



Intelligence Community Technical Specification

CVE Encoding Specification for US Agency Acronyms

Version 2017-MARr2018-FEB

February 16, 2018

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	3
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.6.3 - 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	5
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	10
2.1 - Understanding Access Control	10
2.2 - Relationship to Abstract Data Definition and other encodings	11
2.3 - List Sources	11
2.4 - Additional Guidance	12
2.4.1 - Usage of the USAgency Schema	12
2.4.2 - Usage of the USAgency Schematron Library	12
2.5 - CSV Notes	13
2.6 - JSON Notes	13
2.7 - 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
3.7.5.2 - Revision Constraints	18
3.7.6 - Constraint Rules	19
3.8 - Data Rendering Constraint Rules	19
3.8.1 - Purpose	19

3.8.2 - Rendering Constraint Rules	20
Chapter 4 - Conformance Validation	21
4.1 - Schema Validation	21
4.2 - Business Rule Validation	21
Chapter 5 - Generated Guides	22
5.1 - Schema Guide	22
5.2 - Schematron Guide	23
Appendix A - Feature Summary	24
A.1 - USAgency Feature Comparison	24
Appendix B - Change History	25
B.1 - V2017-MARr2018-FEB Change Summary	25
B.2 - V2017-MAR Change Summary	26
B.3 - V2016-SEP Change Summary	27
B.4 - V2015-FEB Change Summary	28
B.5 - V2014-SEP Change Summary	28
Appendix C - List of Abbreviations	30
Appendix D - Bibliography	32
Appendix E - Points of Contact	36
Appendix F - IC CIO Approval Memo	37

List of Figures

Figure 1 - Inverse Dependency Specifications	7
Figure 2 - Three-legged Stool of Access Decisions	10

List of Tables

Table 1 - XML Namepaces	4
Table 2 - Dependencies	5
Table 3 - Numerical Rule Identifier Ranges	16
Table 4 - Revision Constraints table	19
Table 5 - Constraint Rules	20
Table 6 - Feature Summary Legend	24
Table 7 - USAgency Feature comparison	24
Table 8 - CES Version Identifier History	25
Table 9 - Data Encoding Specification V2017-MARr2018-FEB Change Summary	25
Table 10 - Data Encoding Specification V2017-MAR Change Summary	27
Table 11 - Data Encoding Specification V2016-SEP Change Summary	27
Table 12 - Data Encoding Specification V2015-FEB Change Summary	28
Table 13 - Data Encoding Specification V2014-SEP Change Summary	29

Chapter 1 - Introduction

1.1 - Purpose

This CVE Encoding Specification for US Agency Acronyms (USAgency.CES) defines detailed implementation guidance using several encoding formats including XML, and JSON to encode USAgency.CES controlled vocabulary. USAgency.CES is defined as the “top” level according to USA.gov of the Executive and Legislative branches of the government promoting any of the 16 IC members to the “top”. This list is intended to be used for multiple purposes. For the distribution of ORCON data, it includes a for ORCON-USGOV since OC-USGOV is limited to ONLY the Executive branch. For the exchange of enterprise audit records, it includes a CVE comprised of USAgency and an ICAS approved list of audit routing organizations. This 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.

1.2 - Scope

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

1.3 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC’s enterprise transformation to an “interoperable federated architecture.” Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* ^[1] 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* ^[17] the extensive and consistent use of Extensible Markup Language (XML) within data encoding

specifications allows for improved data exchanges and processing of information, thereby facilitating achievement of the IC's data discovery, data sharing, and interoperability goals.

An encoding specification defines a concrete implementation – a file format for example – for concepts in the *IC Abstract Data Definition* [2]. Many IC encoding specifications are based on XML, but other technologies are possible. For example, IC-ID[8] defines a plain-text format for IC Identifiers as well as an associated XML structure.

