Intelligence Community Technical Specification

XML Data Encoding Specification for Information Resource Metadata

Version 2016-SEP

September 9, 2016

Table of Contents

List of Figures

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 (IC). In some cases, this DES specifies additional constraints on the data or removes constraints on the data.

1.2 - Scope

This specification is applicable to the 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 Intelligence Community 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* [16] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, 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 Information Technology (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 Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [22] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* [2]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID[11] defines a plain-text format for IC Identifiers as well as an associated XML structure.

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.

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[8]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[16]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[17]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[22]
- 200 Series:
  - Intelligence Community Directive (ICD) 206, Sourcing Requirements for Disseminated Analytic Products[13]
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[14]
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[15]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community’s Responsibility to Provide[20]

1.5 - Audience and Applicability

This is a data encoding specification. It defines the structure and related business rules for encoding the described data type. A DES is intended for those developing tools and services that create, modify, store, exchange, search, display, or further process the type of data being described.

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance,* [21] defines the

IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,[5] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

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

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.” [23] When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

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

1.6.3 - Terminology

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, enlighten or inform.

1.6.4 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 1 - XML Namepaces

Prefix	URI
ddms	urn:us:mil:ces:metadata:ddms:5
edh	urn:us:gov:ic:edh
irm	urn:us:gov:ic:irm
ism	urn:us:gov:ic:ism
ntk	urn:us:gov:ic:ntk
xsd	http://www.w3.org/2001/XMLSchema

1.7 - Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in Table 2. The dependencies listed below are directly referenced in this specification (e.g. Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, Figure 1, is an informative graphical representation of all of the IC CIO specifications related to this specification. The graphic depicts direct and transitive dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All specifications listed in Table 2 will be shown in Figure 1; however not all specifications listed in Figure 1 may appear in Table 2. Figure 1 is to aid users in gaining a general understanding of all transitive dependencies.

Table 2 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Information Security Marking Metadata (ISM.XML.V13+)[26]	The specification does not depend on a specific version of Information Security Marking Metadata (ISM.XML); ISM.XML versions later than version 13 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML.V3+)[12]	The specification does not depend on a specific version of Trusted Data Format (IC-TDF.XML); IC-TDF.XML versions later than version 3 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.

Name	Dependency Description
XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML.V1+)[11]	The specification does not depend on a specific version of Intelligence Community Identifier (IC-ID.XML); IC-ID.XML versions later than version 1 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
CVE Encoding Specification for US Agency (USAgency.CES.V2015-FEB+)[37]	The specification does not depend on a specific version of US Agency (USAgency.CES); USAgency.CES versions later than version 2015-FEB MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
CVE Encoding Specification for IC-GENC (IC-GENC.CES.V2016-SEP+)[10]	The specification does not depend on a specific version of IC Geopolitical Entities, Names, and Codes (IC-GENC.CES); IC-GENC.CES versions later than version 2016-SEP MAY be used. The minimum version was based on a technical dependency; The creation of IC-GENC schema and its CESVersion attribute.
CVE Encoding Specification for Production Metrics (PM.CES.2015-NOV+)[34]	The specification does not depend on a specific version of Production Metrics (PM.CES); PM.CES versions later than version 2015-NOV MAY be used. The minimum version was based on a technical dependency; The addition of coverage and non-state actor CVEs.
CVE Encoding Specification for Intelligence Discipline (INTDIS.CES.V2016-SEP+)[24]	The specification does not depend on a specific version of Intelligence Discipline (INTDIS.CES); INTDIS.CES versions later than version 2016-SEP MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
CVE Encoding Specification for Media Type (MIME.CES.V2016-SEP+)[31]	The specification does not depend on a specific version of Media Type (MIME.CES); MIME.CES versions later than version 2016-SEP MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
Department of Defense Discovery Metadata Specification(DDMS 5)[4]	Depends on DoD Discovery Metadata Specification (DDMS).

Name	Dependency Description
Schematron[35]	Schematron — ISO/IEC 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use XSLT 2.0[43] query binding.
XSLT 2.0[43] implementation of Schematron[35] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations (CVEs) included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the IRM CVEs is normative.

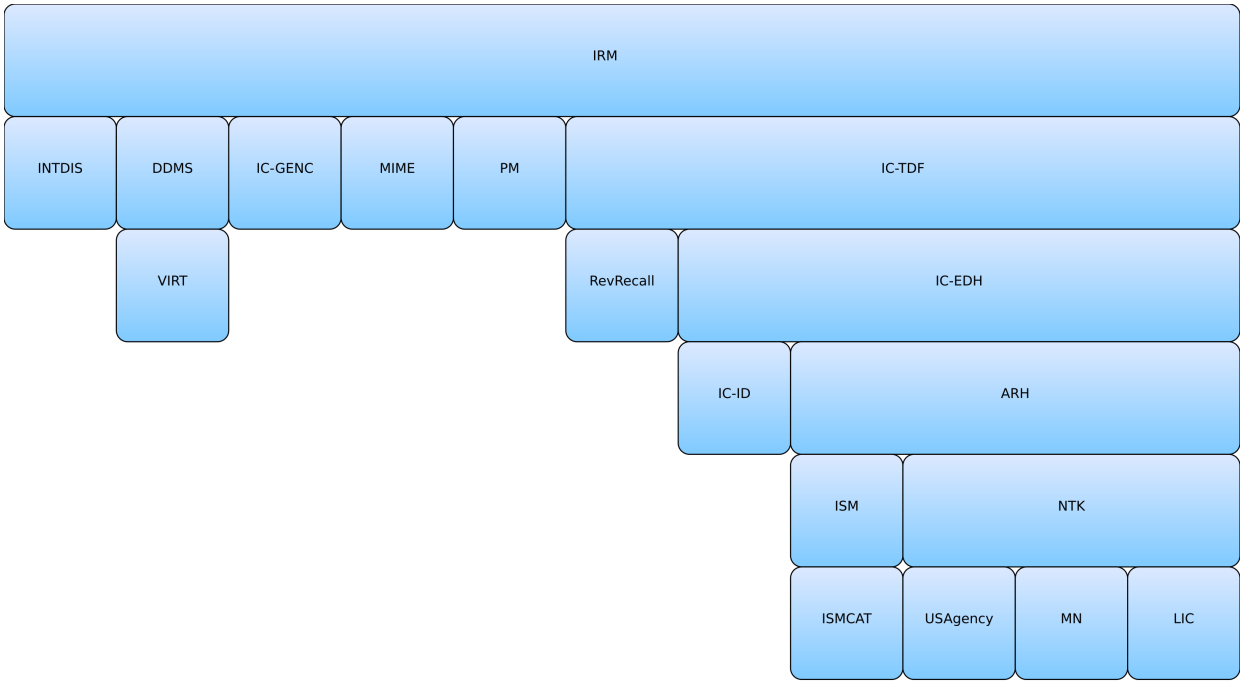

Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions of all transitive dependent specifications at the time the package is generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies and their dependencies will have to be traversed and obtained. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and controlled vocabulary enumerations (CVEs) to validate and operate as intended.

