Intelligence Community Technical Specification

XML Data Encoding Specification for Information Resource Metadata

Version 8

17 July 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 implementation guidance for using Extensible Markup Language (XML) to encode Information Resource Metadata (IRM) 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 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 or removes constraints on the data. See section Section 2.3 - DDMS Constraint Modifications for a table documenting the modifications made to the published DDMS schema.

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 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 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[23] 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
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V9)[13]
XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML.V7)[20]
Department of Defense Discovery Metadata Specification [2] (DDMS 4.1)
ISO Schematron[23] 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. 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[2] 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[2] 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[2]. 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. To properly convey this in ISM requires the use of attribute **@ism:externalNotice** with a value of [true].

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 Manual[1] 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,[3] 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. This type 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.

2.2.7 - ddms:type Use in IRM

The element type in DDMS is used for many specific uses in IRM. These uses are indicated with a specific set of ddms:qualifier values. There are many ways the IC has to categorize and group data. The ddms:type element allows us to keep adding ways without impacting the main schema or most processing systems. A definition for each of the uses is listed below.

2.2.7.1 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intel:disciplines:v1'

The @ddms:value would represent an intelligence discipline to which a resource applies. Prefix the value with "other:" to specify a value that is not in the enumerated list. ISM attributes if present refer to the classification of the Discipline or text in otherDiscipline.

2.2.7.2 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intel:subdisciplines:v1'

The @ddms:value would represent a refinement of the intelligence discipline to which a resource applies. Prefix the value with "other:" to specify a value that is not in the enumerated list. ISM attributes if present refer to the classification of the SubDiscipline or text in other:SubDiscipline.

2.2.7.3 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intel:subdisciplinetechniques:v1'

The @ddms:value would represent a technique used by the intelligence discipline to which a resource applies. Prefix the value with "other:" to specify a value that is not in the enumerated list. ISM attributes if present refer to the classification of the technique or text in other:technique.

2.2.7.4 - @ddms:qualifier= 'urn:us:gov:ic:reportinglevel'

The @ddms:value would represent a designation of the time elapsed between an observation and reporting of the observation.

2.2.7.5 - @ddms:qualifier= 'urn:us:gov:ic:productline'

The @ddms:value would represent a description of an agency-specific suite of resources. ProductLine may be used to specify that a resource is a member of a given category of resources such as serials. It is up to the producing organizations to ensure that the content of the element is consistent from resource to resource. For example, if "CAR" is the accepted acronym for campaign analysis report, producers should check that the acronym is consistently used in each CAR resource.

2.2.7.6 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:activity:v1'

The @ddms:value would represent if the resource is associated with a particular type of activity, the current list of possible values is: crisis, exercise, operation. The contents of the ddms:type element are intended for the name or descriptor of the activity.

2.2.7.7 - @ddms:qualifier= 'urn:us:gov:ic:irm:maliciouscodeindicator'

The @ddms:value would be a value from the CVEnumIRMMaliciouseCodeIndicator that indicates the confidence in the presence or absence of malicious code. This data element is intended to provide a data point, not dictate how a receiving system is to react, which is left to receiving organization policy. Only certain IC systems are certified to process malicious content.

2.2.7.8 - @ddms:qualifier= 'urn:us:gov:ic:irm:executableindicator'

The @ddms:value would be a value from the CVEnumIRMExecutableIndicator that indicates the confidence in the presence or absence of executable code. This data element is intended to provide a data point, not dictate how a receiving system is to react, which is left to receiving organization policy. Only certain IC systems are certified to process executable content.

2.2.7.9 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:authorizationreference'

The @ddms:value would represent an indicator of a unique and documented legal basis for all activities surrounding the creation, retention and use of an information resource.

2.2.7.10 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:evaluated'

The @ddms:value would represent: An indication of whether a resource contains information pertaining to the objectives of that resource's applicable mission authority.

2.2.7.11 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:minimized'

The @ddms:value would represent: An indication of the presence of protected person information in a resource, within the context of that resource's applicable mission authority..