1.4 - Enterprise Need

Many IC encoding specifications use Controlled Vocabulary Enumerations (CVE)s to define allowable values for various elements and attributes. Each specification can define its own CVEs, but more than one specification may depend on the same list of values requiring additional maintenance to keep the lists aligned. Also, changes to a specification's CVEs require an entirely new version of that specification. CESes reduce maintenance burden and insulate specifications from vocabulary changes. Each CES contains one or more CVEs and optionally a master schema (defining elements and attributes limited to the CVE values) and/or Schematron rules.

This defines

- US Agency Acronym CVE. All valid Executive and Legislative branch acronyms
- US Gov Agency Acronym CVE. All valid Executive branch acronyms

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[5]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[11]
 - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[12]
 - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[17]
- 200 Series:
 - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[9]
 - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[10]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide[15]
- 700 Series:
 - Intelligence Community Directive (ICD) 710, Classification and Control Markings System[13]
 - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control[14]

1.5 - Audience and Applicability

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

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*, ^[16] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*, ^[3] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

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

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.” ^[18] 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 - 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 Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism
usagency	urn:us:gov:ic:usagency
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 - Dependencies

Name	Dependency Description
Schematron ^[22]	<p>Schematron — ISO/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 XSLT 2.0^[30] query binding.</p>
<p>XSLT 2.0^[30] implementation of Schematron^[22] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following URL: http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>
Value enumerations used for several XML structures are defined in the various Controlled Vocabulary Enumerations (CVEs) included in this CES.	This specification uses CVEs to encode controlled vocabularies. The use of the USAgency CVEs is normative.

