.[5] These rules will be expanded and modified as the model matures, the CAPCO Register and Manual[1] 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. [1] Elements, which are allowed to only have text content, must have text content specified.

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

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. Obsolete rule numbers are listed in the SchematronGuide.

[1] "white space" is defined in XML 1.0[22] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

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[9] implemented in the CAPCO Register and Manual,[1] ISOO 32 CFR Parts 2001 and 2004 (as of September 22, 2003),[15] E.O. 13526,[7] and E.O. 12829, as amended.[5] These rules will be expanded and modified as the model matures, the CAPCO Register and Manual[1] 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 and10001 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 2 - Constraint Rules

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

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*® [20], 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 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[1] 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)
Cell Colors represent the same information as the Key value	

A.1. ISM Feature Summary

Table 4 - ISM Feature comparison

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

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
ICD 710[9] September 11, 2009	710 Foreign Release	P	P	F	F	F	F	F	F	F
E.O. 13526[7] December 29, 2009	DeclassReasons/Dates	P	P	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
DoD Directive 5230.24[3] March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F	F
DoD Directive 5240.01[4] August 27, 2007	US Person Notice	P	P	P	P	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
ISOO Marking Booklet 2010[16] / ISOO Notice 2009-13[17] December 2010	Remove exempted source	P	P	P	P	F	F	F	F	F
E.O. 13526[7] December 29, 2009	derivativelyClassifiedBy	P	P	P	P	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
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
IC-CIO enhance data quality See IC ESB	Schematron[21] Implementation of rules	N	N	N	N	F	F	F	F	F
E.O. 13526[7] December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
DoD Directive 5200.1-R[2] January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F	F
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[14] June 28, 2010	TFNI	N	N	N	N	N	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F	N
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	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
ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[14] June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F	F
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F	F
ICD 710[9] September 11, 2009	710 POC	N	N	N	N	N	N	F	F	F
DNI ORCON Memo [19] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F
ISOO Marking Booklet[16] December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/event	N	N	N	N	N	N	F	F	F
IC-CIO enhance data quality See IC ESB	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	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
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
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
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	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
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of KDK SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 December 30, 2011	Allow use of SI SubCompartments and Sub-SubCompartments	N	N	N	N	N	N	N	N	F
CAPCO Register and Manual 5.1 Annex A	Allow use of OSTY Open Skies	N	N	N	N	N	N	N	N	F
IC-CIO enhance data quality	External Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[2] February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[2] February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F

Appendix B Change History

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

Table 5 - 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 B.8 - V2 Change Summary
3	4 June 2010	Routine revision to technical specification. For details of changes, see Section B.7 - V3 Change Summary
4	7 September 2010	Routine revision to technical specification. For details of changes, see Section B.6 - V4 Change Summary
5	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.5 - V5 Change Summary
6	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.4 - V6 Change Summary
7	9 August 2011	Routine revision to technical specification. For details of changes, see Section B.3 - V7 Change Summary
8	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.2 - V8 Change Summary
9	17 July 2012	Routine revision to technical specification. For details of changes, see Section B.1 - V9 Change Summary

B.1 - 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 6 - Data Encoding Specification V9 Change Summary

Change	Artifacts changed	Compatibility Notes
Added support for alphanumeric **@DESVersion** 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.

Change	Artifacts changed	Compatibility Notes
Changed declaration of NoticeText from complexContent to simpleContent [artf12153].	Schema	Should only impact some code generation systems.
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.

Change	Artifacts changed	Compatibility Notes
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.sch updated ISM_ID_00128.sch updated ISM_ID_00129.sch updated ISM_ID_00130.sch updated ISM_ID_00134.sch updated ISM_ID_00135.sch updated ISM_ID_00136.sch updated ISM_ID_00137.sch updated ISM_ID_00138.sch updated ISM_ID_00139.sch updated ISM_ID_00150.sch updated ISM_ID_00151.sch updated ISM_ID_00152.sch updated ISM_ID_00153.sch updated ISM_ID_00158.sch updated	Data generation and Ingestion systems need to be updated to properly use the new values.

