
# Intelligence Community Technical Specification

# XML Data Encoding Specification for Enterprise Data Header

## Version 3

10 April 2013

# Table of Contents

# List of Tables

# Chapter 1 - Introduction

## 1.1 - Purpose

This *XML Data Encoding Specification for Enterprise Data Header* (EDH.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode EDH 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 enterprise data header data concepts using XML.

## 1.2 - Scope

This specification is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This DES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the DES should be closely scrutinized and differences separately documented and assessed for applicability.

## 1.3 - Background

The IC Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [6] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture (IC EA).
- Lead the IC's identification, development, and management of IC enterprise standards.
- Incorporate technically sound, deconflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common IT standards, protocols, and interfaces; to establish uniform information security standards; and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces, support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in ICS 500-21,[11] the extensive and consistent use of Extensible Markup Language (XML) within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC's data discovery, data sharing, and interoperability goals.

A DES specifies how to implement the abstract data elements in the IC.ADD in a particular physical encoding (e.g., data or file format). For example:

- DESs for textual markup formats, such as Extensible Markup Language (XML) and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.

- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.

- DESs for application-specific formats, for e.g. Microsoft Word, define document properties; styles; fields; cardinalities; processing requirements; and use.

## 1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information assurance metadata (including enterprise data headers) to allow interagency access control, automated exchanges, and appropriate protection of shared intelligence. A structured, verifiable representation of security metadata bound to the intelligence data is required in order for the enterprise to become inherently "smarter" about the information flowing in and around it. Such a representation, when implemented with other data formats, improved user interfaces, and data processing utilities, can provide part of a larger, robust information assurance infrastructure capable of automating some of the management and exchange decisions today being performed by human beings.

The Intelligence Community (IC) has standardized the various classification and control markings established for information sharing within the Information Security Markings (ISM), Need-To-Know (NTK), and Access Rights and Handling (ARH) XML specifications of the Intelligence Community Enterprise Architecture (ICEA) Data Standards. The IC Enterprise Data Header XML specification further expands on this body of work, adapting and extending it as necessary to meet mission-unique needs. By specifying a data object's header information required for exchange on the IC Enterprise, EDH ensures a secure method of information sharing and discovery, supporting use cases such as the IC Cloud.

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[2]
- 500 Series:
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[7]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[11]
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[4]

- Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[5]
- Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide[9]

## 1.5 - Audience and Applicability

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

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*,[10] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

## 1.6 - Conventions

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

The keywords "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this technical specification are to be interpreted as described in the IETF RFC 2119.[12] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

## 1.7 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in the following table. The documents listed below are referenced in this Data Encoding Specification, and are normative or informative as indicated in the dependencies table.

### Table 1 - Dependencies

| Name | Dependency Description |
|---|---|
| *XML Data Encoding Specification for Access Rights and Handling* (ARH.XML.V1+)[1] | Depends on Access Rights and Handling(ARH) Specification. Starting with ARH v1, the version of ARH imported is no longer normative, so any ARH version 1 or above may be used. |
| *XML Data Encoding Specification for Intelligence Community Identifier* (IC-ID.XML.V1+)[3] | Depends on Intelligence Community Identifier (IC-ID) Specification. Any IC-ID version 1 or above may be used. |
| International Organization for Standardization (ISO) Schematron [14]implementation by Rick Jelliffe (2010-04-14) | Specification uses Schematron to encode IC business rules for this specification. Conformance to the logic of the business rules is normative, whereas use of the schematron language to encode them is informative. |
| Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations (CVE) included in this DES. | Specification uses CVEs to encode controlled vocabularies. The use of the EDH CVEs is normative. |

## 1.7.1 - Dependencies required to download for Standalone Package

The standalone packaging of this specification does not include the specifications that it is dependent on since the version that may be used could be later than this packaging. There is a convenience packaging of the specification that includes all the most recent versions of the dependent specifications at the time it's generated. It is anticipated that this convenience package will be updated when any of the dependent specifications change but it will not be signed as a formal package. Links given here are to IntelLinkU since other networks links should look similar but we do not have the stability of Persistent Uniform Resource Locator (PURL) on other networks to ensure the links remain functional over time. These packages will have to be downloaded and copied into the appropriate directories for paths to the schema and CVE to work. Should you mix versions of the CVE schema you will have to separate the sets of CVEs by Schema or edit the CVEs to point to the correct schema file.

