Intelligence Community Technical Specification

XML Data Encoding Specification for Information Resource Metadata

Version 7

27 February 2012

Table of Contents

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification* for Information Resource Metadata (IRM.XML) defines detailed specifications for using Extensible Markup Language (XML) to encode Information Resource Metadata (IRM) 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 information resource concepts using XML.

This DES uses the Department of Defense Discovery Metadata Specification (DDMS) as a base and builds on that base by specifying additional metadata needed to describe information resources in the Intelligence Community. In some cases, this DES specifies additional constraints on the data.

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 resource metadata to allow users and systems to find and access a wide-range of information resources throughout the enterprise. Information resource visibility, accessibility, and understandability are all critical to providing these capabilities. A successful information sharing enterprise depends on the ability of users and systems to locate and access information resources through a consistent and flexible search, or discovery capability. An enterprise-wide discovery capability will be greatly enhanced by the consistent "digital" description of all information resources. A common specification for the description of information resources allows for a comprehensive capability that can locate all resources across the enterprise regardless of format, type, location, or classification.

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 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 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
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V7)
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V5)
Department of Defense Discovery Metadata Specification (DDMS 4.0.1)

Name
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.

Note: **ddms:resource** nodes pertain to the described resource (e.g. **irm:ICResourceMetadataPackage/ddms:resource/ddms:creator** is the creator of the document). The XPaths listed under **ddms:resource** nodes are relative to **irm:ICResourceMetadataPackage/ddms:resource**. The **ddms:resource/ ddms:metacardInfo** nodes pertain to the metacard, rather than the described resource (e.g. **irm:ICResourceMetadataPackage/ddms:resource/ddms:metacardInfo/ddms:creator** refers to the creator of the metacard, not necessarily the creator of the document). The XPaths listed under **ddms:metacardInfo nodes** are relative to **irm:ICResourceMetadataPackage/ ddms:resource/ddms:metacardInfo**. See Section 2.2.1 - ddms:resource and ddms:metacardInfo for a further discussion of these concepts.

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
Contributor	An entity responsible for making contributions to the resource. Examples of Contributor include a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the entity.	ddms:resource nodes **./ddms:contributor** **./ddms:pointOfContact** ddms:metacardInfo nodes **./ddms:contributor** **./ddms:pointOfContact**
Coverage	The spatial, temporal [or virtual] topic of the resource, the spatial [or virtual] applicability of the resource, or the jurisdiction under which the resource is relevant. Spatial topic may be a named place or a location specified by its geographic coordinates. Temporal period may be a named period, date, or date range. Virtual topic may be a named place or a location specified using a network or email address. A jurisdiction may be a named administrative entity or a geographic place to which the resource applies. Recommended best practice is to use a controlled vocabulary such as the Thesaurus of Geographic Names (TGN) or the NGA Geographic Names Server (GNS) as sanctioned by the United States Board on Geographic Names. Where appropriate, named places or time periods can be used in preference to numeric identifiers such as sets of coordinates or date ranges.	ddms:resource nodes **./ddms:geospatialCoverage** **./ddms:temporalCoverage** **./ddms:virtualCoverage** **./ddms:subjectCoverage** ddms:metacardInfo nodes Not applicable

Abstract Data Element	Definition	XPath and XML implementation notes
Creator	An entity primarily responsible for making the resource. Examples of Creator include a person, an organization, or a service. Typically, the name of a creator should be used to indicate the entity.	ddms:resource nodes **./ddms:creator** ddms:metacardInfo nodes **./ddms:creator**
Date	A point or period of time associated with an event in the lifecycle of the resource. Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the W3CDTF profile of ISO 8601. Typically, date will be associated with the creation or availability of the resource.	ddms:resource nodes **./ddms:dates/@ddms:created** **./ddms:dates/@ddms:infoCutOff** **./ddms:dates/@ddms:posted** **./ddms:dates/@ddms:validTil** **./ddms:dates/@ddms:approvedOn** **./ddms:dates/@ddms:receivedOn** ddms:metacardInfo nodes **./ddms:dates/@ddms:created** **./ddms:dates/@ddms:infoCutOff** **./ddms:dates/@ddms:posted** **./ddms:dates/@ddms:validTil** **./ddms:dates/@ddms:approvedOn** **./ddms:dates/@ddms:receivedOn** **./ddms:processingInfo/ @irm:dateProcessed**

