



Intelligence Community Technical Specification

CVE Encoding Specification for Authority Categories

Version 2018-APR

December 1, 2022

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	3
1.7 - Dependencies	4
1.7.1 - Types of Dependencies	4
1.7.2 - Specification Dependencies	4
1.7.3 - Inverse Dependencies	6
1.8 - Conformance	8
1.9 - Version Policies	8
1.9.1 - XML Namespace Policy	8
1.9.2 - Version Numbering	9
Chapter 2 - Development Guidance	11
2.1 - Understanding Access Control	11
2.2 - Relationship to Abstract Data Definition and other encodings	12
2.3 - Additional Guidance	12
2.3.1 - Usage of the AUTHCAT Schema	12
2.3.2 - Usage of the AUTHCAT Schematron Library	13
2.4 - CSV Notes	13
2.5 - JSON Notes	14
2.6 - RELAX NG Notes	14
Chapter 3 - Definitions, Interfaces, and Constraints	15
3.1 - Constraint Rule Types	15
3.2 - “Living” Constraint Rules	15
3.3 - Classified or Controlled Constraint Rules	15
3.4 - Constraint Terminology	15
3.5 - Errors and Warnings	16
3.6 - Rule Identifiers	16
3.7 - Data Validation Constraint Rules	16
3.7.1 - Purpose	16
3.7.2 - Schematron	17
3.7.3 - Non-null Constraints	17
3.7.4 - Value Enumeration Constraints	17
3.7.5 - Additional Constraints	18
3.7.5.1 - CES Constraints	18
3.7.6 - Constraint Rules	18
3.8 - Data Rendering Constraint Rules	18
3.8.1 - Purpose	18
3.8.2 - Rendering Constraint Rules	18

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 - AUTHCAT.CES Feature Comparison	22
Appendix B - Change History	23
B.1 - V2018-APR Change Summary	23
Appendix C - List of Abbreviations	25
Appendix D - Bibliography	27
Appendix E - Points of Contact	32
Appendix F - IC CIO Approval Memo	33

List of Figures

Figure 1 - Inverse Dependency Specifications 7
Figure 2 - Three-legged Stool of Access Decisions 11

List of Tables

Table 1 - XML Namepaces	4
Table 2 - Direct Dependencies	5
Table 3 - Numerical Rule Identifier Ranges	16
Table 4 - Constraint Rules	18
Table 5 - Feature Summary Legend	22
Table 6 - AUTHCAT.CES Feature comparison	22
Table 7 - CES Version Identifier History	23
Table 8 - Data Encoding Specification V2018-APR Change Summary	23

Chapter 1 - Introduction

1.1 - Purpose

This *CVE Encoding Specification for Authority Categories* (AUTHCAT.CES) defines detailed implementation guidance using several encoding formats including Extensible Markup Language (XML), and JavaScript Object Notation (JSON) to encode Authority Categories controlled vocabulary. This Controlled Vocabulary Enumeration (CVE) Encoding Specification (CES) defines the elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing data concepts using a variety of formats.



Note

NSA Logical Authority Category (LAC) values are in AUTHCAT.CES as the authoritative source for use in for use in Intelligence Community (IC) exchange formats and for use across multiple fabrics. Logical Authority Category (LAC) values are not intended to be the only values in AUTHCAT.CES over time. The authoritative source that AUTHCAT.CES draws National Security Agency (NSA) LAC values from is the JWICS accessible NSA Mission Webspace (MWS) registry.

1.2 - Scope

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

1.3 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [\[8\]](#) 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* ^[13] the extensive and consistent use of 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 ADD* ^[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

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

This CES defines the Authority Category CVE. It contains common valid Authority Categories for Access Control.

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

- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[8]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* ^[9]
 - Intelligence Community Program Guidance (ICPG) 500.1, *Digital Identity* ^[10]
 - ICPG 500.2, *Attribute-based Authorization and Access Management* ^[11]
 - ICS 500-20, *IC Enterprise Standards Compliance* ^[12]
 - ICS 500-27, *Collection and Sharing of Audit Data* ^[14]
 - ICS 500-29, *IC Digital Identifier* ^[15]
 - ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources* ^[16]

1.5 - Audience and Applicability

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

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards*

Compliance [12], defines the Intelligence Community Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

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

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

1.6 - Conventions

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

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 Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119, “Key words for use in RFCs to Indicate Requirement Levels” [17]. When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