Convenience packages convey all dependencies pre-packaged together and are tested as interoperable. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron[35] rules are normative for this specification. 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 PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[23] is considered normative within the scope of the sentence. All other parts of this document are informative.

The XML schemas provided may import other specifications. The versions of dependency specifications imported are not normative in that to import a different version of a component specification you could modify the import or substitute a different version of the component using the existing import path. This could be done by changing the schema file or by using XML Catalogs.[41] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion**='9' to **@ism:DESVersion**='10' in the xsd:schema statement. The ability to specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as PUBS and TDF) to be "decoupled" from the configuration change control of dependent specifications (such as ISM CVE updates). This "decoupling" method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

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

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from “The Disposition of Names in an XML Namespace.”[36] This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 “Versioning and XML namespace policy” of “Architecture of the World Wide Web, Volume One.”[38]

There is a version attribute (e.g. **@DESVersion**, **@CESVersion**, **@TESVersion**, **@version**) for each namespace defined in an IC CIO specification. Version attributes are used to capture the specification version number the specification author intends an instance to conform to. Namespaces do not change, so the version attribute is required to fully understand an instance document.

As changes to the specification are released, the version number captured in the “version” attribute increments. See Section 1.9.2 - Version Numbering for information on the numbering scheme.

This XML namespace policy only applies to the namespaces defined in this specification, any namespaces that are included by reference should define their own namespace policy.

1.9.2 - Version Numbering

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-MMM). This provides a temporal representation of when the specification was released. When the version number is used in the version attribute, the expression follows the Augmented Backus–Naur Form[1] below:

Version Format when used in the version attribute:

[1] Version : := Year Month ["-" CustomizationSuffix]
[2] Year : := 4(DIGIT)
[3] Month : := 2(DIGIT)
[4] Customization Suffix : := 1*27(ALPHA / DIGIT / "_")

Version in XML Lexicon

The following vocabulary helps explain the meaning of terms used in the version documentation, and it may further constrain the set of allowable values:

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version being referenced.
Year	The four digit year from the version of the specification being referenced.
Month	The 2 digit month from the version of the specification being referenced.
CustomizationSuffix	An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

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

The mappings in the ADD provide a starting point for the development of automated transformations between formats defined by the encoding specifications. 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 - ICResourceMetadataPackage Usage

IRM.XML is used in conjunction with IC-TDF objects as structured assertions. A Trusted Data Object (TDO) conforms to the IRM specification when it contains:

- A structured assertion of scope="PAYL" and an IRM ICResourceMetadataPackage element
- A structured assertion of scope="PAYL" and a DDMS resource element

where the token "PAYL" means this assertion applies only to the payload within the TDO.

2.2.2 - Document Identifiers

2.2.2.1 - Document IC-ID

All documents within the IC MUST have a single unique identifier. The identifier MUST conform to the IC-ID specification, and it MUST be encoded using IC-EDH [9] and the **edh:Identifier** element. For the purposes of this specification, such an identifier is referred to as the Document IC-ID. The Document IC-ID MAY be duplicated in DDMS [4] using the “IC-ID” qualifier.

Warning

A Document IC-ID should be unique across the whole of the IC, however, there is no managing body or registry service for Document IC-IDs. Content producers are responsible for ensuring ID uniqueness, including any required coordination amongst content producers.

2.2.2.2 - DocumentID

DocumentID refers to an identifier that is assigned by the agency to carry a document's publication or serial number. DocumentID is assigned by the publishing agency to identify a product or publication to the Community at large. DocumentID is not guaranteed to be unique across the enterprise, or even the agency assigning it. It SHOULD be unique across a productline for an agency. Unlike the IC-ID, the DocumentID may have discernible meaning. DocumentID is an optional identifier in IRM, but when provided in IRM, DocumentID MUST carry the document's publication or serial number. DocumentID is captured in DDMS [4] using ddms:identifier/ @ddms:qualifier= “urn:us:gov:ic:irm:identifier:documentid”.

2.2.2.3 - Other Identifiers

The Document IC-ID referenced in Section 2.2.2.1 - Document IC-IDintended to meet USA Government Policy requirements for an unambiguous, IC-wide identifier for a document. However, a document may have many identifiers, which may be necessary for various purposes including processing, retrieval, or tracking. These additional identifiers SHOULD be captured in DDMS [4]. Qualifiers for these additional identifiers will have the form “urn:us:gov:ic:irm:identifier:XXX” where XXX is the type of the identifier. Examples of identifier types include UUID, and InternalID.

2.2.3 - 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** to represent US or foreign publishing organizations. When identifying US organizations, the values comes from a controlled vocabulary enumeration (CVE) that includes values representing the organizations officially designated as Members of the IC by DNI, [25] plus the DNI, plus additional entries intended to recognize non-IC publishers whose information is commonly used in support of the intelligence mission. The use of a country prefix when identifying a US organization is optional (e.g., CIA, USA:CIA). When identifying foreign organizations, the use of a country prefix is required in order to identify the country to which the foreign organization belongs (e.g., GBR:GCHQ).

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, or DoS), or non-IC designation (e.g.,

OtherUSG). 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., OtherUSG, SLT) 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.

