Intelligence Community Technical Specification

XML Data Encoding Specification for Intelligence Community Enterprise Data Header

Version 2019-MAR

December 1, 2022

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

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

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

Table of Contents

Chapter 1 - Introduction 1
1.1 - Purpose 1
1.2 - Scope 1
1.3 - Enterprise Need 1
1.4 - Conventions 2
1.4.1 - XML Namespaces 2
1.5 - Dependencies 2
1.5.1 - Specification Dependencies 2
1.5.2 - Inverse Dependencies 5
Chapter 2 - Development Guidance 7
2.1 - Additional Guidance 7
2.1.1 - IC-EDH Structure 7
2.1.2 - IC-EDH Creation Date 8
2.1.3 - Internal and External EDH 8
2.1.4 - IC-EDH Elements 8
2.1.5 - MIME Type 9
Chapter 3 - Constraints 10
3.1 - Data Validation Constraint Rules 10
3.1.1 - Inherited Constraints 10
3.1.2 - Value Enumeration Constraints 10
3.1.3 - Additional Constraints 10
3.1.3.1 - DES Constraints 10
3.1.4 - Constraint Rules 10
3.2 - Data Rendering Constraint Rules 11
3.2.1 - Purpose 11
3.2.2 - Rendering Constraint Rules 11
Appendix A - Feature Summary 12
A.1 - IC-EDH Feature Summary 12
A.1.1 - Features from V4 to V2019-MAR 12
A.1.1.1 - Features Partial and N/A from V4 to V2019-MAR 12
A.1.2 - Features from V1 to V4 13
Appendix B - Change History 14
B.1 - 2019-MAR Change Summary 14
B.2 - V2016-SEP Change Summary 16
B.3 - V2015-AUG Change Summary 17
B.4 - V4 Change Summary 18
B.5 - V3 Change Summary 19
B.6 - V2 Change Summary 20
Appendix C - List of Abbreviations 22
Appendix D - Bibliography 23
Appendix E - Points of Contact 26
Appendix F - IC CIO Approval Memo 27

List of Figures

Figure 1 - Related Specifications 5
Figure 2 - Inverse Dependency Specifications 6
Figure 3 - A graphical representation of an IC-EDH 7

List of Tables

Table 1 - XML Namepaces 2
Table 2 - Dependencies 3
Table 3 - Constraint Rules 11
Table 4 - Feature Summary Legend 12
Table 5 - IC-EDH Feature Comparison V4 to V2019-MAR 12
Table 6 - IC-EDH Feature Comparison V4 to V2019-MAR 12
Table 7 - IC-EDH Feature Comparison V1 to V4 13
Table 8 - DES Version Identifier History 14
Table 9 - Data Encoding Specification V2019-MAR Change Summary 14
Table 10 - Data Encoding Specification V2016-SEP Change Summary 16
Table 11 - Data Encoding Specification V2015-AUG Change Summary 18
Table 12 - Data Encoding Specification V4 Change Summary 19
Table 13 - Data Encoding Specification V3 Change Summary 20
Table 14 - Data Encoding Specification V2 Change Summary 20

This document has been approved for Public Release by the Office of the Director of National Intelligence. See Distribution Notice for details.

Chapter 1 - Introduction

1.1 - Purpose

This *XML Data Encoding Specification for Intelligence Community Enterprise Data Header* (IC-EDH.XML) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode IC-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

The *Intelligence Community Technical Specification Framework* (IC-SF.XML[3]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

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

1.3 - 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 *XML Data Encoding Specification for Information Security Marking* (ISM.XML[11]) specification of the Intelligence Community Enterprise Architecture (IC EA) Data Standards. The IC-EDH.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, an IC-EDH ensures a secure method of information sharing and discovery, supporting use cases such as the IC Cloud.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 200 Series:
  - Intelligence Community Directive (ICD) 208, *Write for Maximum Utility* [4]
  - 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* [8]

- 500 Series:
  - ICD 500, *Director Of National Intelligence Chief Information Officer* [6]
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [7]
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [9]
  - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* [10]

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the “Specification Conventions” chapter in the IC-SF.XML[3].

1.4.1 - 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

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML[3].