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

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

1.6.3 - Terminology

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

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

1.6.4 - XML Namespaces

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

Table 1 - XML Namepaces

Prefix	URI
ism	urn:us:gov:ic:ism
xsd	http://www.w3.org/2001/XMLSchema

1.7 - Dependencies

1.7.1 - Types of Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. Dependencies play an important role in functionality or provide informational relationships between the various artifacts. The following terms are defined to help assist with understanding how the various artifacts work together:

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

1.7.2 - Specification Dependencies

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

Table 2 - Direct Dependencies

Name	Dependency Description
Schematron ^[25]	<p>Schematron — International Organization for Standardization (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.</p> <p>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.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0^[33] query binding.</p>
<p>XSLT 2.0^[33] implementation of Schematron^[25] 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 Uniform Resource Locator (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>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations included in this Data Encoding Specification (DES).	Specification uses CVEs to encode controlled vocabularies. The use of the AUTHCAT.CES CVEs is normative.

1.7.3 - 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 1](#) 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.



Figure 1 : Inverse Dependency Specifications

1.8 - Conformance

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

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron^[25] 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 Extensible Stylesheet Language (XSL) transformations, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[17] 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^[31]. For example, a schema could be changed to incorporate a different version of a dependency like ISM.XML^[19] by changing the attribute declaration of `@ism:DESVersion="201508"` to `@ism:DESVersion="201609"` 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 AUTHCAT.CES^[3]) to be “decoupled” from the configuration change control of dependent specifications (such as UIAS.XML^[27] 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.”^[26] This decision allows for systems that process information encoded with these specifications to use the same Path Language (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.”^[29]

There is a version attribute (e.g., `@DESVersion`, `@CESVersion`, `@TESVersion`, `@version`) for each namespace defined in an IC CIO specification. Version attributes are used to capture the specification version number the specification author intends an instance to conform to.

Namespaces do not change, so the version attribute is required to fully understand an instance document.

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

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

1.9.2 - Version Numbering

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

Version Format when used in the version attribute:

- [1] Version ::= [Year Month](#)["." [Revision](#)] ["-" [CustomizationSuffix](#)]
 [2] VersionYear ::= 4(DIGIT)
 [3] VersionMonth ::= 2(DIGIT)
 [4] Customization ::= 1*23(ALPHA / DIGIT / "_")
 Suffix
 [5] RevisionYear ::= 4(DIGIT)
 [6] RevisionMont ::= 2(DIGIT)
 h
 [7] Revision ::= [Year Month](#)

Version in XML Lexicon

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

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

RevisionMonth	The 2 digit month from the revision of the specification being referenced.
Revision	The Year and Month from the revision of the specification being referenced. Revisions are modifications to Versions.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions are based upon three components (data attributes, user attributes, and access control policies) and are held together by the context in which the access control decision is made. The context itself includes various elements, such as the environment, temporal state, and method of access, that together provide the Where, When, and How details of the access request. The context, together with the user making the request and the data/repository/application being requested (the Who and What respectively), make up the framework that supports an access control decision. Access Policy SHOULD be constrained to use data attributes, user attributes, and context information. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. An entity MUST meet all criteria in the framework to be granted access. The concept of the access control decision framework is depicted in [Figure 2](#).

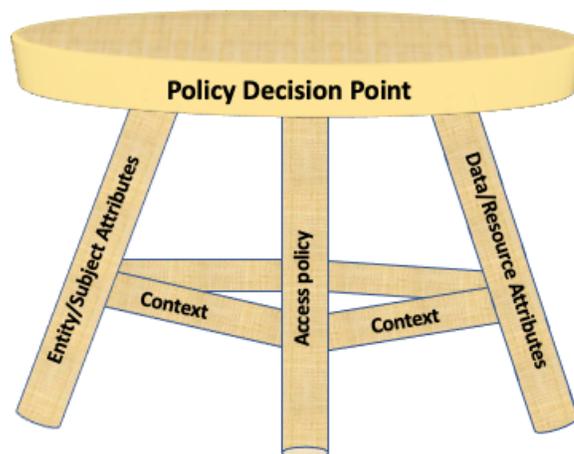


Figure 2 : Three-legged Stool of Access Decisions

All of these parts come together to create a tri-legged stool of access control. When a stool is missing one of the components of its frame, it is unable to function properly. The same is true of access control. Without each component of the framework, access control falls apart. Each component is crucial to make accurate, reliable, and automated access control decisions. Each IC CIO document will address a piece of the framework of access control decisions.