Abstract Data Element	Definition	XPath and XML implementation notes
Description	An account of the resource. Description may include but is not limited to: an abstract, a table of contents, a graphical representation, or a free-text account of the resource.	ddms:resource nodes **./ddms:description** **./ddms:resourceManagement/ ddms:taskingInfo** **./ddms:type[@ddms:qualifier= "urn:us:gov:ic:cvenum:irm: activity:v1"]/@ddms:value** **./ddms:security/ddms:noticeList** **./ddms:subjectCoverage/ ddms:productionMetric** ddms:metacardInfo nodes **./ddms:description** **./ddms:processingInfo**
Format	The file format, physical medium, or dimensions of the resource. Examples of dimensions include size and duration. Recommended best practice is to use a controlled vocabulary such as the list of Internet Media Types (MIME). Format may be used to identify the software, hardware, or other equipment needed to display or operate the resource.	ddms:resource nodes **./ddms:format** **./ddms:resourceManagement/ ddms:recordsManagementInfo/ ddms:applicationSoftware** ddms:metacardInfo nodes **./ddms:recordsManagementInfo/ ddms:applicationSoftware**
Identifier	An unambiguous reference to the resource within a given context. Recommended best practice is to identify the resource by means of a string conforming to a formal identification system. Formal identification systems include but are not limited to the Uniform Resource Identifier (URI) (including the Uniform Resource Locator (URL)), the Digital Object Identifier (DOI), and the International Standard Book Number (ISBN).	ddms:resource nodes **./ddms:identifier** ddms:metacardInfo nodes **./ddms:identifier**

Abstract Data Element	Definition	XPath and XML implementation notes
Language	A language of the resource. Recommended best practice is to use a controlled vocabulary such as RFC 3066, Tags for the Identification of Languages, which specifies use of ISO 639-2, Codes for the Representation of Names of Languages, three character language code, with an optional appended ISO 3166-1, Codes for the representation of names of countries and their subdivisions, two character country code. For example: "eng-US" or "eng-UK."	ddms:resource nodes **./ddms:language** ddms:metacardInfo nodes Not applicable
Publisher	An entity responsible for making the resource available. Examples of a Publisher include a person, an organization, or a service. Typically, the name of a Publisher should be used to indicate the entity.	ddms:resource nodes **./ddms:publisher** ddms:metacardInfo nodes **./ddms:publisher**
Relation	A related resource. Recommended best practice is to identify the referenced resource by means of a label or number conforming to a formal identification system.	ddms:resource nodes **./ddms:relatedResource** ddms:metacardInfo nodes Not Applicable
Rights	Information about rights held in and over the resource. Typically, rights will contain a rights management statement for the resource, or reference a service providing such information. Rights information often encompasses Intellectual Property Rights (IPR), Copyright, and various Property Rights. If the rights element is absent, no assumptions may be made about any rights held in or over the resource.	ddms:resource nodes **./ddms:rights** ddms:metacardInfo nodes Not Applicable

Abstract Data Element	Definition	XPath and XML implementation notes
Resource Security Mark	The overall security classification and security handling instructions carried by the resource. Resource Security Mark applies to the resource-level classification, SCI controls, dissemination controls, non-IC markings, and other security provisions prescribed by Executive Order 13526, as amended, the Information Security Oversight Office (ISOO) Directive 1 of the National Archives and Records Administration, and the Intelligence Community marking standard maintained by the Controlled Access Program Coordination Office (CAPCO). These values are prominently presented, in the case of intelligence publications, at the top and bottom of every page and in other specified locations. See the Intelligence Community Standard for Information Security Marking Metadata for refinements of this conceptual element.	**irm:ICResourceMetadataPackage/ @ism:*** ddms:resource nodes **./ddms:security** ddms:metacardInfo nodes **./ddms:noticeList**
Source	The resource from which the described resource is derived. The described resource may be derived from the related resource in whole or in part. Recommended best practice is to identify the related resource by means of a string conforming to a formal identification system.	ddms:resource nodes **./ddms:source** ddms:metacardInfo nodes Not applicable

Abstract Data Element	Definition	XPath and XML implementation notes
Subject	A topic of the resource. Typically, the topic will be represented using keywords, key phrases, or classification codes. Recommended best practice is to use a controlled vocabulary. To describe the spatial, temporal or virtual topic of the resource, use the Coverage element.	ddms:resource nodes **./ddms:subjectCoverage/ ddms:category** **./ddms:subjectCoverage/ ddms:keyword** **./ddms:subjectCoverage/ ddms:productionMetric** **./ddms:subjectCoverage/ ddms:nonStateActor** ddms:metacardInfo nodes Not applicable
Title	A name given to the resource. Typically, a Title will be a name by which the resource is formally known.	ddms:resource nodes **./ddms:title** **./ddms:subtitle** ddms:metacardInfo nodes Not applicable