- ISM.XML.V9+ http://purl.org/ic/standards/ism
- NTK.XML.V7+ http://purl.org/ic/standards/ntk
- ARH.XML.V1+ http://purl.org/ic/standards/arh
- IC-ID.XML.V1+ http://purl.org/ic/standards/IC-ID-xml

# 1.8 - Conformance

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

Normative: considered to be prescriptive and necessary to conform to the standard.

Informative: serving to instruct or enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and the Schematron[14] code version of the constraint rules are normative for this DES. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and HTML CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119[12] is considered normative within the scope of the sentence. All other parts of this document are informative.

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 [16]. 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 import different versions of dependent specifications decouples parent specifications like PUBS and TDF from changes to dependency specifications, such as ISM CVE updates. The decoupling of dependency versions is not retroactive, see the dependency table for allowed dependency versions.

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

# Chapter 2 - Development Guidance

## 2.1 - Relationship to Abstract Data Definition and other encodings

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

The mappings in the IC.ADD provide a starting point for the development of automated transformations between formats defined by the DESs. However, it should be noted that when these transformations are used between formats with different levels of detail, there might be some data loss.

## 2.2 - Additional Guidance

### 2.2.1 - EDH Structure

The IC-EDH specification incorporates all the information from the Access Rights and Handling (ARH) specification and adds a few other resource level pieces of information necessary for exchange on the IC enterprise. These additional pieces of information are the date and time the data asset was created, which organization is responsible for it in the IC enterprise, and a unique identifier which can be used to identify and locate the object in the IC enterprise. The EDH also introduces the concept of an Authorization Reference as a means of indicating a particular documented legal authorization. The use of this is optional as it is not currently used in all domains, but it is an IC enterprise concept that is expected to be adopted at the enterprise level.

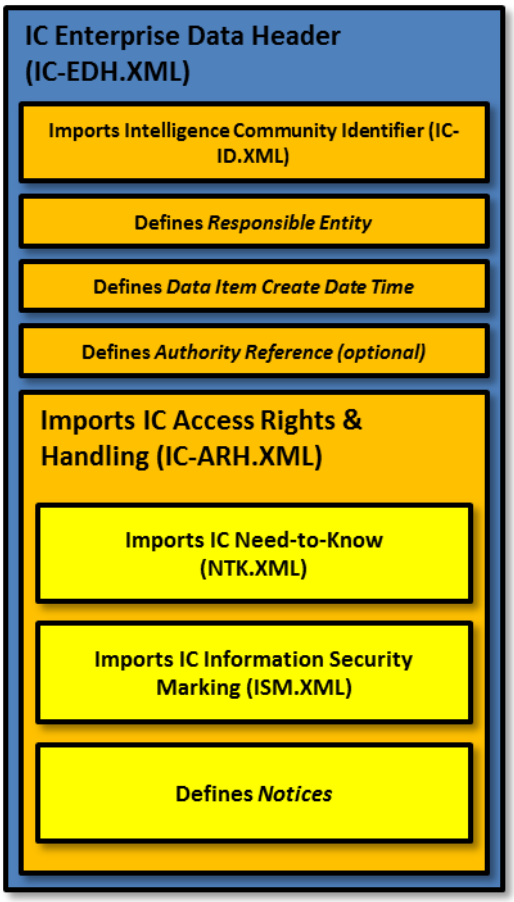


Figure 1 - A graphical representation of an EDH.

## 2.2.2 - EDH Creation Date

An Enterprise Data Header's creation date is reflected in the **@ism:createDate** attribute of the root node. This is not to be confused with the**DataItemCreateDateTime** element, which reflects the creation date of the data object referred to by the EDH.

## 2.2.3 - Internal and External EDH

Enterprise Data Headers can represent both internal and external data objects, as **Edh** and **ExternalEdh** elements, respectively. The **Edh** element is used for internal data objects present in the same instance document. **ExternalEdh** is used to represent external objects that are not in the instance document.