Change	Artifacts changed	Compatibility Notes
	ISM_ID_00159.sch updated ISM_ID_00161.sch updated ISM_ID_00244.sch updated ISM_ID_00245.sch updated ISM_ID_00248.sch added	
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.
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.

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

Significant drivers for Version 8 include:

- CAPCO Register and Manual 5.1
- ISOO Guidance (ISOO Notice 2012-02)[18]
- ISO 3166-1[13]

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

Table 7 - Data Encoding Specification V8 Change Summary

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

Change	Artifacts changed	Compatibility Notes
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.sch ISM_ID_00017.sch ISM_ID_00133.sch ISM_ID_00013.sch ISM_ID_00014.sch ISM_ID_00141.sch	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[9] foreign release indicator on them. [artf11427].	ISM_XML.sch ISM_ID_00119.sch	Data generation and ingestion systems need to be updated to handle these data changes.
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.

Change	Artifacts changed	Compatibility Notes
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.
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.

Change	Artifacts changed	Compatibility Notes
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.3 - 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)[14]
- ISO 3166-1[13]
- DNI ORCON Memo[19]
- ICD 710[9]

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 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.

Change	Artifacts changed	Compatibility Notes
Added **ISMNoticeAttributeGroup** to **ResourceNodeAttributeGroup** and **ResourceNodeOptional-AttributeGroup**.	Schema	Schema developers need to update to use the corrected 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[9] 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.

Change	Artifacts changed	Compatibility Notes
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.
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 and Manual[1], 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.

Change	Artifacts changed	Compatibility Notes
Added country code for South Sudan to the ISO 3166-1[13] CVEs.	CVEnumISMFGIOpen Changed CVEnum-ISMFGIProtected Changed CVEnum-ISMOwnerProducer Changed CVEnumISMRelTo Changed	Data generation and Ingestion systems need to be updated to properly use the new values.

B.4 - V6 Change Summary

Significant drivers for Version 6 include:

- CAPCO Register and Manual 4.1 (HCS Sub Cats missed in V5)
- Executive Order 13526[7] (TFNI)
- ISOO 32 CFR Parts 2001 and 2003 (as of June 28, 2010)[14]

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.

Change	Artifacts changed	Compatibility Notes
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 FGIsourceProtected 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 FGIsourceOpen 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 FGIsourceProtected then both are [FGI].	ISM-ID-00218 Added ISM-ID-00219 Added	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rules.

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

B.4.1 - V6 Change Errata

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

Table 10 - 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.5 - 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 11 - 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 – FGIsourceOpen deprecation warning ISM-ID-00189 – FGIsourceOpen deprecation error ISM-ID-00190 – FGIsourceProtected deprecation warning ISM-ID-00191 – FGIsourceProtected deprecation error ISM-ID-00192 – nonICmarkings deprecation warning ISM-ID-00193 – nonICmarkings deprecation error ISM-ID-00194 – notice deprecation warning ISM-ID-00195 – notice deprecation error ISM-ID-00196 – ownerProducer deprecation warning	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rules.

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

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

B.5.1 - V5 Change Errata

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

Table 12 - 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.6 - V4 Change Summary

Significant drivers for Version 4 include:

- DoD Directive 5230.24[3]
- ICD 710[9] (enforce immediately no grace)

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

Table 13 - 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[9] 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[9] 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.7 - V3 Change Summary

Significant drivers for Version 3 include:

- Executive Order 13526[7] (enforce requirements for Authority block)
- CAPCO Register and Manual 3.1
- ICD 710[9]

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

Table 14 - 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[1] and follow E.O. 13526[7] 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.[9]	Constraint Rules ISM-ID-00119 ISM-ID-00120 ISM-ID-00089	Data generation systems that correctly implement CAPCO guidance[1] and follow E.O. 13526[7] 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[6] 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[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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 *invalid* 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[1] and follow E.O. 13526[7] 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 *invalid* 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[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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[7] requirements for Authority block.	ISM-ID-00141 ISM-ID-00017 ISM-ID-00142 ISM-ID-00143	Data generation systems that correctly implement CAPCO guidance[1] and follow E.O. 13526[7] 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[1] and follow E.O. 13526[7] 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 *invalid* 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[1] and follow E.O. 13526[7] 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.8 - V2 Change Summary