Abstract Data Element	Definition	XPath and XML implementation notes
Type	The nature or genre of the content of the resource. The Type includes terms describing general categories, functions, genres, or aggregation levels for content. Examples of Types include publication forms (e.g., reports or articles) and intelligence disciplines (e.g., SIGINT, MASINT, HUMINT). Recommended best practice is to use a controlled vocabulary. To describe the file format, physical medium, or dimensions of the resource, use the Format element.	ddms:resource nodes **./ddms:type** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: disciplines:v1']/@ddms:value** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: disciplines:v1']/@ddms:value (prefixed with 'other:')** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: subdisciplines:v1']/@ddms:value** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: subdisciplines:v1']/@ddms:value (prefixed with 'other:')** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: subdisciplinetechniques:v1']/ @ddms:value** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:cvenum:intel: subdisciplinetechniques:v1']/ @ddms:value (prefixed with 'other:')** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:reportinglevel']/ @ddms:value** **ddms:type[@ddms:qualifier= 'urn:us:gov:ic:productline']/ @ddms:value** ddms:metacardInfo nodes Not applicable

Abstract Data Element	Definition	XPath and XML implementation notes
Records Management Information	Required information primarily supporting federal record keeping requirements.	ddms:resource nodes **./ddms:resourceManagement/ ddms:recordsManagementInfo** **./ddms:resourceManagement/ ddms:revisionRecall** **./ddms:resourceManagement/ ddms:processingInfo** ddms:metacardInfo nodes **./ddms:recordsManagementInfo** **./ddms:revisionRecall**

2.2 - Additional guidance

This section provides additional guidance for encoding data in specific situations. 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 - ddms:resource and ddms:metacardInfo

Although **ddms:resource** and its sub-element **ddms:metacardInfo** share many of the same constructs, each serves a different purpose as the two major components of a single IRM document. From a Library Card analogy, the **ICResourceMetadataPackage** is the entirety of the "Library Card", the **ddms:resource** contains information about the "book" while the **ddms:metacardInfo** contains information about the "Library Card."

There may be instances in which the author of the book documented in **ddms:resource** and the author of the Library Card documented in **ddms:resource/ddms:metacardInfo** are the same. In those cases the metadata may seem redundant. In the case where they are different, it becomes clear that an organization may create a book documented in **ddms:resource** while an entirely different agency may create the Library Card documented in **ddms:metacardInfo**.

ddms:metacardInfo has a **ddms:identifier**, which can be easily confused with the **ddms:identifier** of the **ddms:resource.** These are similar constructs but serve different purposes. Using the Library Card analogy again, the **ddms:identifier** inside **ddms:resource** identifies the "book" (e.g. an International Standard Book Number (ISBN) number), while the **ddms:identifier** inside **ddms:metacardInfo** identifies the "Library Card" with a unique identifier for the card. Since the **ICResourceMetadataPackage** may be in and of itself a classified document, it needs its own identification for tracking, revision-recall, and auditing purposes.

2.2.2 - DocumentID

For the purposes of the IC there needs to be a single document identifier that all documents will have. This document ID is denoted using the DDMS constructs by having a qualifier of "IC-ID" placed on a **ddms:identifier** element. The document identifier should be unique to this document across the whole of the IC. There is no central registry or managing body for document identifiers across the IC so it is the responsibility of individual producers to coordinate properly.

2.2.3 - ISM Attribute usage

Both IRM and DDMS have adopted the recommended usage of the ISM resource attribute group being used on the root node of their schemas. Because of this decision, both the ISM attributes on the root node of IRM and those on the **ddms:resource** represent the classification attributes for all of their child elements that do not have **@ism:excludeFromRollup**='true'. The only element in IRM that has the **@ism:excludeFromRollup**='true' is the **ddms:security** element in DDMS. This is because the security element represents the classification information about the described item and not the classification of any content in the IRM.

2.2.4 - Specification of ddms:noticeList

The use of **ddms:noticeList** is optional and is provided as a convenient way to specify one or many notices at a single location. There are 2 levels where **ddms:noticeList** is allowed:

- As a child of **ddms:metacardInfo**. For example, a FISA notice in this location is used to indicate that the information in the IRM itself requires a FISA notice.
- As a child of **ddms:security**. For example, a FISA notice in this location is used to indicate that the information about the item being described in the IRM requires a FISA notice, not that the IRM itself requires one.