## 2.2.4 - EDH Elements

The IC-EDH consists of four main elements specific to EDH: **Identifier**, **DataItemCreateDateTime**, **ResponsibleEntity**, and **AuthorityReference**.

- **Identifier** - This attribute holds the IC-ID of the data object referred to by the EDH. For the purposes of the IC there needs to be a single identifier that all data objects will have; the

identifier should be unique to the data object across the whole of the IC. There is no central registry or managing body for data object identifiers across the IC so it is the responsibility of individual producers to coordinate properly.

- **ResponsibleEntity** - This element and its children elements; Country, Organization, and SubOrganization; collectively represent the creating/originating organization that is responsible for the data object.
- **DataItemCreateDateTime** - The creation date of the data object referred to by the EDH.
- **AuthorityReference** - A means of indicating a particular documented legal basis for mission activities associated with the creation, retention and use of a resource (optional).

## 2.2.5 - MIME Type

The Multipurpose Internet Mail Extensions (MIME) type for a EDH.XML document is application/dni-edh+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.

# Chapter 3 - Data Constraint Rules

## 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 to be resolved. 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 DES artifacts wherever they are located.

## 3.4 - Terminology

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

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

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

## 3.5 - 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 ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only” (FOUO). IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules. EDH.XML data validation constraint rule IDs are prefixed with “EDH-ID-”.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

## 3.7 - Data Validation Constraint Rules

### 3.7.1 - Purpose

The EDH.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[14] was selected as the language in which to encode these additional rules. The provided Schematron[14] is used to define the constraint rules; it is NOT a required implementation. Implementers can use any tools at their disposal as long as the data complies with the rules expressed. To facilitate testing and understanding of the rules they are executable in either *oXygen*® [13] or the XML Stylesheet Language for Transformation (XSLT) 2.0[18] implementation of International Organization for Standardization (ISO) Schematron[14] provided by Rick Jelliffe at http://schematron.com/ [http://schematron.com/]. Constraint rules are dependent on XPath 2.0[17] and XSLT 2.0[18] features. According to Mr. Jelliffe, the editor of Schematron[14] for ISO:

> "By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is

> run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this."

Included in the package are the ISO Schematron[14] implementation and XSLT 2.0[18] files provided as a convenience 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 — which allows for empty (or null) content. According to this specification, all required elements (and certain conditional elements) must have content, other than white space. [1] Elements, which are allowed to only have text content, must have text content specified.

## 3.7.4 - Inherited Constraints

In an instance of EDH.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 .

## 3.7.5 - Value Enumeration Constraints

Several elements and attributes of the EDH.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.

[1] "white space" is defined in XML 1.0[15] as "(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs."

## 3.7.7 - Constraint Rules

The detailed constraint rules for the EDH.XML schema can be found in a separate document inside the SchematronGuide directory, in the EDH_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 EDH.XML documents. The intent is to inform the development of systems capable of rendering or displaying EDH.XML data for use by individuals not familiar with the details of the EDH.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 EDH.XML data rendering constraint rules.

### Table 2 - Constraint Rules

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

# Chapter 4 - Conformance Validation

An instance is considered conformant with this specification if it passes all of the following normative validation steps. The following steps do not dictate how this validation strategy is implemented.

## 4.1 - Schema Validation

This first step in validation is to ensure that an instance document is compliant against the normative schema of this specification as well as those of this specification's dependencies.

If an instance is determined to be non-compliant with schema in this step then results from the future steps may be indeterminate. As such, schema compliance should always be ensured prior to taking action on results from other validation steps.

## 4.2 - Business Rule Validation

The second step in validation is to ensure that an instance document complies with the business rules expressed in this specification as well as those of this specification's dependencies. It should be noted that while the business rules for this specification are expressed in Schematron, the Schematron is informative but the constraints they express are normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the Schematron included in this specification and its dependencies.

# Chapter 5 - Generated Guides

## 5.1 - Schema Guide

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

The guide was generated with a commercially available product named *oXygen*®, produced by SyncRO Soft.