2.2.8 - Use of Attribute irm:compliesWith

Attribute irm:compliesWith was created to allow an IRM document to specify which set of rules it complies with. The initial motivation for allowing an IRM document to comply with a subset of IRM rules was to allow IRM documents to specify only the minimum set of attributes required for cloud ingest. Attribute irm:compliesWith is required by schema to force documents to explicitly state which set of rules it complies with. The available tokens are enumerated in the file CVEnumIRMCompliesWith.xml and are explained in more detail in the following subsections.

2.2.8.1 - MIN_ACCESSIBLE

For a data asset, cloud ingest defines a minimum set of fields required to make an access control decision. The MIN_ACCESSIBLE token means that the IRM document complies with the rules which enforce this minimum set of required fields. The minimum set of required fields for cloud ingest include:

1. Classification
2. Creation date
3. Creator organization
4. Identifier

A detailed list of which rules enforce these constraints can be found in Chapter 4 of the IRM_Rules document.

2.2.8.2 - MIN_DISCOVERABLE

IRM instances are intended to contain discovery metadata about a data asset in order to make the asset discoverable, indexable, and useful. Historically, IRM has defined a minimum set of required discoverability attributes (some via schema, some via business rule). The MIN_DISCOVERABLE token enforces this minimum set of discoverability attributes by including all constraints enforced for token MIN_ACCESSIBLE and introducing additional constraints. A detailed list of which rules enforce these constraints can be found in Chapter 5 of the IRM_Rules document.

2.3 - DDMS Constraint Modifications

In order to allow IRM instances to specify only the minimal set of fields required for cloud ingest, several modifications were made to the published DDMS v4.1 schema. Constraints which were previously enforced by the DDMS schema are now enforced by IRM business rules for documents which claim compliance with the minimum set of discoverability attributes. See

Section 2.2.8.2 - MIN_DISCOVERABLE for more information about IRM instances complying with minimum discoverability attributes. See Section 2.2.8.1 - MIN_ACCESSIBLE for more information about fields required for cloud ingest.

The following table documents the exact modifications which were made to the published DDMS schema:

Table 2 - DDMS Constraint Modifications

XPath in DDMS Schema	Published Cardinality	Modified Cardinality
ddms:resource/ddms:title	minOccurs=1, maxOccurs=unbounded	minOccurs=0, maxOccurs=unbounded
choice of {**ddms:resource/ ddms:creator**, **ddms:resource/ ddms:publisher**, **ddms:resource/ ddms:contributor**, **ddms:resource/ ddms:pointOfContact**}	minOccurs=1, maxOccurs=unbounded	minOccurs=0, maxOccurs=unbounded
ddms:resource/ ddms:subjectCoverage	minOccurs=1, maxOccurs=unbounded	minOccurs=0, maxOccurs=unbounded

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[23] was selected as the language in which to encode these additional rules. The provided Schematron[23] 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*® [22] or the XSLT 2.0[27] implementation of ISO Schematron[23] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[26] and XSLT 2.0[27] features. According to Mr. Jelliffe, the editor of Schematron[23] 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[23] implementation and XSLT 2.0[27] 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 starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers. These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft 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. [1] Elements, which are allowed to only have text content, must have text content specified.

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

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[23] files to provide a single searchable document for all of the

[1] "white space" is defined in XML 1.0[25] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

constraint rules encoded in Schematron[23]. Obsolete rule numbers are listed in the SchematronGuide.

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 starter set and do not attempt to address the full scope tradecraft and business rules addressed by multiple policy drivers. These rules will be expanded and modified as the model matures, and as applicable documentation and tradecraft 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 3 - 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 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*® [22], 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[23] 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[23] files to provide a single searchable document for all of the constraint rules encoded in Schematron[23].

Appendix A Feature Summary

The following table shows the version dependencies for IRM on other DES.