2.2.3.1 - 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="USPS">
      <ddms:name>United States Postal Service</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="USA:DIA">
      <ddms:name>Defense Intelligence Agency</ddms:name>
      <ddms:subOrganization>PACOM/J4</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

For British foreign agency GCHQ:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="GBR:GCHQ">
      <ddms:name>Government Communications Headquarters</ddms:name>
   </ddms:organization>
</ddms:publisher>
```

For XYZ component of British foreign agency GCHQ:

```
<ddms:publisher>
   <ddms:organization ddms:acronym="GBR:GCHQ">
      <ddms:name>Government Communications Headquarters</ddms:name>
      <ddms:subOrganization>GBR:XYZ</ddms:subOrganization>
   </ddms:organization>
</ddms:publisher>
```

2.2.4 - MIME Type

The Multipurpose Internet Mail Extensions (MIME) type for an 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.

2.2.5 - 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.

2.2.5.1 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intdis:inteldiscipline'

The **@ddms:value** represents an intelligence discipline to which a resource applies. ISM attributes if present refer to the classification of the discipline.

2.2.5.2 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intdis:inteldiscipline:component'

The **@ddms:value** represents a refinement of the intelligence discipline to which a resource applies. ISM attributes if present refer to the classification of the discipline component.

2.2.5.3 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:intdis:inteldiscipline:component:technique'

The **@ddms:value** represents 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 discipline component technique or text in other:DisciplineComponentTechnique.

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

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

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

The **@ddms:value** represents 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.

2.2.5.6 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:irm:activity'

The **@ddms:value** indicates that 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.

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

The **@ddms:value** is a value from the CVEnumIRMMaliciousCodeIndicator 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.

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

The **@ddms:value** is 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.

2.2.5.9 - @ddms:qualifier= 'urn:us:gov:ic:irm:authorizationreference'

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

2.2.5.10 - @ddms:qualifier= 'urn:us:gov:ic:irm:evaluated'

The **@ddms:value** provides an indication of whether a resource contains information pertaining to the objectives of that resource’s applicable mission authority.

2.2.5.11 - @ddms:qualifier= 'urn:us:gov:ic:irm:minimized'

The **@ddms:value** provides an indication of the presence of protected person information in a resource, within the context of that resource’s applicable mission authority.

2.2.5.12 - @ddms:qualifier= 'urn:us:gov:ic:cvenum:irm:positive:intel'

The **@ddms:value** describes the unavailability of finished intelligence information about a given topic, and are provided for applications in which some sort of statement must be made about each node of a taxonomy, even when no substantive analysis is available.

Chapter 3 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

Data constraint rules fall into two categories - validation and rendering constraints. Data validation constraints explicitly define policy validation constraints, describing how data should be structured and encoded in order to comply with IC policy. Validation constraint rules are implemented as a combination of basic XML Schema constraints and supplemental constraints for more complex rules. Complex constraint rules contain technical rule descriptions, Schematron rule implementations, and *Human Readable* descriptions. The human readable text describes the intent and meaning behind the more technical rule description. The semantics of the constraint rules are normative, whereas the use of the Schematron implementation is informative. Implementers developing alternative validation code should follow the technical rule descriptions and Schematron logic. Should there be a perception of conflict, implementers should bring it to the attention of the appropriate configuration control body for resolution. Rendering constraint rules define constraints on the display and rendering of documents. While expressed in a similar manner to the data validation constraint rules, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.2 - "Living" Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of business rules addressed by authoritative guidance. These rules will be expanded and modified as the model matures, and as applicable security marking policies change.

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

3.3 - Classified or Controlled Constraint Rules

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

3.4 - Constraint Terminology

For the purposes of this document, the following statements apply:

- The term "is specified" indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term "must be specified" indicates that an attribute MUST be applied to an element and the attribute MUST have a non-null value.
- The term "is not specified" indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.

- The term “must not be specified” indicates that an attribute MUST NOT be applied to an element.

3.5 - Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is more severe and is indicative of a clear violation of a constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

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

3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. IRM.XML data validation constraint rule identifiers are prefixed with "IRM-ID-" and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in Section 3.6 - Rule Identifiers [17]. As the constraint rules are managed over time, IDs from deleted rules will not be reused.

Table 3 - Numerical Rule Identifier Ranges

Rule Identifier Range		Description
Start	End	
00001	09999	Reserved for Unclassified constraint rules
10001	19999	Reserved for Unclassified but For Official Use Only (FOUO) constraint rules
20001	20999	Reserved for constraint rules classified at the “Secret//REL USA, FVEY” level
21001	21999	Reserved for constraint rules classified at the “Secret//NF” level
22001	29999	Reserved for constraint rules classified at the “Secret//TBD” level
30001 and above		Reserved for constraint rules classified with other classifications

3.7 - Data Validation Constraint Rules

3.7.1 - Purpose

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.

3.7.2 - Schematron

Schematron[35] is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document MUST meet, exactly as English may be used to convey normative criteria.

It is not necessary for implementers to use the specific Schematron encoding in this specification, and implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

For better understanding, the Schematron[35] rules for this specification may be executed in *Oxygen®* [33] or with an XSLT 2.0-compliant processor using the XSLT 2.0[43] transforms in the Schematron implementation from Rick Jelliffe (see XSLT 2.0 implementation of Schematron by Rick Jelliffe in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0[42] and XSLT 2.0[43] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:[29]

