
# Intelligence Community Technical Specification

# CVE Encoding Specification for Intelligence Discipline

## Version 2017-JUL

July 21, 2017

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1 - Introduction

## 1.1 - Purpose

This *CES CVE Encoding Specification* for Intelligence Discipline (INTDIS.CES) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode Intelligence Discipline (INTDIS) controlled vocabulary. The INTDIS.CES vocabulary defines values that are valid intelligence disciplines as well as each discipline's components and component techniques. This CVE Encoding Specification (CES) defines the CES elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing data concepts.

## 1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This CES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the CES 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* [10] 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* [15] 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[9] defines a plain-text format for IC Identifiers as well as an associated XML structure.

## 1.4 - Enterprise Need

Many IC encoding specifications use Controlled Vocabulary Enumerations (CVEs) to define allowable values for various elements and attributes. Over time, several encoding specifications became dependent on the same list of values, and dual (or more) maintenance was required to keep the lists aligned. Additionally, any changes to a specification's CVEs caused an entire new version of that specification to be created. In order to remove the need for dual maintenance and to remove the need to revision a specification when a CVE was updated, a new type of encoding specification, the CVE Encoding Specification, was created to decouple the vocabulary from the specifications. Each CES contains one or more CVEs and optionally a master schema defining elements and attributes limited to the allowable values.

This CES defines the Intelligence Discipline (INTDIS) CVE and contains valid values for use by the PUBS and IRM specifications.

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[6]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[10]
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[11]

## 1.5 - Audience and Applicability

CESs are primarily intended to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described.

The 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,* [14] 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*,[3] 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.” [16] 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 |
|---|---|
| ism | urn:us:gov:ic:ism |
| xsd | http://www.w3.org/2001/XMLSchema |

## 1.7 - Dependencies

### 1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational

relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

| | |
|---|---|
| Dependency | Directly or transitively influenced by.<br><br>Examples:<br><br>1. A is influenced by B therefore B is a dependency of A.<br><br>2. A is influenced by B and B is influenced by C; therefore C is a dependency of A. |
| Direct Dependency | Explicit influence.<br><br>Example: A influences B. |
| Inverse Dependency | Directly or transitively influences.<br><br>Example: B influences A. |

## 1.7.2 - Specification 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.

### Table 2 - Dependencies

| Name | Dependency Description |
|---|---|
| 22 October 2013, JP 2-0, Joint Intelligence[18] | Policy Driver |
| Value enumerations used for several XML structures are defined in the various controlled vocabulary enumerations included in this CES. | Specification uses CVEs to encode controlled vocabularies. The use of the INTDIS CVEs is normative. |

## 1.7.3 - Inverse Dependencies

Generally, it is only necessary to think of the *direct dependencies* (see Direct Dependency) in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies* (see Inverse Dependency), for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies.

Since this specification is one such specification that is used by other specifications released by the IC CIO, the Figure 1 has been included to assist readers in understanding all of the dependency relationships and how changes in a specification may impact others. This diagram is representative of dependencies at the time of the release of this specification, but are subject to change over time.