The element **ddms:noticeList** is comprised of one or more **ism:Notice** elements, which use the **ISMNoticeAttributeGroup** attributes to provide additional information about each notice, such as the type of notice or the reason it was issued. The attribute **@ism:noticeType** is used to indicate a type of ISM-recognized security notice and ISM provides constraint checking for this 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. The attribute **@ism:unregisteredNoticeType** is used to indicate a security-related notice that is not described in the CAPCO Register and/or is not sufficiently defined to be represented in the Controlled Value Enumeration CVEnumISMNotice.xml. For additional information concerning security-related notices, see the document *XML Data Encoding Specification for Information Security Markings*.

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.

See the example file instance1.xml for a sample **ddms:noticeList** and use of **ism:Notice** for security-related notices and non-security-related notices.

2.2.5 - Specification of publishing organization

The element **ddms:publisher** is used to identify the entity(ies) primarily responsible for releasing the information to the enterprise. The entity(ies) of interest in this context are foremost the organization responsible for the actual distribution of the data. The organizations and/or individuals responsible for creating the information are captured within the **ddms:creator** and **ddms:contributor** structures. The publishing organization's approved identifier value is captured in an element called **ddms:publisher/ddms:organization**. Further decomposition of the **ddms:organization** is captured in the **ddms:subOrganization** element. Depending on the enterprise requirement being addressed, a complete understanding of the Publisher requires evaluating the **ddms:organization/@ddms:acronym** and **ddms:subOrganization** value as well as the values found in the **ddms:affiliation** of the **ddms:publisher**, **ddms:creator** and **ddms:contributor** elements.

The **ddms:publisher** structure provides the ability to identify multiple levels of organizational structure and multiple organizations or individuals responsible for creating the information. The most basic ability to identify is captured with the required element **ddms:publisher** using the attribute **ddms:organization/@ddms:acronym**. The controlled vocabulary enumeration (CVE) for **@ddms:acronym** includes values representing the organizations officially designated as part of the IC as defined in the DNI's Overview of the United States Intelligence Community for the 111th Congress of 2009, plus the DNI, plus additional entries intended to recognize non-IC publishers whose information is commonly used in support of the intelligence mission. One of these values must be selected.

In many cases, the AgencyAcronym CVE only includes the highest level of the organization structure (e.g., DNI), service or agency (e.g., US Army, DHS, DoS), or non-IC designation (e.g., OtherDoD, Foreign). In order to identify a Publisher at a level below what the AgencyAcronym CVE allows, use the **ddms:subOrganization** element of the **ddms:publisher/ ddms:organization**.

For consistency, populate **ddms:subOrganization** with an approved organization acronym designator for the sub-organization. For multiple levels of sub-organization, list the acronyms in descending order delimited with the "/" character.

In cases where non-IC information (e.g., OtherDoD, OtherUSG, SLT, Foreign) is shared with the intelligence enterprise, the **ddms:publisher/ddms:organization/@ddms:acronym** should reflect the organization, which last prepared the information for consumption (e.g., converted the content into PUBS.XML, applied enhanced information resource metadata tagging, translated, or packaged the information into an official IC product) and shared the product with the enterprise. As that organization is affecting the record status of the product, it must take responsibility for addressing any questions about the information.

If a non-IC producer is providing information that is already compliant with IC enterprise data encoding standards, then the **ddms:publisher/ddms:organization/@ddms:acronym** should reflect the appropriate non-IC organization designator and the non-IC organizations office in the **ddms:subOrganization** element. Examples of this scenario might exist in a USG department where there are sub-organizations designated in the IC and sub-organizations not in the IC;

DoD where some sub-organizations support DIA, some support a service, and some are not in the IC; State, Local, Tribal organizations with information that flows into the intelligence enterprise via DHS, NCTC, or other means; or with our foreign partners. In the case of foreign partners designations in the **ddms:subOrganization**, precede the office acronym with the country code trigraph in order to ensure uniqueness.