> 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.

Note

For convenience, the specification package provides the XSLT 2.0[43] implementation of Schematron[35] along with a compiled version of the rules.

3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. 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.

3.7.4 - 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 Section 1.7 - Dependencies.

[1] “White space” is defined in XML 1.0[40] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

3.7.5 - 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.

3.7.6 - Additional Constraints

3.7.6.1 - 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.

3.7.7 - 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. Obsolete rule numbers are listed in the SchematronGuide.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of 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.

3.8.2 - Rendering 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.			

Chapter 4 - Conformance Validation

An instance document conforms with this specification if it conforms to all normative guidance of this specification and this specification's dependencies and it passes all of the following validation steps. This specification does not dictate how this validation strategy is implemented.

4.1 - Schema Validation

An instance document MUST comply with the schemas for this specification and this specification's dependencies, and schema validation SHOULD occur prior to other validation steps. If schema validation fails, results from later steps may be indeterminate.

4.2 - Business Rule Validation

An instance document MUST comply with the business rules expressed in this specification and those expressed in this specification's dependencies. The business rules in this specification are expressed in Schematron, but it is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

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®,* [33] produced by SyncRO Soft.

The guide provides an interactive index to:

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

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (Child Elements)
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of the master HTML file *SchemaGuide.html* with supporting graphics.

5.2 - Schematron Guide

The detailed description and reference documentation for the IRM.XML Schematron[35] 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[35] files to provide a single searchable document for all of the constraint rules encoded in Schematron[35].

Appendix A Feature Summary

The following table shows the version dependencies for IRM on other specifications. Direct dependencies are marked with an asterisk.

Table 5 - IRM Dependency over time

Dependent Specification	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V2014-DEC	V2015-NOV	V2016-SEP
ISM*	Pre-V1	V4	V5	V6	V7	V7	V8	V9	V9+	V9+	V9+	V9+	V9+	V9+	V13+
NTK		V2	V3	V4	V5	V5	V6	V7	V7+	V7+	V7+	V7+	V7+	V7+	V10+
IC-TDF*									V1+	V1+	V1+	V1+	V1+	V1+	V3+
ARH									V1+	V1+	V1+	V1+	V1+	V1+	V3+
IC-EDH									V1+	V1+	V1+	V1+	V1+	V1+	V4+
DDMS*		V3	V3	V3	V3	V4	V4	V4.1	V5	V5	V5	V5	V5	V5	V5
IC-ID*										V1+	V1+	V1+	V1+	V1+	V1+
USAgency*											V1+	V1+	V1+	V1+	V2015-FEB+
IC-GENC*												V1+	V1+	V1+	V2016-SEP+
PM*														V2015-NOV+	V2015-NOV+
INTDIS*															V2016-SEP+
MIME*															V2016-SEP+
MN															V2015-AUG+
LIC															V2015-AUG+
ISMCAT															V2015-MAY+
RevRecall															V1+
VIRT															V1+

The following table summarizes major features by version for this IRM.

Table 6 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can’t comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. IRM Feature Summary

Table 7 - IRM Feature comparison

IRM Feature Comparison																
Required date	**Feature**	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**	**V11**	**V12**	**V2014-DEC**	**V2015-NOV**	**V2016-SEP**
	MIME Types	N	F	F	F	F	F	F	F	F	F	F	F	F	F	F
	Schematron[35] Implementation of rules	N	N	F	F	F	F	F	F	F	F	F	F	F	F	F
	ORCON Memo[32] support	P	P	P	P	F	F	F	F	F	F	F	F	F	F	F
	XLink 1.1[39]	N	N	N	N	F	F	F	F	F	F	F	F	F	F	F
	Allow more than 3 decimal places on times	N	N	N	N	N	N	F	F	F	F	F	F	F	F	F
	MinDiscoverable and MinAccessible modes	N	N	N	N	N	N	N	F	F	F	F	F	F	F	F
	Use TDO as container for all IRM components	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
	Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM V9+, NTK V7+, TDF V1+, ARH V1+, and EDH V1+	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
	Use of GENC [7] for all country code values	N	N	N	N	N	N	N	N	F	F	F	F	F	F	F
	IC-ID V1+	N	N	N	N	N	N	N	N	N	F	F	F	F	F	F
	US Agency V1+	N	N	N	N	N	N	N	N	N	N	F	F	F	F	F
	IC-GENC specification (V1+)	N	N	N	N	N	N	N	N	N	N	N	F	F	F	F
	DNI Negroponte Memorandum for Revision/Recall	N	N	N	N	N	P	P	P	P	P	P	F[a]	F	F	F
	PMv2015-NOV+, updates to non-state actors.	N	N	N	N	N	N	N	N	N	N	N	N	N	F	F
	INTDISv2016-SEP+, updates to intelligence discipline related CVEs and new dependency on INTDIS.	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F
	MIMEv2016-SEP+	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F
	Use of IC-GENC for both countries and subregions	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F
	Added support for foreign agency acronyms	N	N	N	N	N	N	N	N	N	N	N	N	N	N	F

[a]Full support is gained through use of the RevRecall specification and IRM blocks the use of the revisionRecall elements in DDMS.

Appendix B Change History

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

Table 8 - 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.14 - V2 Change Summary
3	6 December 2010	Routine revision to technical specification. For details of changes, see Section B.13 - V3 Change Summary
4	11 April 2011	Routine revision to technical specification. For details of changes, see Section B.12 - V4 Change Summary
5	19 September 2011	Routine revision to technical specification. For details of changes, see Section B.11 - V5 Change Summary
6	7 December 2011	Routine revision to technical specification. For details of changes, see Section B.10 - V6 Change Summary
7	27 February 2012	Routine revision to technical specification. For details of changes, see Section B.9 - V7 Change Summary
8	17 July 2012	Routine revision to technical specification. For details of changes, see Section B.8 - V8 Change Summary
9	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.7 - V9 Change Summary
10	5 April 2013	Routine revision to technical specification. For details of changes, see Section B.6 - V10 Change Summary
11	16 August 2013	Routine revision to technical specification. For details of changes, see Section B.5 - V11 Change Summary
12	14 March 2014	Routine revision to technical specification. For details of changes, see Section B.4 - V12 Change Summary
2014-DEC	4 December 2014	Routine revision to technical specification. For details of changes, see Section B.3 - V2014-DEC Change Summary
2015-NOV	16 November 2015	Routine revision to technical specification. For details of changes, see Section B.2 - V2015-NOV Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.1 - V2016-SEP Change Summary

B.1 - V2016-SEP Change Summary

The following table summarizes the changes made to 2015-NOV in developing 2016-SEP.

Table 9 - Data Encoding Specification V2016-SEP Change Summary

Change	Artifacts changed	Compatibility Notes
Updated IRM to use INTDIS CVEs instead of IRM CVEs for intelligence discipline related CVEs. (CR-2015-098)	Schematron IRM_XML.sch updated IRM-ID-00041 updated IRM-ID-00042 updated IRM-ID-00043 updated IRM-ID-00046 updated IRM-ID-00047 updated IRM-ID-00048 updated IRM-ID-00081 updated	Data generation and ingestion systems need to be updated to enforce the modified rule.