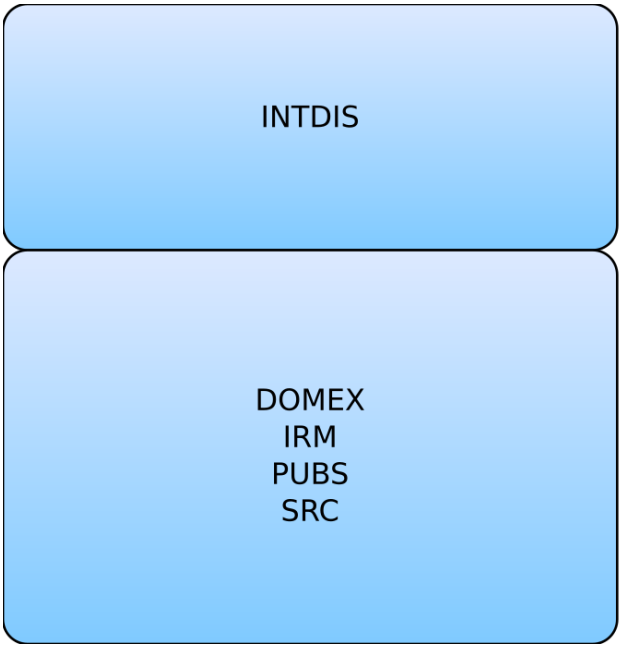


**Figure 1 : Inverse Dependency Specifications**

## 1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron[20] 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[16] 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.[24] 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.”[21] 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.”[22]