2.2.5.1 - Examples

For NCTC:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="DNI">
      <ddms:name>Director of National Intelligence</ddms:name>
      <ddms:subOrganization>NCTC</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

For the XYZ component of NCTC:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="DNI">
      <ddms:name>Director of National Intelligence</ddms:name>
      <ddms:subOrganization>NCTC/XYZ</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

For the XYZ component of CIA:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="CIA">
      <ddms:name>Central Intelligence Agency</ddms:name>
      <ddms:subOrganization>XYZ</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

For the United States Postal Service:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="OtherUSG">
      <ddms:name>United States Postal Service</ddms:name>
      <ddms:name>USPS</ddms:name>
   </ddms:organization>
</ddms:publisher>
```

For the JIOC at PACOM:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="DIA">
      <ddms:name>Defense Intelligence Agency</ddms:name>
      <ddms:subOrganization>PACOM/JIOC</ddms:subOrganization>
```

```
   </ddms:organization>
</ddms:publisher>
```

For the J4 at PACOM:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="OtherDoD">
      <ddms:name>Defense Intelligence Agency</ddms:name>
      <ddms:subOrganization>PACOM/J4</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

2.2.6 - MIME type

The Multipurpose Internet Mail Extensions (MIME) type for a IRM.XML document is application/dni-irm+xml. This is a convention for our community it has NOT been registered with the Internet Assigned Numbers Authority (IANA). Should there be a conflict in the future it will be addressed at that time. Systems can use this MIME type to facilitate communications and address business needs within the community.

Chapter 3 - Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for IRM.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 IRM.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 IRM.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 information resource metadata 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/ [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. IRM.XML data validation constraint rule IDs are prefixed with “IRM-ID-”.

As the 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 IRM.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 - Inherited Constraints

In an instance of IRM.XML, the use of attributes and elements from supplementary data encoding specifications must be fully conformant with the constraint rules defined in those specifications. For a full list of supplementary specifications, see Table 1 .

3.4 - Value Enumeration Constraints

Several elements and attributes of the IRM.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.

3.5 - Additional Constraints

This section provides additional constraints.

3.5.1 - DES Constraints

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

3.6 - Constraint Rules

The detailed constraint rules for the IRM.XML schema can be found in a separate document inside the SchematronGuide directory, in the IRM_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.

3.7 - Obsolete Rule Numbers

Table 3 - Obsolete Rules

Rule Number	Removed/ Replaced	Version
IRM-ID-00004	Removed	V4
IRM-ID-00026	Removed	V4
IRM-ID-00027	Removed	IRM.XML.V6
IRM-ID-00028	Removed	IRM.XML.V6
IRM-ID-00032	Removed	IRM.XML.V6

Chapter 4 - Data Rendering Constraint Rules

The constraint rules in this chapter define constraints on the rendering of IRM.XML documents. The intent is to inform the development of systems capable of rendering or displaying IRM.XML data for use by individuals not familiar with the details of the IRM.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 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. IRM.XML data rendering constrain rule IDs are prefixed with "IRM-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 IRM.XML data rendering constraint rules.

Table 4 - Constraint Rules

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

4.3 - Obsolete Constraint Rules

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

Table 5 - Obsolete Rules

Rule Number	Removed/ Replaced	Version
There are no obsolete Data Rendering Constraint rules at this time.		

Chapter 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the IRM.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 IRM.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 IRM.XML Schematron rules can be found in a separate document named *IRM_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 shows the version dependencies for NTK on other DES.

Table 6 - IRM Dependency over time

Dependent DES	V1	V2	V3	V4	V5	V6	V7
ISM	Pre-V1	V4	V5	V6	V7	V7	V8
NTK		V2	V3	V4	V5	V5	V6

The following table summarizes major features by version for this IRM and all dependent specs.

Table 7 - 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. IRM Feature Summary

Table 8 - IRM Feature comparison

IRM Feature Comparison								
Required date	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**
	Mime Types	N	F	F	F	F	F	F
	Schematron Implementation of rules	N	N	F	F	F	F	F
	ORCON Memo support	P	P	P	P	F	F	F
	XLink 1.1	N	N	N	N	F	F	F
	Allow more than 3 decimal places on times	N	N	N	N	N	N	F

A.2. ISM Feature Summary

Table 9 - ISM Feature comparison

ISM Feature Comparison									
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**
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
E.O. 13526 December 29, 2009	Compilation Reason	N	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
CAPCO Register and Manual 3.1 May 7, 2010	LES-NF	P	N	F	F	F	F	F	F
CAPCO Register and Manual All versions Pre 2008	Require Notices	N	N	F	F	F	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	KDK	N	N	F	F	F	F	F	F
ICD 710 September 11, 2009	710 Foreign Release	P	P	F	F	F	F	F	F
E.O. 13526 December 29, 2009	DeclassReasons/Dates	P	P	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
DoD Directive 5230.24 March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F
DoD Directive 5240.01 August 27, 2007	US Person Notice	P	P	P	P	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