Table 4 - IRM Dependency over time

Dependent DES	V1	V2	V3	V4	V5	V6	V7	V8
ISM	Pre-V1	V4	V5	V6	V7	V7	V8	V9
NTK		V2	V3	V4	V5	V5	V6	V7

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

Table 5 - 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 6 - IRM Feature comparison

IRM Feature Comparison									
Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8
	Mime Types	N	F	F	F	F	F	F	F
	Schematron[23] Implementation of rules	N	N	F	F	F	F	F	F
	ORCON Memo[21] support	P	P	P	P	F	F	F	F
	XLink 1.1[24]	N	N	N	N	F	F	F	F
	Allow more than 3 decimal places on times	N	N	N	N	N	N	F	F
	MinDiscoverable and MinAccessible modes	N	N	N	N	N	N	N	F

A.2. ISM Feature Summary

Table 7 - 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
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[5] March 18, 1987	DoD Distro Statements	N	N	N	F	F	F	F	F	F
DoD Directive 5240.01[6] August 27, 2007	US Person Notice	P	P	P	P	F	F	F	F	F

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
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[17] / ISOO Notice 2009-13[18] 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[23] 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
DoD Directive 5200.1-R[4] 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)[16] 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

ISM Feature Comparison										
Driver **Required date**	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**
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)[16] 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 [21] March 11, 2011	ORCON POC	N	N	N	N	N	N	F	F	F
ISOO Marking Booklet[17] 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
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

ISM Feature Comparison										
Driver Required date	Feature	V1	V2	V3	V4	V5	V6	V7	V8	V9
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[4] February 2012	COMSEC Notice	N	N	N	N	N	N	N	N	F
DoD Directive 5200.1-R[4] February 2012	Support for NNPI	N	N	N	N	N	N	N	N	F

A.3. NTK Feature Summary

Table 8 - NTK Feature comparison

NTK Feature Comparison								
Required date	Feature	V1	V2	V3	V4	V5	V6	V7
	Schematron[23] Implementation of rules	N	N	F	F	F	F	F
	Portion Level NTK	N	N	N	N	N	N	F

Appendix B Change History

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

Table 9 - 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.7 - V2 Change Summary
3	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.6 - V3 Change Summary
4	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.5 - V4 Change Summary
5	19 September 2011	Routine revision to technical specification. For details of changes, see Section B.4 - V5 Change Summary
6	7 December 2011	Routine revision to technical specification. For details of changes, see Section B.3 - V6 Change Summary
7	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.2 - V7 Change Summary
8	17 July 2012	Routine revision to technical specification. For details of changes, see Section B.1 - V8 Change Summary

B.1 - V8 Change Summary

Significant drivers for Version 8 include:

- See ISM V9 drivers
- DDMS[2]
- IC Cloud

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

Table 10 - Data Encoding Specification V8 Change Summary

Change	Artifacts changed	Compatibility Notes
Update ISM to V9 and NTK to V7.	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in these sub-specifications.
Update mapping to ADD	DES	Should not impact data

Change	Artifacts changed	Compatibility Notes
Add Mapping for AUTH-ID as a ddms:type [artf12285].	DES Schema	Data generation and ingestion systems need to be updated to use new structure
Updated IRM-ID-00039 to verify that at least one **productionMetric** exists in one of the **subjectCoverage** elements.	Schematron	Data generation and ingestion systems need to be updated to use the new values and comply with all constraint rules.
Added support for alphanumeric @**DESVersion** identifiers [artf12167].	Schema	Should not impact data but ingestion systems may need to account for it.
Added support for malicious code, executable, authorizationreference, evaluated, and minimized as ddms:types [artf12285].	DES	Data generation and ingestion systems need to be updated to use the new values and comply with all constraint rules.

Change	Artifacts changed	Compatibility Notes
Added attribute compliesWith to allow IRM instance documents to comply with subsets of rules, including rules for minimum access (cloud ingest) and minimum discoverability.	Schema Schematron IRM-ID-00035 Changed IRM-ID-00038 Changed IRM-ID-00039 Changed IRM-ID-00055 Changed IRM-ID-00056 Added IRM-ID-00059 Added IRM-ID-00061 Added IRM-ID-00063 Added IRM-ID-00064 Added IRM-ID-00065 Added CVEnum-IRMCompliesWith.xml Added	Data generation and ingest systems need to be updated to use the new and modified rules and support the modified schema.
Updated rule IRM-ID-00037 to only apply to specific DDMS element creator, publisher, contributor, and pointOfContact to prevent rules from firing on element irm:NoticeText.	IRM-ID-00037 Changed	Should not impact exisiting data but ingestion systems need to account for modified rule.
Removed rule IRM-ID-00011 because it is covered by rule IRM-ID-00012	IRM-ID-00011 Removed	Data generation and ingestion systems need to be updated to use the correct constraint rules.