1.5.1 - Specification Dependencies

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

The subsequent figure, Figure 1, is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts 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 IC CIO specifications listed in Table 2 will be shown in Figure 1; however not all IC CIO specifications

listed in Figure 1 may appear in Table 2. Figure 1 is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 2 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML.V1+[2])	This specification does not depend on a specific version of IC-ID.XML[2]; versions later than version 1 MAY be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 18-3.0 was used for determining the version.
XML Data Encoding Specification for Information Security Marking (ISM.XML.V2019-MAR+[11])	This specification does not depend on a specific version of ISM.XML[11]; versions later than version V2019-MAR MAY be used. The minimum version was based on a technical dependency; the merge of ARH and NTK into ISM.
CVE Encoding Specification for US Agency Acronyms (USAgency.CES.V2017-MAR-r2018-FEB+[16])	This specification does not depend on a specific version of USAgency.CES[16]; versions later than version 2017-MARr2018-FEB MAY be used. The minimum version was based on the earliest non-retired version; ESB 18-3.0 was used for determining the version.
CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES.V2019-MAR+[12])	This specification does not depend on a specific version of ISMCAT.CES[12]; versions later than version 2019-MAR MAY be used. The minimum version was based on authoritative source compliance; Partner Engagement Portal[14].
Intelligence Community Specification Framework (IC-SF.XML.V2019-MAR+[3])	This specification does not depend on a specific version of IC-SF.XML[3]; versions later than version 2019-MAR MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.
International Organization for Standardization (ISO) Schematron[15] 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.

Name	Dependency Description
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumeration (CVE) included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the IC-EDH CVEs is normative.
Schematron[15]	Schematron — ISO/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use Transformations (XSLT) 2.0[17] query binding.
XSLT 2.0[17] implementation of Schematron[15] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.
Value enumerations used for several XML structures are defined in the various CVEs included in this DES.	Specification uses CVEs to encode controlled vocabularies. The use of the IC-EDH.XML CVEs is normative.

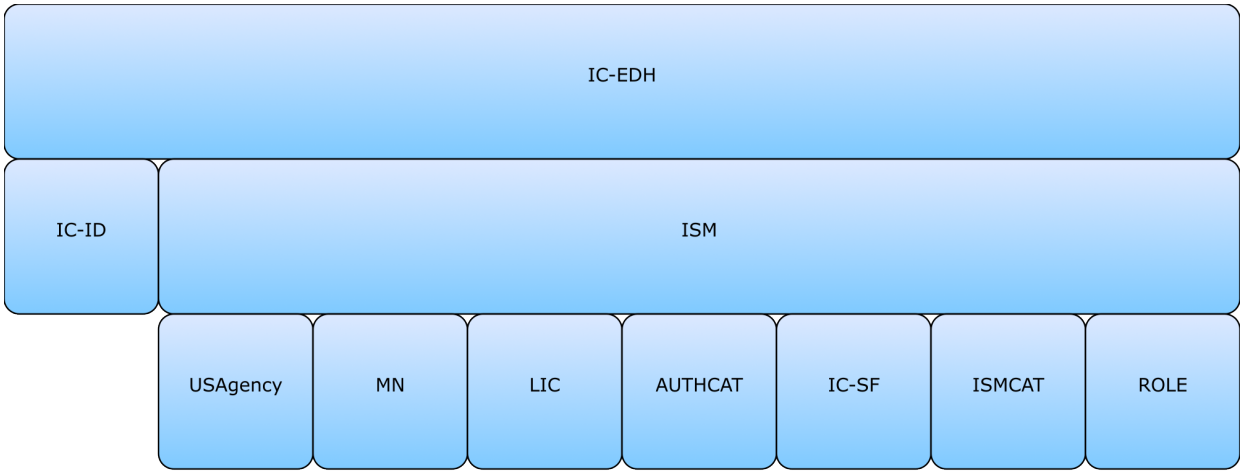

Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

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

Since this specification is one such specification that is used by other specifications released by the IC CIO, the Figure 2 has been included to assist readers in understanding all of the inverse dependency relationships and how changes in this given specification may impact others specifications. This diagram is representative of direct and transitive inverse dependencies at the time of the release of this specification, but are subject to change over time and is presented in a list format that is different than Figure 1.

Figure 2 : Inverse Dependency Specifications

Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML[3] framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

2.1 - Additional Guidance

2.1.1 - IC-EDH Structure

The IC-EDH specification incorporates all the information from the ISM.XML[11] 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 IC-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.