1.7.3 - Inverse Dependencies

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

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

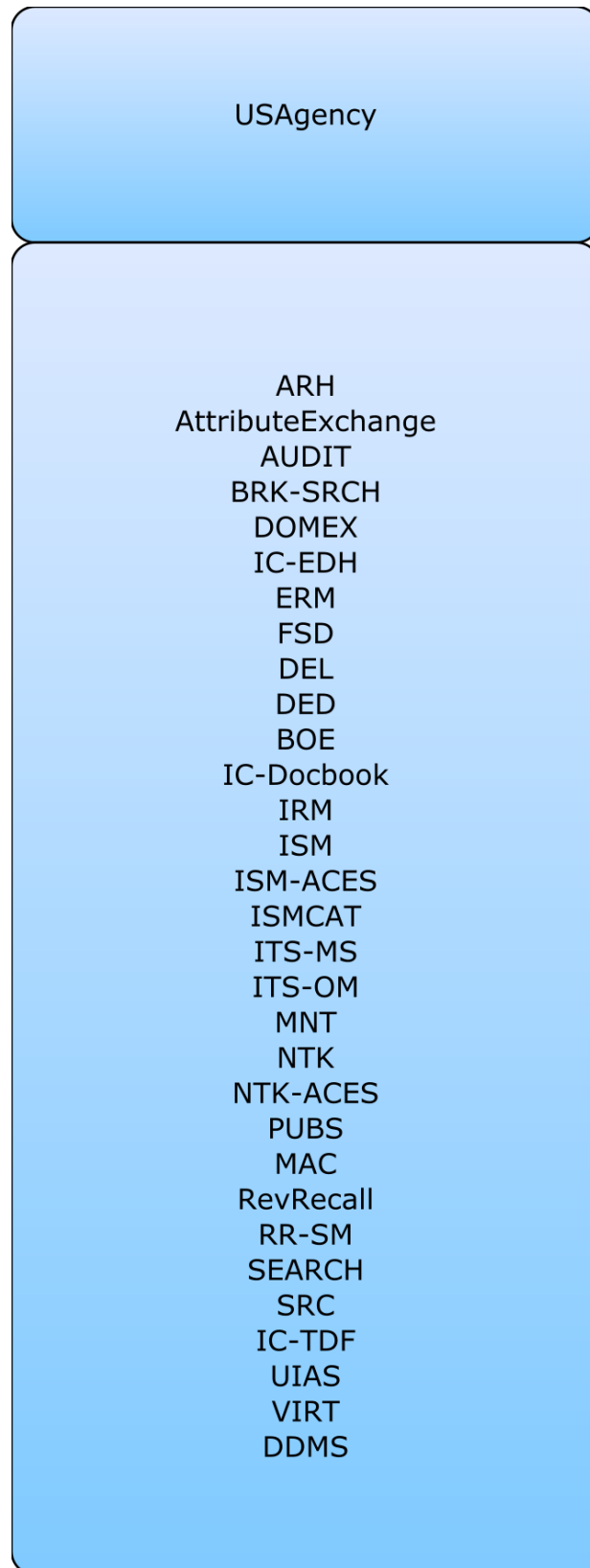


Figure 1 : Inverse Dependency Specifications

1.8 - Conformance

The XML schemas (unless noted otherwise), CVE values from the XML CVE files, and any Schematron^[22] rules are normative for this specification. The rest of this document and the rest of this package, including the descriptive content referenced within the XML Schema Guide, the XSL transformations, the SchematronGuide, and PDF CVE value files, are informative. Additionally, the use of keywords defined in IETF RFC 2119^[18] 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.^[28] For example, a schema could be changed to incorporate a different version of a dependency like ISM by changing the attribute declaration of **@ism:DESVersion='9'** to **@ism:DESVersion='10'** in the `xsd:schema` statement. The ability to specify which version of a dependent specification to import enables the configuration change control of parent specifications (such as PUBS and TDF) to be "decoupled" from the configuration change control of dependent specifications (such as ISM CVE updates). This "decoupling" method has not been in place for all versions of these parent specifications; therefore, please verify with the dependency table to ensure use of allowed dependency versions.

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

1.9 - Version Policies

1.9.1 - XML Namespace Policy

The XML namespaces defined in this specification do not incorporate a version number and do not change with revisions of the specification. This choice aligns with perspective two from "The Disposition of Names in an XML Namespace."^[23] This decision allows for systems that process information encoded with these specifications to use the same XPath expressions across multiple revisions. It was agreed the burden of updating all XPath based systems for every revision to the specification was unacceptable. See section 4.2.2 "Versioning and XML namespace policy" of "Architecture of the World Wide Web, Volume One."^[26]

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](#).

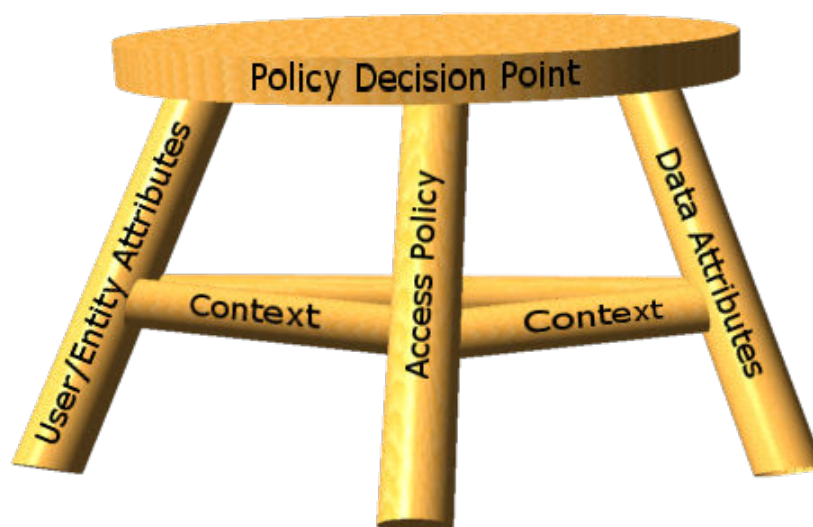


Figure 2 : Three-legged Stool of Access Decisions

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 falls into the user attributes leg of the access control framework. User attribute specifications include:

- Full Service Directory (FSD)^[4]
- Unified Identity Attribute Set (UIAS.XML)^[24]

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 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 - List Sources

The terms in the US Agency Acronym CVE list were either obtained directly or derived from the Members of the IC section of the dni.gov website,^[7] or from the Federal Executive Branch or Federal Legislative Branch sections of the usa.gov website^[25] which is reference from whitehouse.gov website. For the Federal Executive Agencies and the Federal Legislative Agencies which are references to usa.gov, the sub-bullets point to the major headings and include all immediate children of those unless otherwise specified. There is also an ICAS approved list of organizations unique to enterprise audit routing.