Removed IRM intelligence discipline related CVEs. (CR-2015-098)	CVE CVEnum-IRMIntelDisciplines.xml removed CVEnumIRMIntelSub-disciplines.xml removed CVEnumIRMIntelSub-disciplineTechniques.xml removed	Data generation and ingestion systems need to be updated to enforce the modified rule.
Added optional INTDIS CESVersion attribute to IRM attribute group. (CR-2015-098)	Schema IC-IRM.xsd updated Schematron IRM-ID-00086 added IRM-ID-00087 added	Data generation and ingestion systems need to be updated to enforce the modified rule.
Updated IRM to use MIME CVE instead of IRM CVE for mime types. (CR-2015-048)	Schematron IRM_XML updated IRM-ID-00033 updated	Data generation and ingestion systems need to be updated to enforce the modified rule.

Change	Artifacts changed	Compatibility Notes
Added optional MIME CESVersion attribute to IRM attribute group. (CR-2015-048)	Schema IC-IRM.xsd updated Schematron IRM-ID-00088 added IRM-ID-00089 added	Data generation and ingestion systems need to be updated to enforce the modified rule.
Added description for identifying additional document identifier values. (CR-2015-048)	DES	Data generation and ingestion systems need to be updated to handle the new potential values.
Added rule to give warning for use of deprecated MIME types. (CR-2015-048)	Schematron IRM-ID-00091 added	Data generation and ingestion systems need to be updated to utilize the new rule.
Removed 3 values and added one to CVE and updated rules based on changes. (CR-2016-009)	CVEnum CVEnum-IRMCompoundLanguge QualifierType Schematron IRM-ID-00008 removed IRM-ID-00009 removed IRM-ID-00010 updated for new value	Data generation and ingestion systems need to be updated to utilize the new rule.
Updated rules to include checking for the use of DDMS language in PUBS. (CR-2014-056)	Schematron IRM-ID-00005 updated IRM-ID-00006 updated IRM-ID-00007 updated IRM-ID-00010 updated	Data generation and ingestion systems need to be updated to utilize the new rule.

Change	Artifacts changed	Compatibility Notes
Updating to use IC-GENC for both countries and subregions. (CR-2015-089)	CVEnumIRMCoverage-ISO-3166-2SubCountry.xml removed Schema Schematron IRM-ID-00031 removed IRM-ID-00049 removed IRM-ID-00090 added IRM-ID-00093 added IRM-ID-00094 added IRM-ID-00095 added IRM-ID-00098 added	Data generation and ingestion systems need to be updated to utilize the new rules.
Updated schematron rules to enforce minimum versions defined in specification dependency table 1.7	Schematron IRM-ID-00080 updated IRM-ID-00096 added IRM-ID-00097 added IRM_ID-00099 added	Systems need to be updated to accommodate this change.
Updated IRM CVEs with latest ISO 639 updates.	CVE CVEnum-IRMISO639-2Trigraph updated CVEnum-IRMISO639-3Trigraph updated	Systems need to be updated to accommodate this change.

Change	Artifacts changed	Compatibility Notes
Added a schematron rule to enforce that tdf:StatementMetadata is present in a tdf:Assertion if ddms:resource is present within tdf:StructuredStatement to ensure proper classification. Previously, it was possible for the ddms:resource to have no classification, which could impact use and tear-lining. (CR-2016-043)	Schematron IRM-ID-00100 added	Systems need to be updated to accommodate this change.
Consistent qualifiers for UUIDs, DocumentIDs, and InternalIDs (CR-2014-015) Added standard way of including a document identifier that is required to be the publication/serial number if used. The optional DocumentID MUST conform to the standard format that everyone and every system knows as the publication/ serial number. (CR-2014-015)	Documentation	Systems need to be update to accommodate this change.
Correct rule to properly handle nested elements. (CR-2015-003)	Schematron IRM-ID-00075 updated	Systems need to be updated to accommodate this fix.
Added requirement for ddms:NonStateActor values to be from the NonStateActor CVE in PM.CES. (CR-2015-101)	Schematron IRM-ID-00092 added	Systems need to be updated to accommodate this new restriction.
The schema change logs will no longer be maintained as of the 2016-SEP release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2016-SEP, reference the change history in the DES.	Schema	No impact to systems.

Change	Artifacts changed	Compatibility Notes
Updated Schematron rules for IRM to account for @ddms:acronym that contains country code. (CR-2016-028)	Schematron IRM_XML.sch updated TypeConstraintPatterns.sch added IRM-ID-00052 updated IRM-ID-00101 added IRM-ID-00102 added IRM-ID-00103 added IRM-ID-00104 added	Systems need to be updated to accommodate this new restriction.
Update applicability section to reflect a requirement to comply with Law/ Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.2 - V2015-NOV Change Summary

The following table summarizes the changes made to 2014-DEC in developing 2015-NOV.

Table 10 - Data Encoding Specification V2015-NOV Change Summary

Change	Artifacts changed	Compatibility Notes
Updated IRM CVE imports for PMSubject and PMCoverage to use PM CVEs instead of IRM CVEs.	Schematron IRM_XML updated IRM_ID_00050 updated IRM_ID_00051 updated	Data generation and ingestion systems need to be updated to enforce the modified rule.
Removed IRM Coverage and Subject CVEs.	CVE CVEnumIRMProduction-MetricsCoverage.xml removed CVEnumIRMProduction-MetricsSubject.xml removed	Data generation and ingestion systems need to be updated to enforce the modified rule.

Change	Artifacts changed	Compatibility Notes
Added optional PM CESVersion attribute to IRM attribute group.	Schema IC-IRM.xsd updated. Schematron IRM_ID_00084 added. IRM_ID_00085 added.	Data generation and ingestion systems need to be updated to enforce the modified rule.

B.3 - V2014-DEC Change Summary

The following table summarizes the changes made to V12 in developing 2014-DEC.

Table 11 - Data Encoding Specification V2014-DEC Change Summary

Change	Artifacts changed	Compatibility Notes
Corrected rule text replacing the mention of attribute @ddms:type with @ddms:value, since ddms:type doesn't have an attribute named @ddms:type, and the rule assertion is actually looking for @ddms:value.	Schematron IRM-ID-00046 revised IRM-ID-00053 revised IRM-ID-00070 revised IRM-ID-00071 revised	No change to actual code, only changes to the rule text that is rendered.
Made changes to IRM Production Metrics Coverage to match it to high-side version of country names that apply to Production Metrics values. Full details of changes available.	CVEnumProduction-MetricsCoverage.xml changed	Data generation and ingestion systems need to be updated to enforce the modified rule.
Made changes to IRM Production Metrics Subject to update ECFS to Economic Stability and Threat Finance and resorted list to match ordering in USG list.	CVEnumProduction-MetricsSubject.xml changed	Data generation and ingestion systems need to be updated to enforce the new rules.
Wrapped DateListYearRangeRule and DateYearRangeRule abstract Schematron rules in patterns to better conform with Schematron requirements.	DateListYearRangeRule and DateYearRangeRule changed	Data generation and ingestion systems need to be updated to incorporate the rule changes.
Revised rule IRM_ID_00049 to correct use of attributes on ddms:subDivisionCode rule (using codespace and code instead of qualifier and value).	Schematron IRM-ID-00049 changed	Data generation and ingestion systems need to be updated to enforce the modified rule.

Change	Artifacts changed	Compatibility Notes