Change	Artifacts changed	Compatibility Notes
Removed rule IRM-ID-00013 because it is covered by rule IRM-ID-00014	IRM-ID-00013 Removed	Data generation and ingestion systems need to be updated to use the correct constraint rules.
Added rule to require notices within ddms:security to be marked as externalNotice='true' since they refer to the referenced resource	IRM-ID-00066 Added	Data generation and ingestion systems need to be updated to use the new rule.
Added rule to require ntk:Access within ddms:security to be marked as externalReference='true' since it refers to the referenced resource	IRM-ID-00067 Added	Data generation and ingestion systems need to be updated to use the new rule.
Added rule to enforce format of IC-ID identifiers.	IRM-ID-00062 Added	Data generation and ingestion systems need to be updated to use the new rule.
Added rules to enforce network attribute and xlink attribute constraints on ddms:taskID	IRM-ID-00068 Added IRM-ID-00069 Added	Data generation and ingestion systems need to be updated to use the new rules.
Added rules to enforce CVE values for ExecutableIndicator and MaliciousCodeIndicator [artf12660]	IRM-ID-00070 Added IRM-ID-00071 Added CVEnum-IRMMaliciousCodeIndicator Added CVEnum-IRMExecutableIndicator Added	Data generation and ingestion systems need to be updated to use the new rules.

B.2 - 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 11 - 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.3 - V6 Change Summary

Significant drivers for Version 6 include:

- DDMS[2] / IRM Harmonization

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

Table 12 - 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[2] **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.4 - 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[19]

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

Table 13 - Data Encoding Specification V5 Change Summary

Change	Artifacts changed	Compatibility Notes
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[2] and enforce specific IC constrains with new Schematron[23] 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[24] 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[21] memos and points-of-contact by extending DDMS[2] 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.[19]	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 3166-1[15] 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.5 - 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 14 - Data Encoding Specification V4 Change Summary

Change	Artifacts changed	Compatibility Notes
Changed encoding of constraint rules from text to Schematron.[23]	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 3166-1[15] 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 3166-1 Numeric codes.[15]	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[14] 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.[9]	IRM-ID-00026 Removed	Data generation and Ingestion systems need to be updated to no longer enforce this constraint.

B.6 - V3 Change Summary

Significant drivers for Version 3 include:

- See ISM V5 drivers
- Executive Order 13526[7]
- National HUMINT Director for several new markups

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

Table 15 - 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.7 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V4 drivers
- Executive Order 13526[7]
- CAPCO Register for Notice Requirements[1]

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

Table 16 - 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 17 - 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] DDMS
Department of Defense. *DoD Discovery Metadata Specification*. 4.0.1.
Available online at: http://metadata.dod.mil/mdr/irs/DDMS/

[3] DNI Overview
Director of National Intelligence. *An Overview of the United States Intelligence Community for the 111th Congress*. 2009.
Available online at: www.dni.gov/overview.pdf/ [www.dni.gov/overview.pdf]

[4] 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

[5] 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

[6] 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

[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] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/ISM
Available online at: http://purl.org/IC/Standards/public

[14] ISO 639-1
International Organization for Standardization (ISO). *Codes for the representation of names of languages – Part 1: Alpha-2 code*. ISO 639-1:2002.
Available online at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22109

[15] 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

[16] 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

[17] 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

[18] 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

[19] JP 2-0
Joint Chiefs of Staff. *Joint Intelligence*. 22 June 2007.
Available online at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

[20] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/NTK
Available online at: http://purl.org/IC/Standards/public

[21] 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

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

[23] 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/

[24] XLink
World Wide Web Consortium (W3C) . *XML Linking Language (XLink) Version 1.1*. W3C Recommendation 06 May 2010.
Available online at: http://www.w3.org/TR/2010/REC-xlink11-20100506/

[25] 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/

[26] 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/

[27] 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]