The lists in USAgency are derived from the following sources:

- Executive Branch:
 - Members of the IC Community [<http://www.dni.gov/index.php/intelligence-community/members-of-the-ic>]
 - Federal Executive Agencies [<http://www.usa.gov/Agencies/Federal/Executive.shtml>]
 - Executive Office of the President (as a single entity)
 - Cabinets (not named individuals) [<http://www.whitehouse.gov/administration/cabinet/>]
 - Executive Departments [http://www.usa.gov/Agencies/Federal/Executive.shtml#Executive_Departments]
 - Independent Agencies and Government Corporations [<http://www.usa.gov/Agencies/Federal/Independent.shtml>]
 - Boards, Commissions, and Committees (not Federal Advisory Committees) [<http://www.usa.gov/Agencies/Federal/Boards.shtml>]

- Quasi-Officials [<http://www.usa.gov/Agencies/Federal/Quasi-Official.shtml>]
- Legislative Branch:
 - United States Senate <http://www.senate.gov/>
 - Committee Offices (including Joint Committees) http://www.senate.gov/pagelayout/committees/d_three_sections_with_tasers/committees_home.htm
 - Offices of Senate-Elected Officers and Officials http://www.senate.gov/pagelayout/senators/a_three_sections_with_tasers/leadership.htm
 - United States House of Representatives <http://www.house.gov>
 - Committee Offices (including Joint Committees) <http://www.house.gov/committees/>
 - Offices and Organizations of the House http://www.house.gov/content/learn/officers_and_organizations/
 - Federal Legislative Agencies that Support Congress <http://www.usa.gov/Agencies/Federal/Legislative.shtml>
- ICAS approved list of organizations not in US Agency Acronym CVE

2.4 - 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 USAgency can use the USAgency.CES specification: through referencing objects defined in the schema or enforcing the format via running Schematron.

2.4.1 - Usage of the USAgency Schema

The USAgency.CES schema defines an element (USAgency) and an attribute (usagency) 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 USAgency.CES specification should import the USAgency 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 USAgency 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.

2.4.2 - Usage of the USAgency Schematron Library

The USAgency.CES Schematron library contains abstract rules that enforce allowed values as defined in the specification's CVEs (see [Section 3.7.4 - Value Enumeration Constraints](#) for more

details). Consumers of the USAgency.CES specification should include the abstract rule and define an implementation for it. The use of abstract rules allows the consumer to define the rule context and value that should be matched against a USAgency CVE.

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



Warning

The use of abstract patterns across specifications is being phased out. Abstract patterns are retained in USAgency.CES until older dependent specifications that use abstract patterns, such as IRM 2014-DEC, are retired. Developers SHOULD NOT use these patterns in new work.

2.5 - CSV Notes

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



Important

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

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

2.6 - JSON Notes

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

existence. The JSON files are formatted using JSON-LD based on a proposed method for JSON in NIEM.

2.7 - RELAX NG Notes

There are RELAX NG format files provided for all of the CVEs. They are in the CVE folder with the XML, JSON and CSV 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. USAgency.CES data validation constraint rule identifiers are prefixed with “USAgency-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 USAgency.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which USAgency.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^[22] 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^[22] rules for this specification may be executed in *Oxygen*^[21] or with an XSLT 2.0-compliant processor using the XSLT 2.0^[30] 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^[29] and XSLT 2.0^[30] features. Regarding the use of XPath 2.0 and XSLT 2.0 with Schematron, the editor of the ISO Schematron standard stated the following:^[20]

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^[30] implementation of Schematron^[22] 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

The purpose of the USAgency.CES specification is to define the CVE list for allowable Agency Acronym values.

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

¹“White space” is defined in XML 1.0^[27] as “(white space) consists of one or more space (#x20) characters, carriage returns, line feeds, or tabs.”

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.