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. Revisions to a version of the specification also use a year-month structure (e.g., YYYY-MMM). 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["." Revision ] ["-" CustomizationSuffix ]
[2]        VersionYear : := 4( DIGIT )
[3]       VersionMonth : := 2( DIGIT )
[4]  CustomizationSuffix : := 1*23(ALPHA / DIGIT / "_" )
[5]       RevisionYear : := 4( DIGIT )
[6]      RevisionMonth : := 2( DIGIT )
[7]           Revision : := Year Month
```

### 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/revision being referenced. |
| VersionYear | The four digit year from the version of the specification being referenced. |
| VersionMonth | 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. |
| RevisionYear | The four digit year from the revision of the specification being referenced. |
| RevisionMonth | The 2 digit month from the revision of the specification being referenced. |
| Revision | The Year and Month from the revision of the specification being referenced. Revisions are modifications to Versions. |

# 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. In particular, situations for which there is not clearly a single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers of this CES are encouraged to contact the maintainers of this CES for further guidance when necessary.

There are two ways in which a consumer requiring a INTDIS can use the INTDIS.CES specification: through referencing objects defined in the schema or enforcing the format via running their own Schematron.

### 2.2.1 - Usage of the INTDIS Schema

The INTDIS.CES schema defines an element (**intdis:IntelDiscipline**) and an attribute (**@intdis:intelDiscipline**) that enforces the allowable values as defined in the specification's CVE (see Section 3.7.3 - Value Enumeration Constraints for more details). Consumers of the INTDIS.CES specification should import the INTDIS schema and reference the element or attribute, depending on what is needed. Note: the names for the element and the attribute are similar because the content is the same, i.e., both limit the value to the INTDIS CVE, but the expectation on usage is that the consumer would use one or the other. The difference in capitalization is because they follow the IC naming standards, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

## 2.3 - CSV Notes

There are Comma Separated Value files provided for all of the CVEs. They are in the CVE folder with the XML and JSON versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence.

### Important

The CSV files on many systems will open “automatically” in Microsoft Excel; the default opening however, will not correctly read UTF-8 special characters. These are found in some country names such as “Republic of Côte d’Ivoire”. If you need to use a CVE that contains such special characters, or you think may contain such characters in Excel, you should:

- Open Excel to a blank sheet
- Under the Data menu choose to get external data from a text file
- Choose UTF-8 as the file origin
- Choose delimited as the format
- Choose next
- Change from tab to Comma as the delimiter
- Finish import to get the data in with the UTF-8 Characters properly encoded in Excel.

## 2.4 - JSON Notes

There are JSON format files provided for all of the CVEs. They are in the CVE folder with the XML and CSV versions of the information. They are provided to assist developers using the CVEs; the specifications do not use them at this moment. There are no new requirements because of their existence. The JSON files are formatted using JSON-LD based on a proposed method for JSON in NIEM.

# 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 security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710[12] implemented in the IC Markings System Register and Manual,[7] ISOO 32 CFR Parts 2001 and 2004 (as of September 22, 2003),[17] E.O. 13526, as amended,[5] and E.O. 12829, as amended.[4] These rules will be expanded and modified as the model matures, the IC Markings System Register and Manual [8] is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

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

## 3.3 - 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. INTDIS.CES data validation constraint rule identifiers are prefixed with "INTDIS-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 Table 3. 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 INTDIS.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which CES 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 - 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.

## 3.7.3 - Value Enumeration Constraints

Several elements and attributes of the INTDIS.CES model use 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. An appropriate CVE will be provided for use on networks where the list may be reduced or expanded as necessary. If the processing will occur on a network where the provided CVE is not appropriate, the differentiated CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

Developers of systems processing Sensitive Compartmented Information or data related to Special Access Programs from the unpublished register will need to contact the point of contact listed in Appendix E - Points of Contact for guidance as those values may have been omitted from the CVE.

As noted in the specific rules, a failure of validation against a CVE will generate an Error.

## 3.7.4 - Additional Constraints

## 3.7.4.1 - CES Constraints

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

## 3.7.5 - Constraint Rules

There are no Schematron rules defined for INTDIS.CES at this time.

[1] “White space” is defined in XML 1.0[23] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

# 3.8 - Data Rendering Constraint Rules

## 3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of INTDIS.CES documents. The intent is to inform the development of systems capable of rendering or displaying INTDIS.CES data for use by individuals not familiar with the details of the INTDIS.CES 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 INTDIS.CES 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.

# Chapter 5 - Generated Guides

## 5.1 - Schema Guide

The detailed description and reference documentation for the INTDIS.CES 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 INTDIS.CES schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen®,* [19] 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.

## Appendix A Feature Summary

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

### Table 5 - Feature Summary Legend

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

# A.1. INTDIS Feature Comparison

### Table 6 - INTDIS Feature Comparison

| Required date | Feature | V2015-AUG | V2016-SEP | V2017-JUL |
|---|---|---|---|---|