The guide provides an interactive index to:

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

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children (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 EDH.XML Schematron rules can be found in a separate document named *EDH_Rules.pdf*, which is located inside the SchematronGuide directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

## Appendix A Feature Summary

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

### Table 3 - EDH Dependency over time

| Dependent DES | V1 | V2 | V3 |
|---|---|---|---|
| ARH | V1 | V1+ | V1+ |
| ISM | V9 | V9+ | V9+ |
| NTK | V7 | V7+ | V7+ |
| IC-ID | | | V1+ |

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

### Table 4 - 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. IC-EDH Feature Summary

### Table 5 - IC-EDH Feature comparison

| IC-EDH Feature Comparison | | | | |
|---|---|---|---|---|
| **Required date** | **Feature** | **V1** | **V2** | **V3** |
| | Supports multiple versions of ISM.XML (V9 - Current), NTK.XML (V7 - Current), and ARH.XML (V1 - Current) | N | F | F |
| | Supports multiple versions of the IC-ID.XML (V1 - Current) | N | N | F |

## Appendix B Change History

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

### Table 6 - DES Version Identifier History

| Version | Date | Purpose |
|---|---|---|
| 1 | 17 July 2012 | Initial Release |
| 2 | 21 January 2013 | Routine revision to technical specification. For details of changes, see Section B.2 - V2 Change Summary |
| 3 | 5 April 2013 | Routine revision to technical specification. For details of changes, see Section B.1 - V3 Change Summary |

# B.1 - V3 Change Summary

Significant drivers for Version 3 include:

- Creation of IC-ID specification

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

### Table 7 - Data Encoding Specification V3 Change Summary

| Change | Artifacts changed | Compatibility Notes |
|---|---|---|
| Added a schematron rule to ensure that the versions of the IC-ID imported spec meets the minimum allowed version. | Schematron<br><br>IC-EDH-ID-00011 Added | Data generation and ingestion systems need to be updated enforce the new rules. |
| Updated the IC-EDH schema to import the IC-ID specification and use the IC-ID definition of Identifier instead of the element previously defined in IC-EDH. Added the IC-ID DES Version attribute to the EDH top level element. Removed the IC-EDH schematron rule that previously enforced the GUIDE ID format; this is now being done by the IC-ID schema. | Schema<br><br>Schematron<br><br>IC-EDH-ID-00007 Deleted | Data generation and ingestion systems need to be updated to use the latest version of the schema and to no longer enforce the deprecated rule. |

# B.2 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM V10 drivers

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

## Table 8 - Data Encoding Specification V2 Change Summary

| Change | Artifacts changed | Compatibility Notes |
|---|---|---|
| Added schematron rules to ensure that the versions of the imported specs meet the minimum allowed versions. | Schematron<br><br>IC-EDH-ID-00008 Added<br><br>IC-EDH-ID-00009 Added<br><br>IC-EDH-ID-00010 Added | Data generation and ingestion systems need to be updated enforce the new rules. |
| Update ISM to V10 | Schema<br><br>Constraint Rules | Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification. |
| Version decoupling, allowing import of any version of ISM and other dependent specifications at or above ISMv9, NTKv7, and ARHv1 | DES | Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation. |
| The regular expression to check the GUIDE id was updated to ensure that there are no additional characters are before or after the id | Schematron<br><br>IC-EDH-ID-00007 Changed | Data generation and ingest systems complying with the GUIDE id rules do not need to be updated.<br><br>Systems that were allowing invalid GUIDE ids will need to be updated to comply with the constraint rule. |
| Add Cabinet Offices to CVEnum-EDHOrganizationsUS | CVE | Data generation and ingestion systems need to be updated to use the correct CVE definitions and values. |