3.7.5.2 - Revision Constraints

When validating an instance document against the validation rule sets and schema provided by the specification there is a certain philosophy that **SHOULD** be applied to both protect the data and the systems processing that data. This validation philosophy consists of the following seven basic rules that describe how the DESVersion matters to validation:

1. One **MUST NOT** validate with rules older than the integer version declared in an instance; this is an error.
2. One **MAY** validate with rules that are of a greater integer version than an instance.
3. When validating an instance with a lower integer version number than that of the validation rules, there **MAY** be a minimum integer version cutoff for a set of rules. If such a limit exists, this is an error.
4. Within an integer, validation **MUST** only occur with the newest decimal value implemented by the validator; that is a validator **MUST** only implement one signed validation rule set within an integer and it **SHOULD** be the latest.
5. When a validator detects an instance document claiming a version newer than what is implemented in the validator, a notice/log **SHOULD** be generated so a human can evaluate if the validator needs to be updated to the latest rule set, as passing the old rules **MAY** not comply with current law or policy.
6. A validator **SHOULD** document and communicate all versions and revisions it accepts, including the constraints (business/policy rules, allowed values, schema formats, etc.) in each of those versions.

The matrix of fictional generic examples in [Table 4](#) are provided to illustrate these validation concepts with the following assumptions:

- Version 11: Technically incompatible with newer versions
- Version 12: Technically compatible with newer versions, but retired from the Enterprise Standards Baseline

- Version 13: Oldest in the Enterprise Standards Baseline
- Version 13.201701: Revision to version 13
- Version 13.201804: Revision to version 13
- Version 201508: Standard release
- Version 201609: Latest version release

Table 4 - Revision Constraints table

Validation Rules Version	11	12	13	13.201701	13.201804	201508	201609
Instance Version							
11	Version Match	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)	Instance Too Old (Tech)
12	Instance Too New	Version Match	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)	Instance Too Old (ESB)
13	Instance Too New	Instance Too New	Version Match	Same Integer	Same Integer	Allowed	Allowed
13.201701	Instance Too New	Instance Too New	Same Integer	Version Match	Same Integer	Allowed	Allowed
13.201804	Instance Too New	Instance Too New	Same Integer	Same Integer	Version Match	Allowed	Allowed
201508	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match	Allowed
201609	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Instance Too New	Version Match

3.7.6 - Constraint Rules

The detailed constraint rules for the USAgency.CES schema can be found in a separate document inside the SchematronGuide directory, in the USAgency_Rules.pdf file. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron. Obsolete rule numbers are listed in the SchematronGuide.

3.8 - Data Rendering Constraint Rules

3.8.1 - Purpose

Rendering rules define constraints on the rendering and display of USAgency.CES documents. The intent is to inform the development of systems capable of rendering or displaying

USAgency.CES data for use by individuals not familiar with the details of the USAgency.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 USAgency.CES data rendering constraint rules.

Table 5 - Constraint Rules

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

Chapter 4 - Conformance Validation

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

4.1 - Schema Validation

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

4.2 - Business Rule Validation

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

Chapter 5 - Generated Guides

5.1 - Schema Guide

The detailed description and reference documentation for the USAgency.CES schema can be found as a collection of HTML files inside the SchemaGuide directory. These files comprise a guide that serves as an interactive presentation of the USAgency.CES schema as well as an implementation-specific data element dictionary.

The guide was generated with a commercially available product named *oXygen@*, [\[21\]](#) 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 USAgency.CES Schematron rules can be found in a separate document named *USAgency_Rules.pdf*, which is located inside the SchematronGuide directory. This document is generated from the individual Schematron files to provide a single searchable document for all of the constraint rules encoded in Schematron.