ISM Feature Comparison									
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**
ISOO Marking Booklet 2010 / ISOO Notice 2009-13 December 2010	Remove exempted source	P	P	P	P	F	F	F	F
E.O. 13526 December 29, 2009	derivativelyClassifiedBy	P	P	P	P	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
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	Display Only	N	N	N	N	F	F	F	F
IC-CIO enhance data quality See IC ESB	Schematron Implementation of rules	N	N	N	N	F	F	F	F
E.O. 13526 December 29, 2009	50X1-Hum 50X2-WMD	N	N	N	N	F	F	F	F
DoD 5200.1-R January 1997	DoD ACCM Markings	N	N	N	N	N	F	F	F
CAPCO Register and Manual 4.2 May 31, 2011	SSI	N	N	N	N	N	F	F	F
ISOO 32 CFR Parts 2001 and 2003 June 28, 2010	TFNI	N	N	N	N	N	F	F	F
CAPCO Register and Manual 4.1 December 10, 2010	HCS SubCompartments	N	N	N	N	N	F	F	F
CAPCO Register and Manual 4.1 November 16, 2010 (date disestablished)	MCFI Remove	P	P	P	P	P	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

ISM Feature Comparison									
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**
ISOO 32 CFR Parts 2001 and 2003 June 28, 2010	Multivalue declassException	F	N	N	N	N	N	F	F
IC-CIO enhance data quality See IC ESB	SouthSudan	N	N	N	N	N	N	F	F
ICD 710 September 11, 2009	710 POC	N	N	N	N	N	N	F	F
DNI ORCON memo March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F
ISOO Marking Booklet December 2010	Allow 50X1-HUM and 50X2-WMD to not have a date/ event	N	N	N	N	N	N	F	F
IC-CIO enhance data quality See IC ESB	RD, FRD, and Sigma rolldown enforced	N	N	N	N	N	N	N	F
December 30, 2012	Unclassified REL, RELIDO, NF, and DISPLAYONLY	N	N	N	N	N	N	N	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
CAPCO Register and Manual 4.1 December 10, 2011 (1 Year after 4.1)	SINFO Remove	P	P	P	P	P	P	P	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
CAPCO Register and Manual 5.1 December 30, 2011	RSV	N	N	N	N	N	N	N	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

A.3. NTK Feature Summary

Table 10 - NTK Feature comparison

NTK Feature Comparison							
Required date	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**
	Schematron Implementation of rules	N	N	F	F	F	F

Appendix B Change History

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

Table 11 - DES Version Identifier History

Version	Date	Purpose
1.0	July 2009	Initial Release
2	7 September 2010	Routine revision to technical specification. For details of changes, see Section B.6 - V2 Change Summary
3	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.5 - V3 Change Summary
4	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.4 - V4 Change Summary
5	19 September 2011	Routine revision to technical specification. For details of changes, see Section B.3 - V5 Change Summary
6	7 December 2011	Routine revision to technical specification. For details of changes, see Section B.2 - V6 Change Summary
7	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.1 - V7 Change Summary

B.1 - V7 Change Summary

Significant drivers for Version 7 include:

- See ISM V8 drivers

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

Table 12 - Data Encoding Specification V7 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V8 and NTK to V6.	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in these sub-specifications.
Removed IRM-ID-00018 so times are no longer constrained to 3 decimal places.	Schematron	Data generation and ingestion systems need to be updated to properly handle the greater precision now possible.

B.2 - V6 Change Summary

Significant drivers for Version 6 include:

- DDMS / IRM Harmonization

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

Table 13 - Data Encoding Specification V6 Change Summary

Change	Artifacts changed	Compatibility Notes
IRM and DDMS Harmonization: IRM is now an **irm:ICResourceMetadata-Package** wrapper around a DDMS 4.0 **ddms:resource** element.	Schema Documentation IRM-ID-00002 Changed IRM-ID-00005 Changed IRM-ID-00007 Changed IRM-ID-00008 Changed IRM-ID-00009 Changed IRM-ID-00010 Changed IRM-ID-00011 Changed IRM-ID-00012 Changed IRM-ID-00013 Changed IRM-ID-00014 Changed IRM-ID-00016 Changed IRM-ID-00018 Changed IRM-ID-00019 Changed IRM-ID-00020 Changed	Data generation and ingestion systems need to be updated to comply with all constraint rules in these sub-specifications as well as schema changes.