| | Defines the allowable values for Intelligence Discipline | F | F | F |
| | Defines the allowable values for Intelligence Discipline Components and Component Techniques. | N | F | F |
| | Updated the allowable values for Intelligence Discipline Components and Component Techniques for the MASINT Discipline. | N | N | F |

# Appendix B Change History

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

### Table 7 - CES Version Identifier History

| Version | Date | Purpose |
|---|---|---|
| 2015-AUG | 13 August 2015 | Initial Release |
| 2016-SEP | 9 September 2016 | Routine revision to technical specification. For details of changes, see Section B.2 - 2016-SEP Change Summary |
| 2017-JUL | 21 July 2017 | Routine revision to technical specification. For details of changes, see Section B.1 - 2017-JUL Change Summary |

## B.1 - 2017-JUL Change Summary

Significant drivers for Version 2017-JUL include:

- Updates to align with the MASINT functional Manager guidance for MASINT values.

The following table summarizes the changes made to 2016-SEP in developing 2017-JUL.

### Table 8 - Data Encoding Specification 2017-JUL Change Summary

| # | Change | Artifacts Changed | Compatibility Notes |
|---|---|---|---|
| 1 | Reworked INTDIS CVEs to match the revised MASINT Controlled Vocabulary (CV) 3.01 (CR-2016-066)<br>• Removed abbreviations for Geophysical and Radio frequency<br>• Significant rework to MASINT sub-disciplines | CVEs<br>CVEnum-INTDISDisciplines modified<br>CVEnum-INTDISDisciplineComponents modified | Systems may need to be updated to handle new/updated values. |
| 2 | Create JSON version of CVEs in INTDIS (CR-2017-055) | CVEs | No impact to systems. |
| 3 | Create CSV version of CVEs in INTDIS (CR-2017-033) | CVEs | No impact to systems. |
| 4 | Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-113) | Documentation | No impact to systems. |

| # | Change | Artifacts Changed | Compatibility Notes |
|---|---|---|---|
| 5 | Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-237) | Documentation | No impact to systems. |

## B.2 - 2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Migration of additional intelligence discipline related CVEs from IRM to INTDIS.
- Updates to better match the joint publication source document for INTDIS in accordance with Deputy Director of National Intelligence for Intelligence Integration (DDII) guidance.

The following table summarizes the changes made to v2015-AUG in developing 2016-SEP.

### Table 9 - Data Encoding Specification 2016-SEP Change Summary

| Change | Artifacts Changed | Compatibility Notes |
|---|---|---|
| Created INTDIS CVEs for Intelligence Discipline Components and Component Techniques. (CR-2015-098) | CVE<br><br>CVEnum-INTDISDisciplineComponents added.<br><br>CVEnum-INTDISDisciplineComponentTechniques added. | Systems may need to be updated to handle new/updated values. |
| Reworked INTDIS CVEs to better match joint publication source document. (CR-2015-098) | CVE<br><br>CVEnum-INTDISDisciplines had new value added.<br><br>CVEnum-INTDISDisciplineComponents had significant rework. | Systems may need to be updated to handle new/updated values. |
| Added element and attributes to support intelligence discipline components and component techniques. (CR-2015-098) | Schema | Systems may need to be updated to handle new/updated values. |

| Change | Artifacts Changed | Compatibility Notes |
|---|---|---|
| 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 CES. | Schema | No impact to systems. |
| Removed schematron. There was only an abstract pattern and the CMSTT has decided that abstract patterns should not be referenced across specifications. (CR-2015-020) | Schematron | Systems that used the abstract pattern will have to implement in their own specification. |
| 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. |

# Appendix C List of Abbreviations

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

| | |
|---|---|
| ADD | Abstract Data Definition |
| CES | Controlled Vocabulary Enumeration Encoding Specification |
| CFR | Code of Federal Regulations |
| CMSTT | Common Metadata Standards Tiger Team |
| CVE | Controlled Vocabulary Enumeration |
| DNI | Director of National Intelligence |
| E.O. | Executive Order |
| FOUO | For Official Use Only |
| HTML | HyperText Markup Language |
| 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 |
| ICD | Intelligence Community Directive |
| ICS | Intelligence Community Standard |
| IETF | Internet Engineering Task Force |
| INTDIS | Intelligence Discipline |
| IRM | Information Resource Metadata |
| ISM | Information Security Markings |
| ISOO | Information Security Oversight Office |
| IT | Information Technology |
| JSON | JavaScript Object Notation |
| JSON-LD | JavaScript Object Notation for Linked Data |
| NIEM | National Information Exchange Model |

| | |
|---|---|
| OCIO | Office of the Intelligence Community Chief Information Officer |
| ODNI | Office of the Director of National Intelligence |
| PUBS | Intelligence Publications |
| RFC | Request for Comments |
| TDF | Trusted Data Format |
| XML | Extensible Markup Language |
| XPath | XML Path Language |
| XSL | Extensible Stylesheet Language |

# 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] DoD Instruction 8310.01
DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/831001p.pdf

[4] E.O. 12829
The White House. *Executive Order 12829 – National Industrial Security Program, as Amended*. Federal Register, Vol. 58, No. 240. 16 December 1993.
Available online at: http://www.archives.gov/isoo/policy-documents/eo-12829.html

[5] 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

[6] 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

[7] IC Markings
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.
Available online Intelink-TS at: http://go.ic.gov/5DjqqWz
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings [https://w3id.org/ic/standards/policy/icmarkings ]

[8] IC Markings DEC 2014
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2014.
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] ISOO 32 CFR Parts 2001 and 2004

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information (Directive No. 1); Final Rule*. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 28, No. 183. 22 September 2003.
Available online at: https://www.gpo.gov/fdsys/pkg/FR-2003-09-22/pdf/03-24047.pdf

[18] 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

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

[20] 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/

[21] 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

[22] 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

[23] 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

[24] 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

# 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.[14]