This specification participates in at least one of the legs of the access control framework either as a primary specification or as a dependency of a primary specification. The primary specifications for the legs include:

- Access policy specifications:
 - *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*^[18]
- Data attribute specifications:
 - *CVE Encoding Specification for Authority Categories (AUTHCAT.CES)*^[3]
 - *XML Data Encoding Specification for Information Security Markings (ISM.XML)*^[19]
 - *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*^[20]
 - *XML CVE Encoding Specification for License (LIC)*^[22]
 - *XML CVE Encoding Specification for Mission Need (MN.CES)*^[23]
 - *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*^[28]
- Entity attribute specifications:
 - *CVE Encoding Specification for Authority Categories (AUTHCAT)*^[3]
 - *CVE Encoding Specification for Fine Access Control (FAC.CES)*^[4]
 - *Data Encoding Specification for IC Full Service Directory Schema (FSD)*^[5]
 - *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*^[27]
 - *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*^[28]

2.2 - 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 Abstract Data Definition (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.

2.3 - Additional Guidance

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

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

2.3.1 - Usage of the AUTHCAT Schema

The AUTHCAT.CES schema defines an element (**AuthorityCategory**) and an attribute (**authorityCategory**) that enforces the allowable values as defined in the specification's CVE (see

[Section 3.7.4 - Value Enumeration Constraints](#) for more details). Consumers of the AUTHCAT.CES specification should import the AUTHCAT.CES schema and reference the element or attribute, depending on what is needed. Note: the names for the element and the attribute are similar because the content is the same, i.e., both limit the value to the AUTHCAT.CES CVE, but the expectation on usage is that the consumer would use one or the other. The difference in capitalization is because they follow the IC naming standards, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

2.3.2 - Usage of the AUTHCAT Schematron Library

The AUTHCAT.CES Schematron library contains an abstract rule that enforces the allowable values as defined in the specification's CVE (see [Section 3.7.4 - Value Enumeration Constraints](#) for more details). Consumers of the AUTHCAT.CES specification should include the abstract rule and define an implementation for it. This allows for the consumer to define the context that triggers the rule and the value that should be matched against the AUTHCAT.CES CVE.

Note that consumers of the AUTHCAT.CES Schematron library also need to import the AUTHCAT.CES schema within their schema. The importing schema needs to reference the CES Version for AUTHCAT.CES in order to let systems reviewing the data know what Schematron library to import.

2.4 - CSV Notes

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



Important

The CSV files on many systems will open "automatically" in Microsoft Excel; the default opening however, may not correctly read UTF-8 special characters. These are found in some country names such as "Republic of Côte d'Ivoire". We added the Byte Order Mark (BOM) as this appears to make newer versions of Excel work properly without the following workaround. If you need to use a CVE that contains such special characters, or you think may contain such characters in Excel, you should:



Note

The following steps tested successfully for macOS Excel version 15.3.9 and Microsoft Windows Excel version 14.0.7; it was unsuccessful for macOS Excel version 14.7.1

1. Open Excel to a blank sheet
2. Under the Data menu choose to get external data from a text file
3. Choose UTF-8 as the file origin

4. Choose delimited as the format
5. Choose next
6. Change from tab to Comma as the delimiter
7. Finish import to get the data in with the UTF-8 Characters properly encoded in Excel.

2.5 - JSON Notes

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

2.6 - RELAX NG Notes

There are REgular LAnguage for XML Next Generation (RELAX NG) format files provided for all of the CVEs. They are in the Schema folder with the XML Schema Definition (XSD) versions of the information. They are provided as a convenience to developers who wish to import IC Specification CVEs into other XML specifications that utilize RELAX NG. They will not affect specifications that do not utilize RELAX NG and there are no new requirements because of their existence. RELAX NG is an alternative schema language for XML and it provides both an XML syntax and a compact non-XML syntax. The XML syntax format fragments are provided with the .rng file name extension and the Compact syntax fragments are provided with the .rnc file name extensions.

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. AUTHCAT.CES data validation constraint rule identifiers are prefixed with "AUTHCAT-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 \[16\]](#). 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 AUTHCAT.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which AUTHCAT.CES instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable IC policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

3.7.2 - Schematron

Schematron^[25] 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^[25] rules for this specification may be executed in *Oxygen*^[24] or with an XSLT 2.0-compliant processor using the XSLT 2.0^[33] 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^[32] and XSLT 2.0^[33] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard^[21] stated the following:

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^[33] implementation of Schematron^[25] 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 - Value Enumeration Constraints

Several elements and attributes of the AUTHCAT.CES model use CVE 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

¹“White space” is defined in XML 1.0^[30] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

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.