Appendix A Feature Summary

The following table summarizes major features by version for US Agency Acronyms and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. For those changes driven by the IC Markings System Register and Manual, the date is often one year after the date of publication. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

Table 6 - Feature Summary Legend

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

A.1. USAgency Feature Comparison

Table 7 - USAgency Feature comparison

USAgency Feature Comparison							
Required date	Feature	V1	2014-SEP	2015-FEB	2016-SEP	2017-MAR	2017-MARr2018-FEB
	Defines the allowable values for US Agency Acronyms	F	F	F	F	F	F
	Support ORCON USGov with the USGovAgency CVE	N	N	N	F	F	F
	Add CVE auditRoutingOrganization	N	N	N	F	F	F
	Add CVE auditRoutingUnique	N	N	N	F	F	F
	Treat enforcement of CESVersion as a warning	N	N	N	N	N	F

Appendix B Change History

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

Table 8 - CES Version Identifier History

Version	Date	Purpose
1	August 16, 2013	Initial Release
2014-SEP	September 16, 2014	Routine revision to technical specification. For details of changes, see Section B.5 - V2014-SEP Change Summary
2015-FEB	February 2, 2015	Routine revision to technical specification. For details of changes, see Section B.4 - V2015-FEB Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.3 - V2016-SEP Change Summary
2017-MAR	March 13, 2017	Routine revision to technical specification. For details of changes, see Section B.2 - V2017-MAR Change Summary
2017-MARr2018-FEB	February 16, 2018	Routine revision to technical specification. For details of changes, see Section B.1 - V2017-MARr2018-FEB Change Summary

B.1 - V2017-MARr2018-FEB Change Summary

Significant drivers for Version 2017-MAR include:

- Correct bug in *CESVersion* which hampered usage.
- Update to align with content and constructs being propagated to all IC CIO specifications.

The following table summarizes the changes made to 2017-MAR in developing 2017-MARr2018-FEB.

Table 9 - Data Encoding Specification V2017-MARr2018-FEB Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Correct <i>CESVersion</i> bug from 2017-MAR release by enforcing the <i>CESVersion</i> value with a warning Schematron rule. (CR-2018-004, CR-2017-097, CR-2017-234)	Schema Schematron USAgency-ID-00001 added	Data generation and ingesting systems will have to be updated to handle the change in the code.
2	Update documentation of version number to reflect the existence of revisions (CR-2017-259)	Documentation	This change has minimal impact to implementations.

#	Change	Artifacts changed	Compatibility Notes
3	Create RelaxNG forms of CVEs (CR-2017-188)	RelaxNG Fragments added	This change has no impact to existing implementations, but offers a different format for digesting the CVE values.
4	Create JSON forms of CVEs (CR-2017-069)	JSON CVE files added	This change has no impact to existing implementations, but offers a different format for digesting the CVE values.
5	Create CSV forms of CVEs (CR-2017-047)	CSV CVE files added	This change has no impact to existing implementations, but offers a different format for digesting the CVE values.
6	Fixed maxLength inconsistencies within CVE documentation (CR-2016-079)	Documentation	This change has no impact to implementations.
7	Updated dependency information to document inverse dependencies. (CR-2017-126)	Documentation	This change has no impact to implementations.
8	Added schema PDF. (CR-2018-030)	Documentation	No impact to systems.
9	Added ISM.XML ^[19] attributes to Schematron files to mark up the documentation. (CR-2017-318)	Schematron	No impact to systems.
10	Updated Purpose section to be less XML centric. (CR-2018-059)	Documentation	No impact to systems.

B.2 - V2017-MAR Change Summary

Significant drivers for Version 2017-MAR include:

- Requirement of White House Military Office for provisioning.

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

Table 10 - Data Encoding Specification V2017-MAR Change Summary

Change	Artifacts changed	Compatibility Notes
Added new token, White House Military Office, to the executive branch entities (CR-2017-012)	CVEnum-AuditRoutingOrg.xml updated CVEnum-USAgencyAcronym.xml updated CVEnum-USGOVAgencyAcronym.xml updated	Data generation and ingesting systems will have to be updated to handle the change in the code.

B.3 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Consolidation of USAgency and USGovAgency.
- decision to create auditRoutingOrganization

The following table summarizes the changes made to 2015-FEB in developing 2016-SEP.

