



Intelligence Community Technical Specification

XML Data Encoding Specification for Enterprise Data Header

Version 2016-SEP

September 9, 2016

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	2
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - Terminology	3
1.6.4 - XML Namespaces	4
1.7 - Dependencies	4
1.7.1 - Standalone and Convenience Packages	7
1.8 - Conformance	7
1.9 - Version Policies	7
1.9.1 - XML Namespace Policy	7
1.9.2 - Version Numbering	8
Chapter 2 - Development Guidance	10
2.1 - Relationship to Abstract Data Definition and other encodings	10
2.2 - Additional Guidance	10
2.2.1 - EDH Structure	10
2.2.2 - EDH Creation Date	12
2.2.3 - Internal and External EDH	12
2.2.4 - EDH Elements	12
2.2.5 - MIME Type	12
Chapter 3 - Definitions, Interfaces, and Constraints	14
3.1 - Constraint Rule Types	14
3.2 - “Living” Constraint Rules	14
3.3 - Classified or Controlled Constraint Rules	14
3.4 - Constraint Terminology	14
3.5 - Errors and Warnings	15
3.6 - Rule Identifiers	15
3.7 - Data Validation Constraint Rules	15
3.7.1 - Purpose	15
3.7.2 - Schematron	16
3.7.3 - Non-null Constraints	16
3.7.4 - Inherited Constraints	16
3.7.5 - Value Enumeration Constraints	17
3.7.6 - Additional Constraints	17
3.7.6.1 - DES Constraints	17
3.7.7 - Constraint Rules	17
3.8 - Data Rendering Constraint Rules	17
3.8.1 - Purpose	17
3.8.2 - Rendering Constraint Rules	17
Chapter 4 - Conformance Validation	19
4.1 - Schema Validation	19

4.2 - Business Rule Validation	19
Chapter 5 - Generated Guides	20
5.1 - Schema Guide	20
5.2 - Schematron Guide	21
Appendix A - Feature Summary	22
A.1 - IC-EDH Feature Summary	22
Appendix B - Change History	23
B.1 - V2016-SEP Change Summary	23
B.2 - V2015-AUG Change Summary	24
B.3 - V4 Change Summary	25
B.4 - V3 Change Summary	26
B.5 - V2 Change Summary	27
Appendix C - List of Abbreviations	29
Appendix D - Bibliography	31
Appendix E - Points of Contact	35
Appendix F - IC CIO Approval Memo	36

List of Figures

Figure 1 - Related Specifications	6
Figure 2 - A graphical representation of an EDH	11

List of Tables

Table 1 - XML Namepaces	4
Table 2 - Dependencies	4
Table 3 - Numerical Rule Identifier Ranges	15
Table 4 - Constraint Rules	18
Table 5 - EDH Dependency over Time	22
Table 6 - Feature Summary Legend	22
Table 7 - IC-EDH Feature Comparison	22
Table 8 - DES Version Identifier History	23
Table 9 - Data Encoding Specification V2016-SEP Change Summary	23
Table 10 - Data Encoding Specification V2015-AUG Change Summary	24
Table 11 - Data Encoding Specification V4 Change Summary	26
Table 12 - Data Encoding Specification V3 Change Summary	26
Table 13 - Data Encoding Specification V2 Change Summary	27

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 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* ^[9] 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* ^[14] 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^[6] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

Information sharing within the national intelligence enterprise will increasingly rely on information 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 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)^[3] specifications of the Intelligence Community Enterprise Architecture (IC EA) 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^[5]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[9]
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC^[10]
 - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information^[14]
- 200 Series:
 - Intelligence Community Directive (ICD) 208, Write for Maximum Utility^[7]
 - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination^[8]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide^[12]

1.5 - Audience and Applicability

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

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*, ^[13] 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*,^[4] 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.” ^[15] 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
arh	urn:us:gov:ic:arh
ism	urn:us:gov:ic:ism
ntk	urn:us:gov:ic:ntk
edh	urn:us:gov:ic:edh
xsd	http://www.w3.org/2001/XMLSchema

1.7 - Dependencies

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

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

Table 2 - Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Access Rights and Handling (ARH.XML.V3+)</i> ^[3]	This specification does not depend on a specific version of Access Rights and Handling (ARH.XML); ARH.XML versions later than version 3 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
<i>XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML.V1+)</i> ^[6]	This specification does not depend on a specific version of Intelligence Community Identifier (IC-ID.XML); IC-ID.XML versions later than version 1 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.