# Appendix C Acronyms

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

## Table 9 - Acronyms

| Name | Definition |
|---|---|
| A&A | Authorization and Accreditation |
| ABAC | Attribute Based Access Control |
| ABNF | Augmented Backus-Naur Form |
| ADD | Abstract Data Definition |
| API | Applications Programming Interface |
| ARH | Access Rights and Handling |
| AS | Attribute Service |
| ATO | Authority To Operate |
| BBOX | Bounding Box |
| BNF | Backus-Naur Form |
| CAPCO | Controlled Access Program Coordination Office |
| CAT | Catalog Services Interface Standard |
| CDR | Content Discovery and Retrieval |
| CF-NetCDF | Climate and Forecast - Network Common Data Format |
| CMS | Cryptographic Message Syntax |
| COMET | Completely Open Mapping Environment |
| CONOPS | Concept of Operations |
| CORBA | Common Object Request Broker Architecture |
| CQL | Common Catalog Query Language (CQL) |
| CRL | Certificate Revocation List |
| CSW | Catalog Service for Web |
| CVE | Controlled Vocabulary Enumeration |
| D & R | Discovery and Retrieval |
| DAA | Designated Approval Agent |
| DCMI | Dublin Core Metadata Initiative |
| DC MES | Dublin Core Metadata Element Set |
| DDMS | Department of Defense Discovery Metadata Specification |
| DES | Data Encoding Specification |
| DIA | Defense Intelligence Agency |

| Name | Definition |
|---|---|
| DISR | DoD Information Technology Standards and Profile Registry |
| DNS | Domain Name System |
| DOI | Digital Object Identifier |
| DN | Distinguished Name |
| DNI | Director of National Intelligence |
| EBNF | Extended Backus-Naur Form |
| EDH | Enterprise Data Header |
| E.O. | Executive Order |
| ES&IS | Enterprise Search & Integration Services |
| EPR | Endpoint Reference |
| FOUO | For Official Use Only |
| FTP | File Transfer Protocol |
| GENC | Geopolitical Entities, Names, and Codes |
| GeoRSS | Geographic Really Simple Syndication |
| GeoTIFF | Geographic Tagged Image File Format |
| GIF | Graphics Interchange Format |
| GIS | Geospatial Information System |
| GML | Geography Markup Language |
| GNS | Geographic Names Server |
| GUIDE | Globally Unique Identifiers for Everything |
| GVS | GEOINT Visualization Services |
| HDF-EOS | Hierarchical Data Format - Earth Observing System |
| HTML | HyperText Markup Language |
| HTTP | Hypertext Transfer Protocol |
| I2 | Information Integration |
| IC | Intelligence Community |
| IC.ADD | Intelligence Community Abstract Data Definition |
| IC CIO | Intelligence Community Chief Information Officer |
| IC EA | IC Enterprise Architecture |
| IC ESB | Intelligence Community Enterprise Standards Baseline |
| IC ITE | IC Information Technology Enterprise |
| ICD | Intelligence Community Directive |
| ICEA | Intelligence Community Enterprise Architecture |
| ICPG | Intelligence Community Program Guidance |
| ICS | Intelligence Community Standard |

| Name | Definition |
|---|---|
| ICSR | Intelligence Community Standards Registry |
| IdAM | Identity and Access Management |
| IDM | Interface Data Model |
| IDMView | Interface Data Model View |
| IETF | Internet Engineering Task Force |
| IOC | Initial Operating Capability |
| IP | Internet Protocol |
| IPT | Integrated Project Team |
| IRM | Information Resource Metadata |
| ISBN | International Standard Book Number |
| ISM | Information Security Marking |
| ISO | International Organization for Standardization |
| ISOO | Information Security Oversight Office |
| JPEG | Joint Photographic Experts Group |
| JPIP | JPEG 2000 Interactive Protocol |
| JSON | JavaScript Object Notation |
| JWE | JSON Web Encryption |
| JWICS | Joint Worldwide Intelligence Communications System |
| JWT | JSON Web Token |
| KA | Knowledge Assertion |
| KML | Keyhole Markup Language |
| KOS | Knowledge Organization System |
| KVP | Key Value Pair |
| LIMDIS | Limited Distribution |
| LNI | Library of National Intelligence |
| MAC | Multi Audience Collection |
| MCG&GIL | Mapping, Charting, and Geodesy Information Library |
| MCGView | Mapping, Charting, and Geodesy View |
| MIME | Multipurpose Internet Mail Extensions |
| MTOM | Message Transmission Optimization Mechanism |
| NARA | National Archives and Records Administration |
| NCES | Net-Centric Enterprise Services |
| NGA | National Geospatial Intelligence Agency |
| NGDS | Net-Centric GEOINT Discovery Services |
| NGT | Next Generation Trident |