Changed DESVersion to represent the year and month of release. Also allowed for extension of specification by adding a '-' followed by a string to denote a custom implementation.	DES Schema Schematron IRM-ID-00079 changed IRM-ID-00080 changed	Data generation and ingestion systems need to be updated to enforce the modified rules.
Corrected qualifiers listed in section 2.2.5 of the DES bringing them into consistent alignment with CVE namespaces and their use in Schematron. Also, corrected a bad qualifier usage in IRM-ID-00041. Corrected typo in URN of CVEnum-IRMPostitiveIntel.	DES CVEnum-IRMPositiveIntel.xml Schematron IRM-ID-00041 changed	Data generation and ingestion systems need to evaluated the effect of these changes on their system and updated as necessary.
Added rule IRM-ID-00083 requiring a DDMS assertion if an IRM Trusted Data Object structured statement exists.	Schematron IRM-ID-00083 added	Data generation and ingestion systems need to be updated to enforce the new rule.

B.4 - V12 Change Summary

Significant drivers for Version 12 include:

- Use of GENC for country codes
- Full implementation of DNI Negroponte Revision/Recall Memorandum

The following table summarizes the changes made to V11 in developing V12.

Table 12 - Data Encoding Specification V12 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated the IRM Schematron to import the IC-GENC specification and use the IC-GENC abstract rule to enforce allowable values for country codes.	Schematron IC-IRM-ID-00031 Changed	Data generation and ingestion systems need to be updated to enforce the modified rule.
Added a schematron rule to prevent use of the ddms:revisionRecall element which is now replaced by the new RevRecall.XML specification.	Schematron IC-IRM-ID-00082 Added	Data generation and ingestion systems need to be updated to enforce the new rules.

B.4.1 - V12 Change Errata

The following table summarizes the changes that were discovered to have been omitted from the original publication of V12.

Table 13 - Data Encoding Specification V12 Change Errata

Change	Artifacts changed	Compatibility Notes
Change "FD&D" to "FDND".	IRM DES	Data generation and Ingestion systems need to be updated to properly enforce the change.

B.5 - V11 Change Summary

Significant drivers for Version 11 include:

- Creation of the US Agency specification

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

Table 14 - Data Encoding Specification V11 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated the IRM schema to import the US Agency specification and use the US Agency abstract rule to enforce allowable values for the agency acronym attribute for the organization element. Added the US Agency CES Version attribute to the EDH top level element.	Schema Schematron IC-IRM-ID-00052 Changed	Data generation and ingestion systems need to be updated to use the latest version of the schema and enforce the modified rule.
Added a schematron rule to ensure that the versions of the US Agency imported spec meets the minimum allowed version.	Schematron IC-IRM-ID-00080 Added	Data generation and ingestion systems need to be updated enforce the new rules.

B.6 - V10 Change Summary

Significant drivers for Version 10 include:

- Creation of the IC-ID specification

The following table summarizes the changes made to V9 in developing V10.

Table 15 - Data Encoding Specification V10 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated the IRM schematron rule that verified the format of the GUIDE ID to use the abstract rule defined in IC-ID.	Schematron IRM-ID-00062	Data generation and ingestion systems need to be updated to enforce the updated rule.
Updated the IRM schema to import the IC-ID specification and added the IC-ID DES Version attribute to the IRM assertion.	Schema	Data generation and ingestion systems need to be updated to use the latest version of the schema.

B.7 - V9 Change Summary

Significant drivers for Version 9 include:

- See ISM V10 drivers
- DDMS [4]

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

Table 16 - Data Encoding Specification V9 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated a rule checking for child nodes on the **ddms:TemporalCoverage** element to ignore **ddms:name**.	Schematron IRM-ID-00075 Changed	Data generation and ingestion systems need to be updated to enforce the modified rule.

Change	Artifacts changed	Compatibility Notes
Moved several rules from PUBS to IRM as they should be run whenever DDMS is present, not just if the XML Instance is a PUBS document.	Schematron IRM-ID-00074 Added (originally PUBS-ID-00109) IRM-ID-00075 Added (originally PUBS-ID-00088) IRM-ID-00076 Added (originally PUBS-ID-00107) IRM-ID-00077 Added (originally PUBS-ID-00105) IRM-ID-00078 Added (originally PUBS-ID-00090)	Data generation and ingestion systems need to be updated to no longer enforce the removed rules, and instead upgraded to enforce the IRM versions.
Added a new CVE to define an enumeration for Positive Intel values. Created schematron rules to enforce that if an element of **ddms:type** is qualified as a Positive Intel value, the attribute **ddms:value** is defined within the CVE.	CVEnumIRMPositiveIntel Schematron IRM-ID-00073 Added	Data generation and ingestion systems will have to recognize the qualifier for Positive Intel and enforce the schematron rule that confirms the values are valid.
The refactoring of the DDMS card to be a TDO with a DDMS assertion removed the need for the **ddms:publisher**, **ddms:language**, **ddms:productionMetric**, **ddms:title**, **ddms:creator**, **ddms:contributor**, and **ddms:pointOfContact** to be defined within the DDMS structure. These values are now stored in the Payload scoped Handling Assertion's EDH and are required by the schema. The business rules previously enforcing that these values be defined if MIN_DISCOVERABLE_OR_GREATER have been removed.	Schematron IRM-ID-00035 Removed IRM-ID-00038 Removed IRM-ID-00039 Removed IRM-ID-00056 Removed IRM-ID-00061 Removed	Data generation and ingestion systems will have to be updated to no longer enforce that rule.

Change	Artifacts changed	Compatibility Notes
The refactoring of the DDMS card to be a TDO with a DDMS assertion allows that TDO to contain an inline payload. The rules previously enforcing that a DDMS card had ism markings for external references has been removed.	Schematron IRM-ID-00066 Removed IRM-ID-00067 Removed	Data generation and ingestion systems will have to be updated to no longer enforce those rules.
The refactoring of the DDMS card to be a TDO with a DDMS assertion removed the need for the IC-ID for the resource and the DDMS card to be defined within the DDMS structure. The IC-ID for the complete DDMS card, originally in **ddms:metacardInfo/ ddms:identifier**, is now defined in the Identifier element in the TDO scoped Handling Assertion's EDH for the TDO. The IC-ID for the resource, originally in **ddms:resource/ddms:identifier**, is now defined in the Identifier element in the Payload scoped Handling Assertion's EDH. The business rules previously enforcing the existence of those IC-IDs have been removed.	Schematron IRM-ID-00012 Removed IRM-ID-00014 Removed	Data generation and ingestion systems will have to be updated to no longer enforce those rules.
The regular expression to check the GUIDE id was updated to ensure that there are no additional characters before or after the id.	Schematron IRM-ID-00062 Changed Examples	Data generation and ingestion systems complying with the GUIDE id rules do not need to be updated. Systems that were allowing invalid GUIDE ids will need to be updated to comply with the constraint rule.