Name	Dependency Description
<i>XML Data Encoding Specification for Information Security Marking (ISM.XML.V13+)</i> [16]	This specification does not depend on a specific version of Information Security Markings (ISM.XML); ISM.XML versions later than version 13 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
<i>XML CVE Encoding Specification for Need-to-Know Metadata (NTK.XML.V10+)</i> [19]	This specification does not depend on a specific version of Need To Know Metadata (NTK.XML); NTK.XML versions later than version 10 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
<i>CVE Encoding Specification for US Agency Acronyms (USAgency.CES.V2015-FEB+)</i> [23]	This specification does not depend on a specific version of US Agency (USAgency.CES); USAgency.CES versions later than version 2015-FEB MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
<i>CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES.V2015-MAY+)</i> [17]	This specification does not depend on a specific version of ISM Country Codes and Tetragraphs (ISMCAT.CES); ISMCAT.CES versions later than version 2015-MAY MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
International Organization for Standardization (ISO) Schematron [21] 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.

Name	Dependency Description
<p>XSLT 2.0^[28] implementation of Schematron^[21] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>

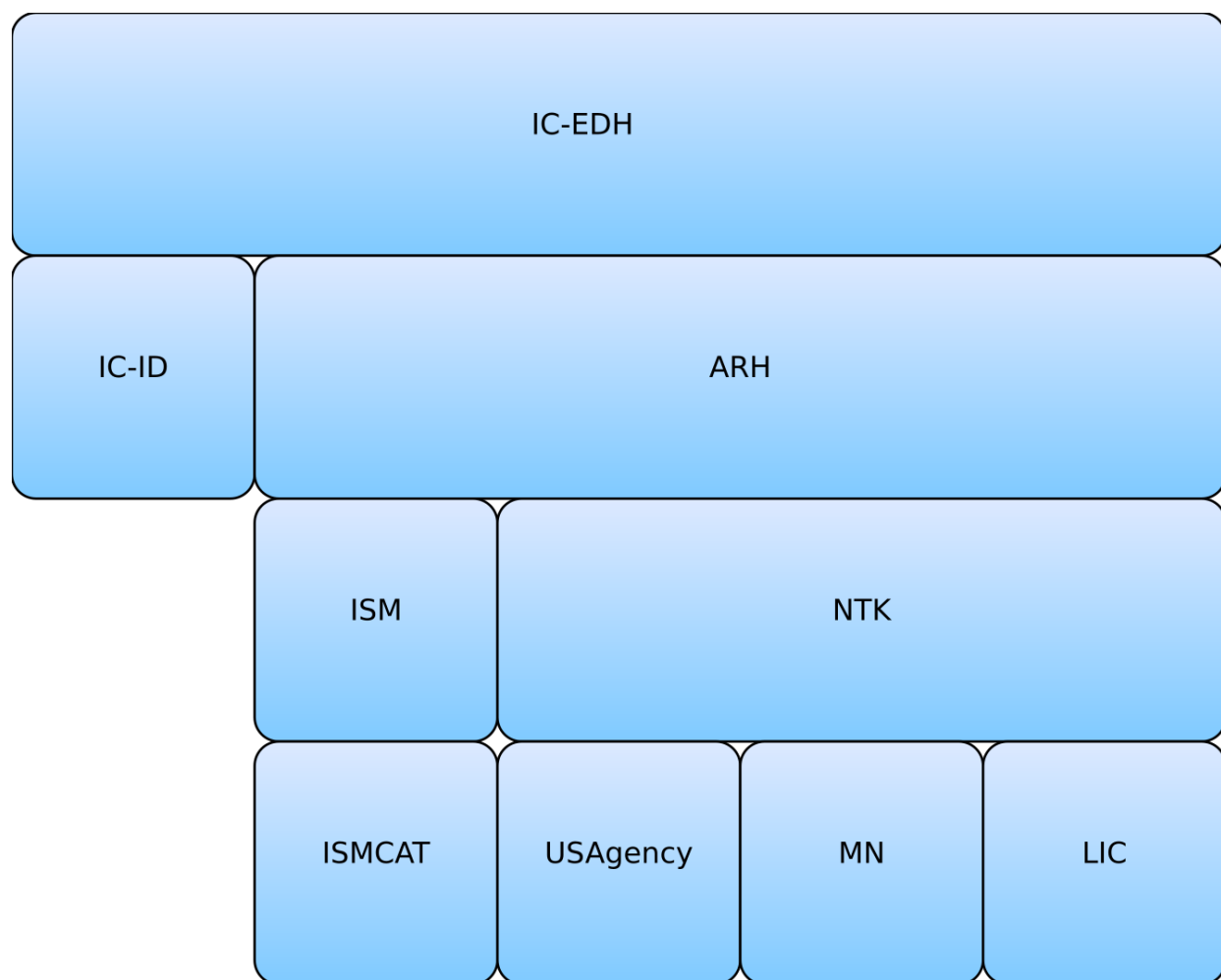


Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

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

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

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron^[21] 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^[15] 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.^[26] 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.”^[22] 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.”^[24]

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

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

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

1.9.2 - Version Numbering

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

Version Format when used in the version attribute:

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

Version in XML Lexicon

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

Version	The version number as it might be expressed in a DESVersion, CESVersion or other XML attribute for indicating the version being referenced.
Year	The four digit year from the version of the specification being referenced.
Month	The 2 digit month from the version of the specification being referenced.

CustomizationSuffix An optional suffix used when customizing a version of a specification. This would be used to indicate that you have extended the specification in some fashion for a particular use case.

Chapter 2 - Development Guidance

2.1 - Relationship to Abstract Data Definition and other encodings

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

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

2.2 - Additional Guidance

2.2.1 - EDH Structure

The IC-EDH specification incorporates all the information from the 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.