Change	Artifacts changed	Compatibility Notes
	IRM-ID-00021 Changed IRM-ID-00022 Changed IRM-ID-00024 Changed IRM-ID-00025 Changed IRM-ID-00027 Removed IRM-ID-00028 Removed IRM-ID-00029 Changed IRM-ID-00030 Changed IRM-ID-00031 Changed IRM-ID-00032 Removed IRM-ID-00033 Changed IRM-ID-00034 Changed IRM-ID-00035 Changed IRM-ID-00037 Changed IRM-ID-00038 Added IRM-ID-00039 Added	

Change	Artifacts changed	Compatibility Notes
	IRM-ID-00040 Added IRM-ID-00041 Added IRM-ID-00042 Added IRM-ID-00043 Added IRM-ID-00044 Added IRM-ID-00045 Added IRM-ID-00046 Added IRM-ID-00047 Added IRM-ID-00048 Added IRM-ID-00049 Added IRM-ID-00050 Added IRM-ID-00051 Added IRM-ID-00052 Added IRM-ID-00053 Added IRM-ID-00054 Added IRM-ID-00055 Added	

B.3 - V5 Change Summary

Significant drivers for Version 5 include:

- See ISM V7 drivers
- National HUMINT Director for several new markups
- Joint Chiefs of Staff Pub 2.0: Appendix B - Intelligence Disciplines

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

Table 14 - Data Encoding Specification V5 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V7 and NTK to V5.	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in these sub-specifications.
Removed IRM **NoticeList**, **Notice**, and **NoticeText** elements, and updated references to **irm:NoticeList** to **ism:NoticeList**.	Schema IRM-ID-00002 Changed	Data generation and ingestion systems need to be updated to use the new values.
Replaced IC-DDMS with clean version of DDMS 3.0 and enforce specific IC constrains with new Schematron rules	IRM-ID-00031 Added IRM-ID-00032 Added IRM-ID-00033 Added IRM-ID-00034 Added IRM-ID-00035 Added	Data generation and ingestion systems need to be updated to use the new constraint rules.
Updated XLink to version 1.1, which further restricts the types of certain attributes.	Schema IRM-ID-00036 Added	Data generation and ingestion systems need to be updated to use the new values. Note: Data generated under previous releases may not be valid under this release.
Added support for ORCON memos and points-of-contact by extending DDMS elements **creator, publisher, contributor** and **pointOfContact** to include the **ism:POCAttributesGroup**.	Schema IRM-ID-00037 Added	Data generation and ingestion systems need to be updated to use the new values and comply with all constraint rules. Note: Data generated under previous releases may not be valid under this release.

Change	Artifacts changed	Compatibility Notes
Added **irm:Dates/@dateReceived** attribute to track when a product is received from an external source.	Schema IRM-ID-00016 Changed IRM-ID-00018 Changed IRM-ID-00024 Changed	Data generation and ingestion systems need to be updated to use the new values and comply with all constraint rules.
Added **ProcessingInfoList** and **ProcessingInfo** elements, with the required **@dateProcessed** attribute, to track when a product has been transformed in some way post-production.	Schema IRM-ID-00016 Changed IRM-ID-00018 Changed IRM-ID-00024 Changed	Data generation and ingestion systems need to be updated to use the new values and comply with all 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.
Fixed type errors generated when using a schema-aware processor.	Constraint Rules	Should not affect data.
Updated Intelligence Discipline and Subdiscipline CVE values in accordance with JP 2-0: Joint Intelligence.	CVEnum-IRMIntelDisciplines.xml, CVEnumIRMIntelSub-disciplines.xml	Data generation and ingestion systems need to be updated to use the updated CVE values.
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.

B.4 - V4 Change Summary

Significant drivers for Version 4 include:

- See ISM V6 drivers
- National HUMINT Director for several new markups

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

Table 15 - Data Encoding Specification V4 Change Summary

Change	Artifacts changed	Compatibility Notes
Changed 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.
Removed support for ISO 3166 Digraph codes	Documentation, Schema, CVEnumIRMCoverageISO3166-Digraph, IRM-ID-00002 (Value Enumeration Constraints) Removed	Data generation and Ingestion systems need to be updated to not use these values anymore and to properly enforce only the remaining constraint rules. Note: Rule identifier IRM-ID-00002 was previously used for two rules, one under Value Enumeration Constraints and the other under Global Constraints. Now, only the Global Constraints rule remains.
Removed support for ISO 3166 Numeric codes	Documentation, Schema, CVEnumIRMCoverageISO3166-Numeric, IRM-ID-00004 Removed	Data generation and Ingestion systems need to be updated to not use these values anymore and to properly enforce only the remaining constraint rules.
Corrected incorrect reference to ISO 639 CVE file	IRM-ID-00010 Changed	Data generation and Ingestion systems need to be checked to ensure the correct values are being used.