Significant drivers for Version 2 include:

- Executive Order 12958, as amended [6](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])[15]

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

Table 15 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated ISM XSL rendering stylesheet to include new CAPCO changes such as removal of declass dates from banner.	Stylesheet	Data rendered using provided stylesheets will render differently
Removed version number from file names.	Schema	Systems need to be updated to use the new file names.
Added ability for instance documents to specify DES versions used.	Constraint Rules Schema	Data generation systems need to be updated to include DES version(s) in output. Ingestion systems need to be updated to properly handle the new data. Schemas and/or DESs using ISM.XML need to implement the attribute appropriately.
Added **@compilationReason** to indicate compilation and provide a reason that the element has an aggregate classification higher than its parts or a control marking has been applied that is not in the individual parts.	Schema	Data generation systems should be updated to use the attribute if they need the feature. Ingestion systems need to use the new specification, including schema.
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[1] and follow E.O. 12958, as amended[6] 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[1] and follow E.O. 12958, as amended[6] 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[1] and follow E.O. 12958, as amended[6] 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 **@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.

Change	Artifacts changed	Compatibility Notes
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 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 16 - Acronyms

Name	Definition
ATO	Authority To Operate
BNF	Backus-Naur Form
CAPCO	Controlled Access Program Coordination Office
CVE	Controlled Vocabulary Enumeration
DAA	Designated Approval Agent
DCMI	Dublin Core Metadata Initiative
DC MES	Dublin Core Metadata Element Set
DES	Data Encoding Specification
DOI	Digital Object Identifier
DN	Distinguished Name
DNI	Director of National Intelligence
E.O.	Executive Order
ES&IS	Enterprise Search & Integration Services
GNS	Geographic Names Server
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 ESB	Intelligence Community Enterprise Standards Baseline
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISBN	International Standard Book Number
ISM	Information Security Marking
ISO	International Organization for Standardization

Name	Definition
ISOO	Information Security Oversight Office
KA	Knowledge Assertion
KOS	Knowledge Organization System
MIME	Multipurpose Internet Mail Extensions
NARA	National Archives and Records Administration
NGA	National Geospatial Intelligence Agency
NGT	Next Generation Trident
NSI	National Security Information
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PK	Private Key
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
SSD	Special Security Directorate
SSL	Secure Socket Layer
SOAP	Simple Object Access Protocol
TGN	Thesaurus of Geographic Names
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3CDTF	World Wide Web Consortium Date Time Format
XML	Extensible Markup Language

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 5. Edition 1 (Version 5.1). Effective: 30 December 2011.
Available online at: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register%20and%20Manual%20v5.1_04Jan11_FOUO.pdf

[2] DoD Directive 5200.1

Under Secretary of Defence for Intelligence. *DoD Information Security Program:*. 5200.1. February 24, 2012.
Vol 1 Available online at: 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
Vol 3 Available online at: 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

[3] DoD Directive 5230.24

Secretary of Defense. *Distribution Statements on Technical Documents*. 5230.24. 18 March 1987.
Available online at: http://www.dtic.mil/dtic/pdf/submit/523024p.pdf

[4] DoD Directive 5240.01

Secretary of Defense. *DoD Intelligence Activities*. 5240.01. August 2007.
Available online at: http://www.dtic.mil/dtic/pdf/submit/5240.01.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] 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/electronic_reading_room/ICD_500.pdf

[9] 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/electronic_reading_room/ICD_710.pdf

[10] 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 at: https://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[11] 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 at: https://www.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS-500-21.aspx

[12] 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

[13] 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

[14] 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

[15] 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

[16] ISOO Marking Booklet

Information Security Oversight Office. *Marking Classified National Security Information*. December 2010.
Available online at: http://www.archives.gov/isoo/training/marking-booklet.pdf

[17] 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

[18] 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

[19] 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.
Available online at: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20A.doc.pdf
Attachment B: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20B.pdf
Attachment C: https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/DNI%20ORCON%20Memo%20Attach%20C.pdf

[20] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 13.2.
Available online at: http://www.oxygenxml.com/

[21] 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/

[22] 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/

[23] 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/

[24] 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.

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.[10]