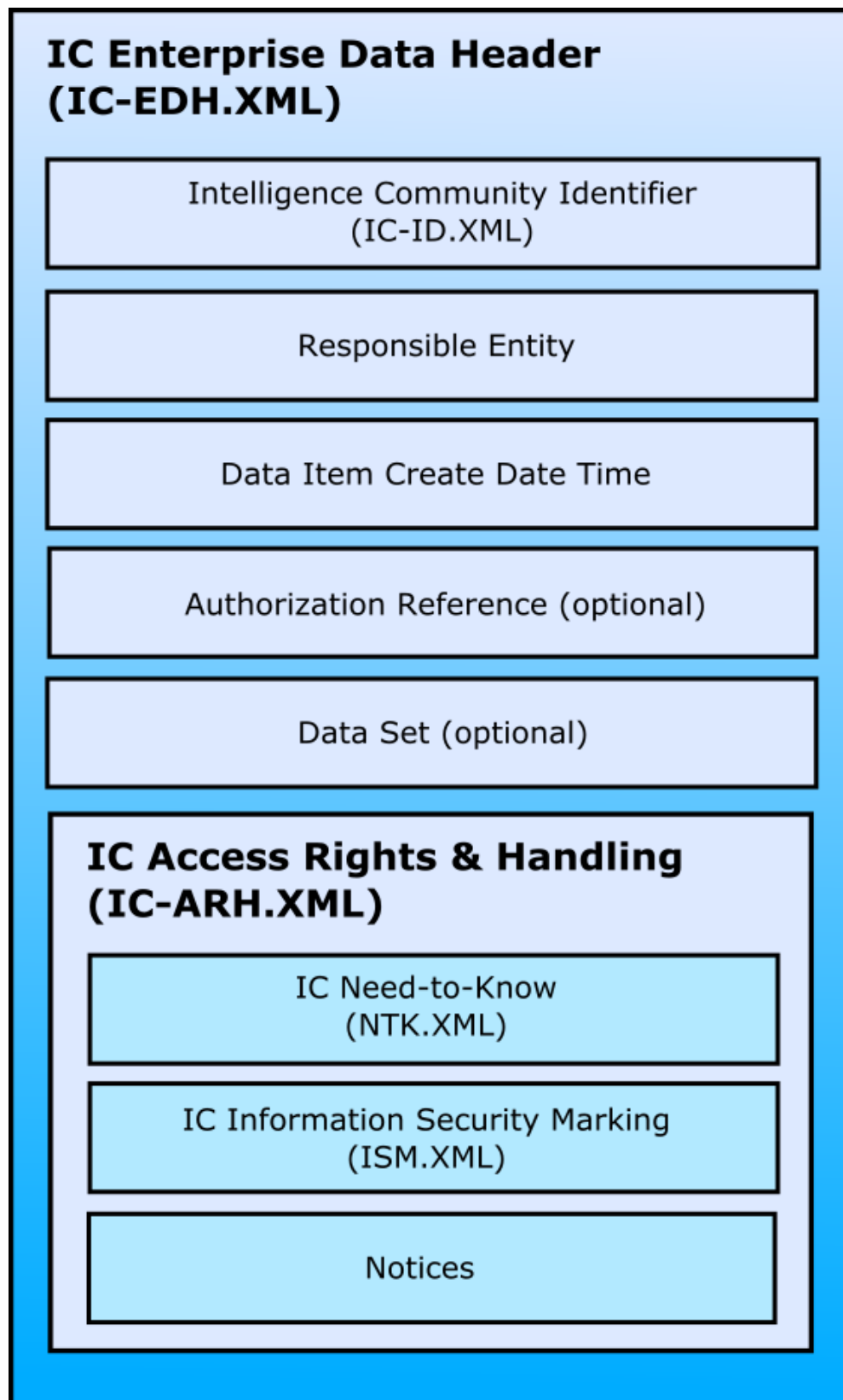


Figure 2 : A graphical representation of an EDH

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 the following main elements specific to EDH:

- **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. There may be up to two **ResponsibleEntity** elements. In previous versions, the ResponsibleEntity represented the Custodian role. In the current version, this must be explicitly specified via the role attribute. There must be one and only one Custodian, but there may be zero or one Originator.
 - **Country** - The allowed values for this element are trigraphs for country codes defined by the Responsible Entity CVE in ISMCAT [\[17\]](#)
 - **Organization** - The allowed values for this element are defined by the US Agency [\[23\]](#) specification.
- **DataItemCreateDateTime** - The creation date of the data object referred to by the EDH.
- **AuthorizationReference** - A means of indicating a particular documented legal basis for mission activities associated with the creation, retention and use of a resource (optional). MUST not impact access control, access control MUST be entirely contained in the ARH section.
- **DataSet** - A means of indicating a particular association of data. MUST not impact access control, access control MUST be entirely contained in the ARH section.

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 - Definitions, Interfaces, and Constraints

3.1 - Constraint Rule Types

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

3.2 - "Living" Constraint Rules

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

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

3.3 - Classified or Controlled Constraint Rules

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

3.4 - Constraint Terminology

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

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

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

3.5 - Errors and Warnings

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

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

3.6 - Rule Identifiers

Each constraint rule has an assigned rule identifier, indicated in brackets preceding the constraint rule description. EDH.XML data validation constraint rule identifiers are prefixed with “EDH-ID-” and followed by a 5 digit unique number, assigned from pre-defined ranges to group rules by classification. The numerical ranges are described in [Section 3.6 - Rule Identifiers \[15\]](#). 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 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^[21] is the formal language used in this specification to encode normative data validation constraints. The Schematron rules are normative in the sense that they convey criteria a document **MUST** meet, exactly as English may be used to convey normative criteria.