3.7.5 - Additional Constraints

3.7.5.1 - CES Constraints

The CES version is specified through attributes on the root element. The schema constrains the values of these attributes. The **CESVersion** attribute enables systems 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.

3.7.6 - Constraint Rules

The detailed constraint rules for the AUTHCAT.CES schema can be found in a separate document inside the Schematron/AUTHCAT directory, in the AUTHCAT_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 AUTHCAT_Rules.pdf file.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of AUTHCAT.CES documents. The intent is to inform the development of systems capable of rendering or displaying AUTHCAT.CES data for use by individuals not familiar with the details of the AUTHCAT.CES markup. While expressed in a similar manner to the data validation constraint rules above, there is no expectation that evaluation of these rules can be automated; rather these rules should inform the evaluation of a system's capabilities and functionality.

3.8.2 - Rendering Constraint Rules

The following table contains the information for the AUTHCAT.CES data rendering constraint rules.

Table 4 - Constraint Rules

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

Chapter 4 - Conformance Validation

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

4.1 - Schema Validation

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



Warning

If IC-TDF.XML^[7] is being used it is critical to follow the validation strategy outlined in IC-TDF.XML^[7] to achieve proper schema validation. Failure to do so will have a high probability of schema invalid data appearing to be valid.

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 AUTHCAT.CES schema can be found as a collection of HyperText Markup Language (HTML) files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the AUTHCAT.CES schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen*^[24], 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 AUTHCAT.CES Schematron rules can be found in a separate document named *AUTHCAT_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 tables summarize major features by version for AUTHCAT.CES. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g. The IC Marking System Register and Manual has an implementation date of one year after issuance).

Table 5 - Feature Summary Legend

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

A.1. AUTHCAT.CES Feature Comparison

Table 6 - AUTHCAT.CES Feature comparison

Required date	Feature	V1	V2018-APR
	Defines the allowable values for Authority Categories	F	F

Appendix B Change History

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

Table 7 - CES Version Identifier History

Version	Date	Purpose
1	March 14, 2014	Initial Release
1	May 9, 2014	Re-release
2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see Section B.1 - V2018-APR Change Summary

B.1 - V2018-APR Change Summary

Significant drivers for Version V2018-APR include:

- Community Change Requests

The following table summarizes the changes in V2018-APR.

Table 8 - Data Encoding Specification V2018-APR Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Remove AUTHCAT from UIAS (it had been merged in for 2016-SEP) to allow it to update faster as needed for the new NTK profile that uses AUTHCAT. (CR-2016-005, CR-2017-159)	CES CVE AUTHCAT	Data generation and ingestion systems need to be updated to use the modified version string.
2	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-278)	Documentation	No impact to systems.
3	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-240)	Documentation	No impact to systems.
4	Update prose to align with current specifications. Change e-mail address to ic-standards-support@iarpa.gov. (CR-2017-285)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
5	The schema change logs will no longer be maintained as of the 2018-APR release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2018-APR, reference the change history in the DES.	Schema	No impact to systems.
6	Create RelaxNG CVE Fragments for ISMCAT. (CR-2017-191)	CVEs	No impact to systems.
7	Create JSON version of CVEs in AUTHCAT (CR-2017-287)	CVEs	No impact to systems.
8	Create CSV version of CVEs in AUTHCAT (CR-2017-286)	CVEs	No impact to systems.
9	Updated CESVersion attribute to generic regex in the schema and created schematron rule to check current CESVersion (CR-2017-340)	Schema Schematron AUTHCAT-ID-00001 added	Data generation and ingestion systems need to be updated to accommodate the changes.
10	Added schema PDF. (CR-2018-032)	Documentation	No impact to systems.
11	Rename short name to AUTCATH.CES from AUTHCAT.XML since there are multiple non XML formats included. Updated Purpose section to be less XML centric. (CR-2018-040)	Documentation	No impact to systems.
12	Updated section on Understanding Access Control to more accurately represent all of the specifications that participate in access control decisions. (CR-2018-071)	Documentation	No impact to systems.
13	Updated list of values to new set provided during final review. (CR-2018-075)	CVEs	Systems using values removed will need to coordinate with the prior owning agency for guidance on how to migrate to the new values.
14	Updated CSV generation to include a column for deprecation date information. (CR-2018-091)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.