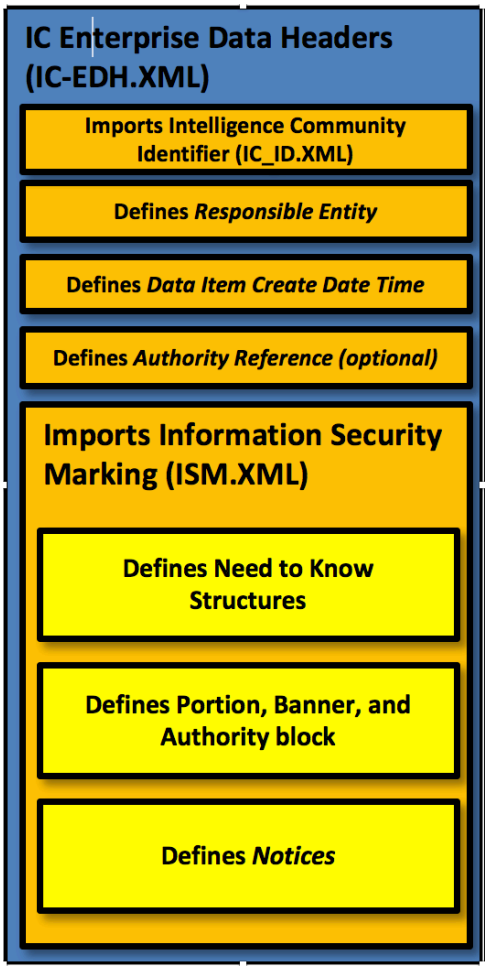

Figure 3 : A graphical representation of an IC-EDH

2.1.2 - IC-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 IC-EDH.

2.1.3 - 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.

2.1.4 - IC-EDH Elements

The IC-EDH consists of the following main elements:

- **`Identifier`** - This attribute holds the IC Identifier (IC-ID) of the data object referred to by the IC-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 **`ResponsibleEntity`** CVE in *CVE Encoding Specification for ISM Country Codes and Tetragraphs* (ISMCAT.CES[12]).

    - **`Organization`** - The allowed values for this element are defined by the *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES[16]).

- **`DataItemCreateDateTime`** - The creation date of the data object referred to by the IC-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 Access Rights and Handling (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.

2.1.5 - MIME Type

The Media Type (MIME) type for a IC-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 - Constraints

3.1 - Data Validation Constraint Rules

The IC-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. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML[3] framework document.

3.1.1 - Inherited Constraints

In an instance of IC-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 1.5 - Dependencies.

3.1.2 - Value Enumeration Constraints

Several elements and attributes of the IC-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.

3.1.3 - Additional Constraints

3.1.3.1 - 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.

3.1.4 - Constraint Rules

The detailed constraint rules for the IC-EDH.XML schema can be found in a separate document inside the Documents/IC-EDH directory, in the “IC-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 “IC-EDH_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - Purpose

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

3.2.2 - Rendering Constraint Rules

The following table contains the information for the IC-EDH.XML data rendering constraint rules.

Table 3 - Constraint Rules

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

Appendix A Feature Summary

The following table summarizes major features by version for this IC-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

A.1.1. Features from V4 to V2019-MAR

Table 5 - IC-EDH Feature Comparison V4 to V2019-MAR

Required date	Feature	V4	V2015-AUG	V2016-SEP	V2019-MAR
	Supports multiple versions of ISM.XML[11] (V12 - 2016-SEPr2018-JUL), NTK.XML[13] (V7 - v2016-SEP), and ARH.XML[1] (V1 - V3)	F	F	F	N/A
	Eliminated ambiguous time zones on dates	N	F	F	F
	Externalized country codes to ISMCAT.CES[12]	N	F	F	F
	Support Originating & Custodian ResponsibleEntities.	N	N	F	F
	Support DataSet	N	N	F	F
	Support ISM.XML[11] 2019-MAR (incorporated ARH/NTK) and later	N	N	N	F

A.1.1.1. Features Partial and N/A from V4 to V2019-MAR

Table 6 - IC-EDH Feature Comparison V4 to V2019-MAR

Required date	Feature	V4	V2015-AUG	V2016-SEP	V2019-MAR
	Supports multiple versions of ISM.XML[11] (V12 - 2016-SEPr2018-JUL), NTK.XML[13] (V7 - v2016-SEP), and ARH.XML[1] (V1 - V3)	F	F	F	N/A

A.1.2. Features from V1 to V4

Table 7 - IC-EDH Feature Comparison V1 to V4

Required date	Feature	V1	V2	V3	V4
	Supports multiple versions of ISM.XML[11] (V12 - 2016-SEPr2018-JUL), NTK.XML[13] (V7 - v2016-SEP), and ARH.XML[1] (V1 - V3)	N	F	F	F
	Supports multiple versions of the IC-ID.XML[2] (V1 - Current)	N	N	F	F
	Supports multiple versions of the USAgency.CES[16] (V1 - Current)	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	July 17, 2012	Initial Release
2	January 21, 2013	Routine revision to technical specification. For details of changes, see Section B.6 - V2 Change Summary
3	April 5, 2013	Routine revision to technical specification. For details of changes, see Section B.5 - V3 Change Summary
4	August 16, 2013	Routine revision to technical specification. For details of changes, see Section B.4 - V4 Change Summary
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see Section B.3 - V2015-AUG Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.2 - V2016-SEP Change Summary
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see Section B.1 - 2019-MAR Change Summary

B.1 - 2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Community Change Requests

The following table summarizes the changes made to V2016-SEP in developing V2019-MAR.