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

For better understanding, the Schematron^[21] rules for this specification may be executed in *Oxygen*^[20] or with an XSLT 2.0-compliant processor using the XSLT 2.0^[28] transforms in the Schematron implementation from Rick Jelliffe (see [XSLT 2.0 implementation of Schematron by Rick Jelliffe](#) in the Dependency table).

The constraint rules for this specification are dependent on XPath 2.0^[27] and XSLT 2.0^[28] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[18]

By default, Schematron uses the XPath language as used in XSLT 1.0, and is typically implemented by converting the schema into an XSLT 1.0 script which is run against the document being validated. However, ISO Schematron also allows XSLT 2.0 to be used, and this is becoming an increasingly popular choice because of the extra expressive convenience of XPath 2.0: a different skeleton is available for this.



Note

For convenience, the specification package provides the XSLT 2.0^[28] implementation of Schematron^[21] along with a compiled version of the rules.

3.7.3 - Non-null Constraints

XML syntax allows all elements with content declared to be of data type “string” to have zero or more characters of content, meaning elements can be empty or null. According to this specification, all required elements (and certain conditional elements) **MUST** have content, other than white space.¹ Elements, which are allowed to only have text content, **MUST** have text content specified.

3.7.4 - Inherited Constraints

In an instance of 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](#).

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

3.7.5 - Value Enumeration Constraints

Several elements and attributes of the EDH.XML 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. A subset CVE will be provided for use on networks not approved for the entire list. If the processing will occur on a network where the entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

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

3.7.6 - Additional Constraints

3.7.6.1 - DES Constraints

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

3.7.7 - Constraint Rules

The detailed constraint rules for the 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 4 - Constraint Rules

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

Chapter 4 - Conformance Validation

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

4.1 - Schema Validation

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

4.2 - Business Rule Validation

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

Chapter 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the 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 specifications. Direct dependencies are marked with an asterisk.

Table 5 - EDH Dependency over Time

Dependent Specification	V1	V2	V3	V4	V2015-AUG	V2016-SEP
ARH*	V1	V1+	V1+	V1+	V1+	V3+
ISM*	V9	V9-V11	V9-V11	V12+	V12+	V13+
NTK*	V7	V7+	V7+	V7+	V10+	V10+
IC-ID*			V1+	V1+	V1+	V1+
USAgency*				V1+	V1+	V2015-FEB+
ISMCAT*					V2015-MAY+	V2015-MAY+
MN						V2015-AUG+
LIC						V2015-AUG+

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

Table 6 - Feature Summary Legend

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

A.1. IC-EDH Feature Summary

Table 7 - IC-EDH Feature Comparison

IC-EDH Feature Comparison							
Required date	Feature	V1	V2	V3	V4	V2015-AUG	V2016-SEP
	Supports multiple versions of ISM.XML (V12 - Current), NTK.XML (V7 - Current), and ARH.XML (V1 - Current)	N	F	F	F	F	F
	Supports multiple versions of the IC-ID.XML (V1 - Current)	N	N	F	F	F	F
	Supports multiple versions of the USAgency.CES (V1 - Current)	N	N	N	F	F	F
	Eliminated ambiguous time zones on dates	N	N	N	N	F	F
	Externalized country codes to ISMCAT	N	N	N	N	F	F
	Support Originating & Custodian ResponsibleEntities.	N	N	N	N	N	F
	Support DataSet	N	N	N	N	N	F

Appendix B Change History

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

Table 8 - DES Version Identifier History

Version	Date	Purpose
1	17 July 2012	Initial Release
2	21 January 2013	Routine revision to technical specification. For details of changes, see Section B.5 - V2 Change Summary
3	5 April 2013	Routine revision to technical specification. For details of changes, see Section B.4 - V3 Change Summary
4	16 August 2013	Routine revision to technical specification. For details of changes, see Section B.3 - V4 Change Summary
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.2 - V2015-AUG Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Section B.1 - V2016-SEP Change Summary

B.1 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Harmonization with NSA EDH.

The following table summarizes the changes made to V2015-AUG in developing V2016-SEP.