IRM is now designed to live inside of a TrustedDataObject resulting in DDMS being removed from the Schema. As part of this change, all schematron rules were updated with xpaths for the new format.	Schema Schematron	Data generation and ingestion systems will have to be updated to handle the new TDO formatted IRM instances.

Change	Artifacts changed	Compatibility Notes
DDMS now resides in a peer assertion within the a TrustedDataObject.	Schematron	Data generation and ingestion systems will have to be updated to handle the new TDO formatted IRM instances.
Added check to require **ddms:start** dateTime be less than **ddms:end** dateTime for **ddms:searchableDate**.	IRM-ID-00072 Added	Data generation and ingestion systems need to be updated to use the additional rule.
Fixed bug in IRM-ID-00010 to not error in the edge case where attribute **ddms:value** contains the empty string.	IRM-ID-00010 Changed	Data validation systems should update to include the syntax improvement.
Updated MIME Types to current IANA list + DNI types +application/x-autocad.	CVEnumIRMMimeType	Data generation and ingestion systems will have to be updated to handle the new mime values.
Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISM v9+, NTK V7+, ARH V1+, TDF V1+, and EDH V1+.	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.
Updated Schema to ISM V10.	Schema	Updated the Schema itself to use ism:DESVersion to 10 to mark the xsd schema instance with classification markings.
Adopt GENC [7] as the only Country code list for IRM.	IRM-ID-00001 Removed CVEnumIRMCoverage-FIPSDigraph Removed CVEnumIRMCoverage-ISO3166Trigraph Changed CVEnumIRMCoverage-ISO3166Trigraph Changed	Data generation and ingestion systems will have to be updated to support the current CVE values.
Remove ORCON POC related rules as ISM.XML.V10 removed ORCON POC.	Schematron IRM-ID-00037 Removed	Data generation and ingestion systems need to be updated to no longer use rule
Updated Schema to ISM V10.	Schema	Updated the Schema itself to use ism:DESVersion to 10 to mark the xsd schema instance with classification markings.

Change	Artifacts changed	Compatibility Notes
Update to use VIRT instead of IC Common for virtual coverage concepts.	Schematron Removed IRM-ID-00069	Data generation and ingestion systems need to be updated to no longer use this rule
Update rule to enforce that attribute @ism:excludeFromRollup must not be specified for any element in the namespace [urn:us:mil:ces:metadata:ddms:5] in a TDF IRM assertion.	Schematron Removed IRM-ID-00025	Data generation and ingestion systems need to be aware of this rule
Add Cabinet Offices to CVEnum-IRMAgencyAcronym.	CVE	Data generation and ingestion systems need to be updated to use the correct CVE definitions and values.

B.7.1 - V9 Change Errata

The following table summarizes the changes that were discovered to have been omitted from the original publication of V9.

Table 17 - Data Encoding Specification V9 Change Errata

Change	Artifacts changed	Compatibility Notes
Removed Schematron rules	Schematron Removed IRM-ID-00003	Data generation and ingestion systems need to be updated to properly enforce the new constraint rules.

B.8 - V8 Change Summary

Significant drivers for Version 8 include:

- See ISM V9 drivers
- DDMS [4]
- IC Cloud

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

Table 18 - 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.
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 ingestion) 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 ingestion 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 existing 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.9 - 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 19 - 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 IRM-ID-00018 Removed	Data generation and ingestion systems need to be updated to properly handle the greater precision now possible.

B.10 - V6 Change Summary

Significant drivers for Version 6 include:

- DDMS [4] / IRM Harmonization

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

Table 20 - 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[4] **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.11 - 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[30]

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

Table 21 - 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[4] and enforce specific IC constrains with new Schematron[35] 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[39] 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 [32] memos and points-of-contact by extending DDMS [4] 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.[30]	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[28] 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.12 - 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 22 - Data Encoding Specification V4 Change Summary

Change	Artifacts changed	Compatibility Notes
Changed encoding of constraint rules from text to Schematron.[35]	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[28] 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.[28]	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[27] 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.[18]	IRM-ID-00026 Removed	Data generation and Ingestion systems need to be updated to no longer enforce this constraint.

B.13 - V3 Change Summary

Significant drivers for Version 3 include:

- See ISM V5 drivers
- Executive Order 13526[6]
- National HUMINT Director for several new markups

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

Table 23 - Data Encoding Specification V3 Change Summary

Change	Artifacts changed	Compatibility Notes
Uses ISM V5.	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule.
Added 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.
Removed Appendix H Reading the Schematics.	Documentation	Knowledge of how to interpret these schema images is common making this appendix unnecessary.
Added support for expressing coverage of NonState Actors.	Documentation Schema	Data generation and Ingestion systems need to be updated to properly support new elements.

B.14 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V4 drivers
- Executive Order 13526[6]
- CAPCO Register and Manual[3]

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

Table 24 - 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:IC-ResourceMetadataPackage**.

Appendix C List of Abbreviations

This appendix lists all the acronyms and abbreviations referenced in this encoding specification.

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CES	Controlled Vocabulary Enumeration Encoding Specification
CIA	Central Intelligence Agency
CVE	Controlled Vocabulary Enumeration
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOS	U.S. Department of State
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
FOUO	For Official Use Only
GENC	Geopolitical Entities, Names, and Codes
HTML	HyperText Markup Language
HUMINT	Human Intelligence
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
IC-ID	IC Identifier

ICD	Intelligence Community Directive
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INTDIS	Intelligence Discipline
IRM	Information Resource Metadata
ISM	Information Security Markings
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
IT	Information Technology
LIC	License
MIME	Multipurpose Internet Mail Extensions
MN	Mission Need Profile
NCTC	National Counterterrorism Center
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
ORCON	See OC.
PM	Production Metrics
PUBS	Intelligence Publications
RFC	Request for Comments
TDF	Trusted Data Format
TDO	Trusted Data Object
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URL	Uniform Resource Locator

VIRT	Virtual Coverage
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