Table 9 - Data Encoding Specification V2019-MAR Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated documentation to use the specification framework. (CR-2018-126, CR-2017-245)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
2	Cleanup obsolete rules and documentation after ARH and NTK consolidation into ISM (CR-2018-095).	Documentation Schematron IC-EDH-ID-00009 deleted. IC-EDH-ID-00010 deleted.	Systems need to be updated to accommodate this change.
3	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-221)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
4	Added ISM.XML attributes to Schematron files to mark up the documentation. (CR-2017-300)	Schematron	No impact to systems.
5	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-109)	Documentation	No impact to systems.
6	Added schema PDF. (CR-2018-012)	Documentation	No impact to systems.
7	Changed "Multipurpose Internet Mail Extensions" to "Media Type". (CR-2018-054)	Documentation	No impact to systems.
8	Added schematron rule to warn if edh:DESVersion is earlier than current version. (CR-2017-079)	Schematron	Systems need to be updated to accommodate this change.
9	Changed schema to make both ism:ISMCATCESVersion and usagency:CESVersion optional in the schema. Enforcement of existence somewhere in the instance document is done by Schematron rules. (CR-2018-039)	Schema Schematron IC-EDH-ID-00017 added. IC-EDH-ID-00018 added.	Systems need to ensure they provide the relevant version attributes.

#	Change	Artifacts changed	Compatibility Notes
10	Update min version rules to check infrastructure instead of instance documents (CR-2018-133)	Schematron ValidateValidationEnvCVE added ValidateValidationEnvSchema added IC-EDH-ID-00008 modified IC-EDH-ID-00011 modified IC-EDH-ID-00012 modified IC-EDH-ID-00014 modified	Validation systems need to ensure they are compliant with min versions.
11	Removed the Dependency Over Time table. (CR-2018-152)	Documentation	No impact to systems.

B.2 - 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 10 - Data Encoding Specification V2016-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Refactored schema to allow multiple ResponsibleEntities (CR-2016-010).	Schema Schematron	Systems need to be updated to accommodate this change.
2	Add optional DataSet element (CR-2016-011).	Schema	Systems need to be updated to accommodate this change.

#	Change	Artifacts changed	Compatibility Notes
3	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.
4	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.
5	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.
6	Created new ResponsibilityEntityWithRoleTyp e to enforce a role attribute being present on ResponsibleEntity elements (CR-2016-010).	Schema	Systems need to be updated to accommodate this change.
7	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.3 - 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 11 - Data Encoding Specification V2015-AUG Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Refactored schema to use ISMCAT.CES[12] 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.CES[12].
2	Created Schematron rule to enforce existence of timezone in element edh:DataItemCreateDateTime.	Schematron IC-EDH-ID-00013 added	Systems that do not provide the timezone in **`edh:DataItemCreateDateTime`** need to be updated.
3	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.
4	Updated code descriptions to improve readability.	Schematron	No impact to data generation and ingestion systems.
5	Updated rule 00012 to accommodate extensions to USAgency.CES[16].	Schematron IC-EDH-ID-00012 modified	Systems need to be updated to accommodate extensions of USAgency.CES[16].
6	Updated schema to make @ism:CATCESVersion mandatory for edhType.	Schema	Systems need to be updated to accommodate the schema change.
7	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.
8	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.
9	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.4 - V4 Change Summary

Significant drivers for Version 4 include:

- Creation of US Agency specification
- See ISM.XML[11] V12 drivers

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

Table 12 - Data Encoding Specification V4 Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	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 USAgency.CES[16] CESVersion attribute to the IC-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.
2	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.
3	Added an optional attribute to declare the CESVersion for ISMCAT.CES[12] on the IC-EDH root elements.	Schema	Data generation and ingestion systems need to be updated enforce the updated schema.
4	Updated the schematron rules for the minimum allowed version of ISM.XML[11].	Schematron IC-EDH-ID-00008 Modified	Data generation and ingestion systems need to be updated enforce the modified rule.