Table 9 - Data Encoding Specification V2016-SEP Change Summary

Change	Artifacts changed	Compatibility Notes
Refactored schema to allow multiple ResponsibleEntities (CR-2016-010).	Schema Schematron	Systems need to be updated to accommodate this change.
Add optional DataSet element (CR-2016-011).	Schema	Systems need to be updated to accommodate this change.
Updated schematron rules to enforce minimum versions defined in specification dependency table 1.7.	Schematron IC-EDH-ID-00008 updated. IC-EDH-ID-00009 updated. IC-EDH-ID-00014 updated.	Systems need to be updated to accommodate this change.

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 DES.	Schema	No impact to systems.
Added a schematron rule to enforce that there must be one and only one ResponsibleEntity with role="Custodian" and zero or one with role="Originator" (CR-2016-010)	Schematron IC-EDH-ID-00015 added.	Systems need to be updated to accommodate this change.
Created new ResponsibilityEntityWithRoleType to enforce a role attribute being present on ResponsibleEntity elements (CR-2016-010).	Schema	Systems need to be updated to accommodate this change.
Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.2 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Enterprise AUDIT requirement to use timezones
- Refactoring to externalize country code CVE

The following table summarizes the changes made to V4 in developing V2015-AUG.

Table 10 - Data Encoding Specification V2015-AUG Change Summary

Change	Artifacts changed	Compatibility Notes
Refactored schema to use ISMCAT Responsible Entity CVE.	CVEnumEDHCountry-ISO3166Trigraph.xml removed Schema Schematron IC-EDH-ID-00014 added	Systems need to be updated to accommodate this change including the new CVE in ISMCAT.

Change	Artifacts changed	Compatibility Notes
Created Schematron rule to enforce existence of timezone in element <code>edh:DataItemCreateDateTime</code> .	Schematron IC-EDH-ID-00013 added	Systems that do not provide the timezone in <code>edh:DataItemCreateDateTime</code> need to be updated.
Refactored schema to use types and avoid inline element declarations.	Schema	Code generation systems will likely generate different code. There is no impact to other systems.
Updated code descriptions to improve readability.	Schematron	No impact to data generation and ingestion systems.
Updated rule 00012 to accommodate extensions to USAgency CES.	Schematron IC-EDH-ID-00012 modified	Systems need to be updated to accommodate extensions of USAgency CES.
Updated schema to make <code>@ism:CATCESVersion</code> mandatory for <code>edhType</code> .	Schema	Systems need to be updated to accommodate the schema change.
Updated context of Schematron rule 00005 to invalid element instead of parent of invalid element.	Schematron IC-EDH-ID-00005 modified	This update does not change the logic of the rule, but error reporting will be more precise. Systems may upgrade for improved error reporting.
Update context of rule 00003 to simplify	Schematron IC-EDH-ID-00003 modified	This update does not impact the logic of the rule only readability and simplicity.
Remove dependency on external abstract patterns.	Schematron IC-EDH-ID-00006 modified	This update should not impact the logic of the rule so there should be no impact to generation or ingestion systems.

B.3 - V4 Change Summary

Significant drivers for Version 4 include:

- Creation of US Agency specification
- See ISM V12 drivers

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

Table 11 - Data Encoding Specification V4 Change Summary

Change	Artifacts changed	Compatibility Notes
Updated the IC-EDH schema to import the US Agency specification and use the US Agency abstract rule to enforce allowable values for the Organization element when the Country is 'USA'. Added the US Agency CES Version attribute to the EDH top level element.	Schema Schematron IC-EDH-ID-00006 Updated	Data generation and ingestion systems need to be updated to use the latest version of the schema and to enforce the modified rule.
Added a schematron rule to ensure that the versions of the US Agency imported spec meets the minimum allowed version.	Schematron IC-EDH-ID-00012 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Added an optional attribute to declare the CES Version for ISMCAT on the IC-EDH root elements.	Schema	Data generation and ingestion systems need to be updated enforce the updated schema.
Updated the schematron rules for the minimum allowed version of ISM.	Schematron IC-EDH-ID-00008 Modified	Data generation and ingestion systems need to be updated enforce the modified rule.