Bibliography

[1] ABNF
Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.
Available online at: http://tools.ietf.org/html/std68
Also known as: http://www.ietf.org/rfc/rfc5234.txt

[2] ADD
Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.
Available online Intelink-TS at: http://go.ic.gov/soSC6M8
Available online Intelink-U at: https://w3id.org/ic/standards/ADD
Available online at: https://w3id.org/ic/standards/public

[3] CAPCO Register and Manual V3.1
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*. Version 3.1. 7 May 2010.

[4] DDMS
Department of Defense. *DoD Discovery Metadata Specification*.
Available online at: http://metadata.ces.mil/dse/irs/DDMS/

[5] DoD Instruction 8310.01
DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf

[6] 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

[7] GENC
Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 3.0.
Available online Intelink-TS at: http://go.ic.gov/QWkfrXy
Available online at: https://geo.aitcnet.org/NSGREG/genc/discovery

[8] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: http://go.ic.gov/4X6TOc1

[9] IC-EDH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Data Header (IC-EDH.XML)*.
Available online Intelink-TS at: http://go.ic.gov/TQjVx3d
Available online Intelink-U at: https://w3id.org/ic/standards/EDH

Available online at: https://w3id.org/ic/standards/public

[10] IC-GENC.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES)*.
Available online Intelink-TS at: http://go.ic.gov/QWkfrXy
Available online Intelink-U at: https://w3id.org/ic/standards/GENC
Available online at: https://w3id.org/ic/standards/public

[11] IC-ID.XML
Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.
Available online Intelink-TS at: http://go.ic.gov/mQ4IUDk
Available online Intelink-U at: https://w3id.org/ic/standards/IC-ID
Available online at: https://w3id.org/ic/standards/public

[12] IC-TDF.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (TDF.XML)*.
Available online Intelink-TS at: http://go.ic.gov/sonBSai
Available online Intelink-U at: https://w3id.org/ic/standards/TDF
Available online at: https://w3id.org/ic/standards/public

[13] ICD 206
Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Analytic Products*. Intelligence Community Directive 206. 22 January 2015.
Available online at: http://www.dni.gov/files/documents/ICD/ICD%20206.pdf

[14] ICD 208
Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.
Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[15] ICD 209
Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.
Available online at: http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf

[16] ICD 500
Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.
Available online Intelink-TS at: http://go.ic.gov/5Ot5sbK
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[17] ICD 501
Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.
Available online Intelink-TS at: http://go.ic.gov/GG61roi

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[18] ICD 710
Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[19] ICPG 710.1
Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at: http://go.ic.gov/0d147Ee
Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf

[20] ICPM 2007-200-2
Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2 . 11 December 2007.
Available online at: http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf

[21] 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 Intelink-TS at: http://go.ic.gov/sLKNq3N
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-20

[22] 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 Intelink-TS at: http://go.ic.gov/cWyv9nw
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-21

[23] 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

[24] INTDIS.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Intelligence Discipline (INTDIS.CES)*.
Available online Intelink-TS at: http://go.ic.gov/oQWEPEl
Available online Intelink-U at: https://w3id.org/ic/standards/INTDIS
Available online at: https://w3id.org/ic/standards/public

[25] Intelligence Community
Director of National Intelligence. *Members of the IC*.
Available online at: http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

[26] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at: http://go.ic.gov/3oipfOY
Available online Intelink-U at: https://w3id.org/ic/standards/ISM
Available online at: https://w3id.org/ic/standards/public

[27] 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

[28] 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

[29] Jelliffe
Richard Alan Jelliffe. *FAQ*. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?.
Available online at: http://www.schematron.com

[30] 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

[31] MIME.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Media Type (MIME.CES)*.

[32] ORCON Memo
Director of National Intelligence. *Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities*. 29 March 2011.

ICPG 710.1 signed July 2012[19], rescinded the ORCON Memo.
Available online at: https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/Guiding%20Principles%20for%20Use%20of%20the%20ORCON%20Markings_ES%2000045.pdf
Attachment A: https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20A.pdf
Attachment B: https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20B.pdf
Attachment C: https://intelshare.intelink.gov/sites/a2/csa/Publications%20and%20Manuals/ICD,%20ICPG%20and%20ICS/IC%20Information%20Security/ORCON/DNI%20ORCON%20Memo%20Attach%20C.pdf

[33] Oxygen

SyncRO Soft. *<oXygen/> XML Editor*.
Available online at: http://www.oxygenxml.com/

[34] PM.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for Production Metrics (PM.CES)*.
Available online Intelink-TS at: http://go.ic.gov/tUfhLVI
Available online Intelink-U at: https://w3id.org/ic/standards/PM
Available online at: https://w3id.org/ic/standards/public

[35] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
ISO Spec Available online at: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
StyleSheets for compiling Available online at: http://code.google.com/p/schematron/

[36] TAG-9-Jan-2006
W3C Technical Architecture Group (TAG). *The Disposition of Names in an XML Namespace*. 9 January 2006.
Available online at: http://www.w3.org/2001/tag/doc/namespaceState.html

[37] USAgency.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.
Available online Intelink-TS at: http://go.ic.gov/MmBEpFU
Available online Intelink-U at: https://w3id.org/ic/standards/USAgency
Available online at: https://w3id.org/ic/standards/public

[38] WEBARCH-15-Dec-2004
W3C. *Architecture of the World Wide Web, Volume One*. 15 December 2004.
Available online at: http://www.w3.org/TR/webarch

[39] 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/

[40] 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

[41] XML Catalogs
The Organization for the Advancement of Structured Information Standards [OASIS]. *XML Catalogs*. Committee Specification 06 Aug 2001.
Available online at: https://www.oasis-open.org/committees/entity/spec-2001-08-06.html

[42] 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/

[43] 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 the following DNI-sponsored web sites.

Public Website: https://w3id.org/ic/standards/public

Intelshare: https://w3id.org/ic/standards/data-specs

Direct all inquiries about this IC technical specification, IC technical specification collaboration and coordination forums, or IC element representatives involved in those forums, to the IC CIO.

E-mail: ic-standards-support@iarpa.gov.

Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.[21]