B.5 - V3 Change Summary

Significant drivers for Version 3 include:

- Creation of IC-ID.XML[2] specification

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

Table 13 - Data Encoding Specification V3 Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Added a schematron rule to ensure that the versions of the IC-ID.XML[2] 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.
2	Updated the IC-EDH schema to import the IC-ID.XML[2] specification and use the IC-ID.XML[2] definition of Identifier instead of the element previously defined in IC-EDH. Added the IC-ID.XML[2] DESVersion attribute to the Enterprise Data Header (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.XML[2] 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.6 - V2 Change Summary

Significant drivers for Version 2 include:

- See ISM.XML[11] V10 drivers

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

Table 14 - Data Encoding Specification V2 Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	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.
2	Update ISM.XML[11] to V10	Schema Constraint Rules	Data generation and ingestion systems need to be updated to comply with all constraint rules in this sub-specification.

#	Change	Artifacts changed	Compatibility Notes
3	Version decoupling, allowing import of any version of ISM.XML[11] and other dependent specifications at or above ISM.XML[11] v9, NTK.XML[13] v7, and ARH.XML[1] v1	DES	Data ingestion systems need to be aware of this change and ensure they check appropriate dependent spec versions for validation.
4	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.
5	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 List of Abbreviations

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

ARH	Access Rights and Handling
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
EDH	Enterprise Data Header
ESB	Enterprise Standards Baseline
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC-ID	IC Identifier
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MIME	Media Type
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

[1] 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: https://go.ic.gov/FTSj6AO (case sensitive – Foxtrot Tango Sierra juliet 6 Alpha Oscar)
Available online Intelink-U at: https://w3id.org/ic/standards/ARH
Available online at: https://w3id.org/ic/standards/public

[2] 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: https://go.ic.gov/aKlfr9y (case sensitive – alpha Kilo lima foxtrot romeo 9 yankee)
Available online Intelink-U at: https://w3id.org/ic/standards/IC-ID
Available online at: https://w3id.org/ic/standards/public

[3] IC-SF.XML
Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.
Available online Intelink-TS at: https://go.ic.gov/pNFyuVg (case sensitive – papa November Foxtrot yankee uniform Victor golf)
Available online Intelink-U at: https://w3id.org/ic/standards/IC-SF
Available online at: https://w3id.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%20209%20Tearline%20Production%20and%20Dissemination.pdf

[6] 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: https://go.ic.gov/U7v6ZRL (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[7] 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: https://go.ic.gov/fTBM8OS (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[8] 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

[9] 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: https://go.ic.gov/kh8NMVJ (case sensitive – kilo hotel 8 November Mike Victor Juliet)
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-20

[10] 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: https://go.ic.gov/0Agmenr (case sensitive – 0 Alpha golf mike echo november romeo)
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-21

[11] ISM.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.
Available online Intelink-TS at: https://go.ic.gov/qoNICy7 (case sensitive – quebec oscar November India Charlie yankee 7)
Available online Intelink-U at: https://w3id.org/ic/standards/ISM
Available online at: https://w3id.org/ic/standards/public

[12] ISMCAT.CES
Office of the Director of National Intelligence. *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.
Available online Intelink-TS at: https://go.ic.gov/mLF5WA9 (case sensitive – mike Lima Foxtrot 5 Whiskey Alpha 9)
Available online Intelink-U at: https://w3id.org/ic/standards/ISMCAT
Available online at: https://w3id.org/ic/standards/public

[13] 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: https://go.ic.gov/6wFIZpE (case sensitive – 6 whiskey Foxtrot India Zulu papa Echo)
Available online Intelink-U at: https://w3id.org/ic/standards/NTK
Available online at: https://w3id.org/ic/standards/public

[14] PE-Portal

ODNI/Partner Engagement Tetragraph Portal. Office of the Director of National Intelligence
Available online Intelink-TS at: https://intellipedia.intelink.ic.gov/wiki/Portal:Tetragraphs
Available online Intelink-S at: https://intellipedia.intelink.sgov.gov/wiki/Portal:Tetragraphs

[15] 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/

[16] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.
Available online Intelink-TS at: https://go.ic.gov/wmyIRCV (case sensitive – whiskey mike yankee India Romeo Charlie Victor)
Available online Intelink-U at: https://w3id.org/ic/standards/USAgency
Available online at: https://w3id.org/ic/standards/public

[17] 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 Director of National Intelligence (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@odni.gov.

Appendix F IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO 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 IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO 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 Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20[9].