Change	Artifacts changed	Compatibility Notes
Changed wording of rules to distinguish between attributes and elements using similar constructs	IRM-ID-00018 Changed IRM-ID-00024 Changed	As the intent of the rules remains unchanged, this should not impact data.
Added **irm:CountryCodeCoverageList** and **irm:CountryCode** element	Schema IRM-ID-00027 Added IRM-ID-00028 Added IRM-ID-00029 Added	Data generation and Ingestion systems need to be updated to properly support new elements.
Added **irm:SubCountryCodeCoverageList** and **irm:SubCountryCode** elements	Schema	Data generation and Ingestion systems need to be updated to properly support new elements.
Added @**irm:order** attribute to specify a user-defined ordering of elements, including **irm:NonStateActor, irm:CountryCode** and **irm:SubCountryCode**	Schema IRM-ID-00030 Added	Data generation and Ingestion systems need to be updated to properly support new attribute.
Removed rules for @**ism:compliesWith** ICD-710	IRM-ID-00026 Removed	Data generation and Ingestion systems need to be updated to no longer enforce this constraint.

B.5 - V3 Change Summary

Significant drivers for Version 3 include:

- See ISM V5 drivers
- Executive Order 13526
- National HUMINT Director for several new markups

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

Table 16 - Data Encoding Specification V3 Change Summary

Change	Artifacts changed	Compatibility Notes
Use ISM V5	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Add IRM.XML MIME type	DES, Schema	IRM.XML MIME type has been declared in order to facilitate communications and address business needs within the community
Remove Appendix H Reading the Schematics	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.
Add support for expressing coverage of NonState Actors	Documentation Schema	Data generation and Ingestion systems need to be updated to properly support new elements.

B.6 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V4 drivers
- Executive Order 13526
- CAPCO Register for Notice Requirements

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

Table 17 - Data Encoding Specification V2 Change Summary

Change	Artifacts changed	Compatibility Notes
Added all constructs other than **ddms:resource**	All	Prior data will need to have the constructs other than **ddms:resource** and will have to map **ddms:resource** to **irm:ICResourceMetadata-Package**

Appendix C Acronyms

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

Table 18 - Acronyms

Name	Definition
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
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 Information
ODNI	Office of the Director of National Intelligence
SSD	Special Security Directorate
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 D 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 Register and Manual)

Intelligence Community Authorized Classification and Control Markings Register and Manual Unclassified FOUO version. Volume 5, Edition 1 (Version 5.1) (Effective: 30 December 2011). Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register%20and%20Manual%20v5.1_04Jan11_FOUO.pdf .

(CAPCO Register and Manual Appendix A)

Intelligence Community Classification and Control Markings Manual for Non-US Protective Markings Appendix A Unclassified FOUO version. Volume 5, Edition 1 (Version 5.1) (Effective: 30 December 2011). Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Manual_Appendix%20A_Non%20US_v5.1_30Dec11_FOUO.pdf .

(CAPCO Register and Manual Appendix B)

Intelligence Community Classification and Control Markings Manual for NATO Protective Markings Appendix B Unclassified FOUO version. Volume 5, Edition 1 (Version 5.1) (Effective: 30 December 2011). Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Manual_Appendix%20B_NATO_v5.1_30Dec11_FOUO.pdf .

(DC MES)

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

(DoD Directive 5200.1-R)

Information Security Program 5200.1-R January, 1997, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf .

(DoD Directive 5230.24)

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

(DoD Directive 5240.01)

DoD Intelligence Activities 5240.01 August 27, 2007, Secretary of Defense http://www.dtic.mil/whs/directives/corres/pdf/524001p.pdf .

(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 .

(ICD 710)

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

(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 32 CFR Parts 2001 and 2003)

Classified National Security Information; Final Rule. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. Monday, June 28, 2010 Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf .

(ISOO notice 2012-02)

ISOO Notice 2012-02: Classification Marking Instructions on the Use of "50X1-HUM" vs "25X1-human" as a Declassification Instruction. Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). http://www.archives.gov/isoo/notices/notice-2012-02.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/marking-booklet.pdf

http://www.schematron.com/ .

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.