Appendix C List of Abbreviations

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

ADD	Abstract Data Definition
CES	Controlled Vocabulary Enumeration Encoding Specification
CSV	Comma Separated Value
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
FOUO	For Official Use Only
HTML	HyperText Markup Language
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
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LAC	Logical Authority Category
NIEM	National Information Exchange Model
NSA	National Security Agency

PDP	Policy Decision Point
RELAX NG	REgular LAnguage for XML Next Generation
RFC	Request for Comments
URL	Uniform Resource Locator
XML	Extensible Markup Language
XPath	XML Path Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D 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: <https://go.ic.gov/6I5LJNo> (case sensitive – 6 India 5 Lima Juliet November oscar)
Available online Intelink-U at: <https://w3id.org/ic/standards/ADD>
Available online at: <https://w3id.org/ic/standards/public>

[3] AUTHCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Authority Category (AUTHCAT.CES)*. Available online Intelink-TS at: <https://go.ic.gov/JIMIYN5> (case sensitive – Juliet India Mike lima Yankee November 5)
Available online Intelink-U at: <https://w3id.org/ic/standards/AUTHCAT>
Available online at: <https://w3id.org/ic/standards/public>

[4] FAC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Fine Access Control (FAC.CES)*. Available online Intelink-TS at: <https://go.ic.gov/uZz5I7T> (case sensitive – uniform Zulu zulu 5 India 7 Tango)
Available online Intelink-U at: <https://w3id.org/ic/standards/FAC>
Available online at: <https://w3id.org/ic/standards/public>

[5] FSD

Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD)*. Available online Intelink-TS at: <https://go.ic.gov/TAHlnW8> (case sensitive – Tango Alpha Hotel lima november Whiskey 8)
Available online Intelink-U at: <https://w3id.org/ic/standards/FSD>
Available online at: <https://w3id.org/ic/standards/public>

[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: <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>

[7] IC-TDF.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Trusted Data Format (IC-TDF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/hdwc8fn> (case sensitive – hotel delta whiskey charlie 8 foxtrot november)

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

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

[8] 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

[9] 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

[10] ICPG 500.1

Deputy Director of National Intelligence for Policy, Plans, and Requirements. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 7 May 2010.

Available online Intelink-TS at: <https://go.ic.gov/kEqL6Dh> (case sensitive – kilo Echo quebec Lima 6 Delta hotel)

[11] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online Intelink-TS at: <https://go.ic.gov/NUAEWk1> (case sensitive – November Uniform Alpha Echo Whiskey kilo 1)

Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[12] 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>

[13] 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>

[14] ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <https://go.ic.gov/Jznuy0x> (case sensitive – Juliet zulu november uniform yankee 0 xray)

[15] ICS 500-29

Director of National Intelligence Chief Information Officer. *Intelligence Community Digital Identifier*. Intelligence Community Standard 500-29. 12 July 2012.

Available online Intelink-TS at: <https://go.ic.gov/ObgTCPJ> (case sensitive – Oscar bravo golf Tango Charlie Papa Juliet)

[16] ICS 500-30

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*. Intelligence Community Standard 500-30. 24 April 2014.

Available online Intelink-TS at: <https://go.ic.gov/lqk775v> (case sensitive – lima quebec kilo 7 7 5 victor)

[17] 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>

[18] ISM.ACES

Office of the Director of National Intelligence. *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*.

Available online Intelink-TS at: <https://go.ic.gov/rOG2Bjt> (case sensitive – romeo Oscar Golf 2 Bravo juliet tango)

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

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

[19] 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>

[20] 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>

- [21] Jelliffe
Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.
Available online at: <http://www.schematron.com>
- [22] LIC.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for License (LIC.CES)*.
Available online Intelink-TS at: <https://go.ic.gov/IsHgQxJ> (case sensitive – India sierra Hotel golf Quebec xray Juliet)
Available online Intelink-U at: <https://w3id.org/ic/standards/LIC>
Available online at: <https://w3id.org/ic/standards/public>
- [23] MN.CES
Office of the Director of National Intelligence. *CVE Encoding Specification for Mission Need (MN.CES)*.
Available online Intelink-TS at: <https://go.ic.gov/ndd7V1R> (case sensitive – november delta delta 7 Victor 1 Romeo)
Available online Intelink-U at: <https://w3id.org/ic/standards/MN>
Available online at: <https://w3id.org/ic/standards/public>
- [24] Oxygen
SyncRO Soft. *<oxygen/> XML Editor*.
Available online at: <http://www.oxygenxml.com/>
- [25] 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/>
- [26] 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>
- [27] UIAS.XML
Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.
Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1)
Available online Intelink-U at: <https://w3id.org/ic/standards/UIAS>
Available online at: <https://w3id.org/ic/standards/public>
- [28] 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>

[29] 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>

[30] 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>

[31] 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>

[32] 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/>

[33] 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 IC ESB as defined in ICS 500-20^[12].