| Name | Definition |
|---|---|
| NIPR | Non-Classified Internet Protocol Router Network |
| NITF | National Imagery Transmission Format |
| NPE | Non-Person Entity |
| NRO | National Reconnaisance Office |
| NSG | National System for Geospatial Intelligence |
| NSI | National Security Information |
| NTK | Need-To-Know Metadata |
| OCIO | Office of the Intelligence Community Chief Information Officer |
| OCSP | Online Certificate Status Protocol |
| ODNI | Office of the Director of National Intelligence |
| OGC | Open Geospatial Consortium |
| OGCA | Open Geospatial Consortium Australia |
| OGCE | Open Geospatial Consortium Europe |
| OWS | OGC Web Services |
| PAP | Policy Administration Point |
| PAYL | Payload |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| PK | Private Key |
| PKI | Public Key Infrastructure |
| PNG | Portable Network Graphics |
| PUBS | Intelligence Publications |
| PURL | Persistent Uniform Resource Locator |
| RA | Reference Architecture |
| RDBMS | Relational Database Management System |
| REST | REpresentational State Transfer |
| RFC | Request for Comments |
| RR-ID | REST Security Encoding Specification for End-to-End Identity Propagation |
| SAML | Security Assertion Markup Language |
| SIPR | Secret Internet Protocol Router Network |
| SOAP | Simple Object Access Protocol |
| SQL | Structured Query Language |
| SSD | Special Security Directorate |
| SSL | Secure Sockets Layer |
| STIL | Saint Louis Information Library |

| Name | Definition |
|---|---|
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TDC | Trusted Data Collection |
| TDF | Trusted Data Format |
| TDO | Trusted Data Object |
| TGN | Thesaurus of Geographic Names |
| TIFF | Tagged Image File Format |
| TIN | Triangulated Irregular Network |
| TLS | Transport Layer Security |
| UDDI | Universal Description, Discovery and Integration |
| UML | Unified Modeling Language |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| URN | Uniform Resource Name |
| UUID | Universal Unique Identifier |
| VIRT | Virtual Coverage |
| W3CDTF | World Wide Web Consortium Date Time Format |
| WARP | Web Based Access and Retrieval Portal |
| WCS | Web Coverage Service |
| WFS | Web Feature Service |
| WMS | Web Map Service |
| WSDL | Web Service Definition Language |
| XACML | eXtensible Access Control Markup Language |
| XML | Extensible Markup Language |
| XPath | XML Path Language |
| XPointer | XML Pointer Language |
| Xquery | XML Query |
| XSLT | XML Stylesheet Language for Transformations |

# Appendix D Bibliography

## Bibliography

[1] ARH.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.
Available online IntelLinkU at: http://purl.org/IC/Standards/ARH
Available online at: http://purl.org/IC/Standards/public

[2] 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 JWICS at: http://go.ic.gov/HvBHBmY

[3] 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 IntelLinkU at: http://purl.org/IC/Standards/ICID
Available online at: http://purl.org/IC/Standards/public

[4] 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

[5] 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 209 Tearline Production and Dissemination.pdf

[6] ICD 500
Director of National Intelligence Chief Information Officer. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[7] ICD 501
Director of National Intelligence Chief Information Officer. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[8] ICPG 710.1
Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online JWICS at: http://go.ic.gov/fU3HML

[9] ICPM 2007-200-2
Assistant Director of National Intelligence for . *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

[10] ICS 500-20
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online IntelLinkU at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[11] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online IntelLinkU at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[12] IETF-RFC 2119
Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.
Available online at: http://tools.ietf.org/html/rfc2119

[13] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*. version 14.1.
Available online at: http://www.oxygenxml.com/

[14] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
Available online at: http://www.schematron.com/

[15] 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

[16] 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

[17] 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/

[18] XSLT2
World Wide Web Consortium (W3C) . *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.
Available online at: http://www.w3.org/TR/xslt20/

# Appendix E Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Public Website: http://purl.org/ic/standards/public

E-mail: <datastandardssupport@ugov.gov> or <ic-standards-support@intelink.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.[10]