B.4 - 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 12 - 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 IC-EDH-ID-00011 Added	Data generation and ingestion systems need to be updated enforce the new rules.

Change	Artifacts changed	Compatibility Notes
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 Schematron 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.5 - 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 13 - 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 IC-EDH-ID-00008 Added IC-EDH-ID-00009 Added IC-EDH-ID-00010 Added	Data generation and ingestion systems need to be updated enforce the new rules.
Update ISM to V10	Schema 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 ISM v9, NTK v7, and ARH v1	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.

Change	Artifacts changed	Compatibility Notes
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 IC-EDH-ID-00007 Changed	Data generation and ingest systems complying with the GUIDE id rules do not need to be updated. Systems that were allowing invalid GUIDE ids will need to be updated to comply with the constraint rule.
Add Cabinet Offices to CVEEnum-EDHOrganizationsUS	CVE	Data generation and ingestion systems need to be updated to use the correct CVE definitions and values.

Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
ARH	Access Rights and Handling
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
FOUO	For Official Use Only
HTML	HyperText Markup Language
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
IC-ID	IC Identifier
ICD	Intelligence Community Directive
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
ISM	Information Security Markings
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISO	International Organization for Standardization
IT	Information Technology

LIC	License
MIME	Multipurpose Internet Mail Extensions
MN	Mission Need Profile
NTK	Need-To-Know Metadata
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
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URL	Uniform Resource Locator
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

Bibliography

[1] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.

Available online at: <http://tools.ietf.org/html/std68>

Also known as: <http://www.ietf.org/rfc/rfc5234.txt>

[2] ADD

Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/soSC6M8>

Available online Intelink-U at: <https://w3id.org/ic/standards/ADD>

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

[3] ARH.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Access Rights and Handling (ARH.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/Fub6Gnw>

Available online Intelink-U at: <https://w3id.org/ic/standards/ARH>

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

[4] DoD Instruction 8310.01

DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.

Available online at: <http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf>

[5] 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>

[6] 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>

[7] 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

[8] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.

Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>

[9] 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

[10] 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

[11] 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>

[12] ICPM 2007-200-2

Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2. 11 December 2007.

Available online at: <http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf>

[13] 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>

[14] 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>

[15] 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>

[16] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <http://go.ic.gov/3oipfOY>

Available online Intelink-U at: <https://w3id.org/ic/standards/ISM>

- Available online at: <https://w3id.org/ic/standards/public>
- [17] ISMCAT.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.
Available online Intelink-TS at: <http://go.ic.gov/xhPfil3>
Available online Intelink-U at: <https://w3id.org/ic/standards/ISMCAT>
Available online at: <https://w3id.org/ic/standards/public>
- [18] Jelliffe
Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.
Available online at: <http://www.schematron.com>
- [19] NTK.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online Intelink-TS at: <http://go.ic.gov/YLXsYUX>
Available online Intelink-U at: <https://w3id.org/ic/standards/NTK>
Available online at: <https://w3id.org/ic/standards/public>
- [20] Oxygen
SyncRO Soft. *<oXygen/> XML Editor*.
Available online at: <http://www.oxygenxml.com/>
- [21] 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/>
- [22] 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>
- [23] USAgency.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.
Available online Intelink-TS at: <http://go.ic.gov/MmBEpFU>
Available online Intelink-U at: <https://w3id.org/ic/standards/USAgency>
Available online at: <https://w3id.org/ic/standards/public>
- [24] 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>
- [25] XML 1.0
World Wide Web Consortium (W3C). *Extensible Markup Language (XML) 1.0, Second Edition*. W3C, 6 October 2000.

Available online at: <http://www.w3.org/TR/2000/REC-xml-20001006>

[26] 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>

[27] 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/>

[28] XSLT2

World Wide Web Consortium (W3C). *XSL Transformations (XSLT) Version 2.0*. W3C Recommendation 23 January 2007.

Available online at: <http://www.w3.org/TR/xslt20/>

Appendix E Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at the following DNI-sponsored web sites.

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

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

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

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

Appendix F IC CIO Approval Memo

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

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

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.^[13]