Table 11 - Data Encoding Specification V2016-SEP Change Summary

Change	Artifacts changed	Compatibility Notes
USGovAgency CES collapsed into USAgency. Abstract Schematron rule for USGovAgency CVE not ported since we no longer use Abstract Schematron rules across specifications. (CR-2016-012)	CVEnum-USGovAgencyAcronym.xml added	Data generation and ingesting systems that use USGovAgency will need to adopt USAgency.
auditRoutingOrganization CVE added to support routing of enterprise audit records. (CR-2015-018)	CVEnum-AuditRoutingOrg.xml added	Data generation and ingesting systems that route Audit Records or provision the attribute will need to adopt auditRoutingOrganization.
auditRoutingUnique CVE added to support routing of enterprise audit records and provide a source for auditRoutingOrg values that do not appear in USAgency CVE. (CR-2015-018)	CVEnum-AuditRoutingUnique.xml added	CVE provided for convenience and clarity of auditRoutingOrg unique values.

Change	Artifacts changed	Compatibility Notes
Documentation cleanup. (CR-2015-031, CR-2015-111)	USAgency.xsd updated CVEnum- USAgencyAcronym.xml updated	No impact to systems.
The schema change logs will no longer be maintained as of the 2016-SEP release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2016-SEP, reference the change history in the CES.	Schema	No impact to systems.
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.4 - V2015-FEB Change Summary

Significant drivers for Version 2015-FEB include:

- Office of Legislative Affairs requirements for provisioning users

The following table summarizes the changes made to 2014-SEP in developing 2015-FEB.

Table 12 - Data Encoding Specification V2015-FEB Change Summary

Change	Artifacts changed	Compatibility Notes
Added tokens for the following legislative branch entities: <ul style="list-style-type: none"> • Committee Offices (House and Senate) • Offices of Senate-Elected Officers and Officials • Offices and Organizations of the House 	CVEnum- USAgencyAcronym.xml	Data generation and ingesting systems will have to be updated to handle the change in the code.

B.5 - V2014-SEP Change Summary

Significant drivers for Version 2014-SEP include:

- Alignment with Marking System Register and Manual 31 December 2013^[6]
- Community Coding request to remove the '&' special characters

The following table summarizes the changes made to V1 in developing 2014-SEP.

Table 13 - Data Encoding Specification V2014-SEP Change Summary

Change	Artifacts changed	Compatibility Notes
Updated code ONCE to ONCIX.	CVEnum- USAgencyAcronym.xml	Data generation and ingesting systems will have to be updated to handle the change in the code.
Corrected code USPC to USCP.	CVEnum- USAgencyAcronym.xml	Data generation and ingesting systems will have to be updated to handle the change in the code.
Replaced ampersands with underscores in CVE values (H-E&C, H-T&I, H-W&M, and S-R&A)	CVEnum- USAgencyAcronym.xml	Data generation and ingesting systems will have to be updated to handle the change in the codes.
Corrected ISMCATCESVersion to replace 12 with 2.	CVEnum- USAgencyAcronym.xml	Minor correction to metadata in CVE should have minimal or no impact to implementing systems.

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
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
FOUO	For Official Use Only
HTML	HyperText Markup Language
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
ICAS	Intelligence Community Audit Subcommittee
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISM	Information Security Markings
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
NIEM	National Information Exchange Model

OCIO	Office of the Intelligence Community Chief Information Officer
OC-USGOV	An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies.
ODNI	Office of the Director of National Intelligence
ORCON	See OC.
PDP	Policy Decision Point
PUBS	Intelligence Publications
RELAX NG	REgular LAnguage for XML Next Generation
RFC	Request for Comments
TDF	Trusted Data Format
URL	Uniform Resource Locator
US	United States
XML	Extensible Markup Language
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D Bibliography

Bibliography

[1] ABNF

Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*.
Available online at: <http://tools.ietf.org/html/std68>
Also known as: <http://www.ietf.org/rfc/rfc5234.txt>

[2] ADD

Office of the Director of National Intelligence. *Intelligence Community Abstract Data Definition (IC-ADD.XML)*.
Available online Intelink-TS at: <http://go.ic.gov/soSC6M8>
Available online Intelink-U at: <https://w3id.org/ic/standards/ADD>
Available online at: <https://w3id.org/ic/standards/public>

[3] DoD Instruction 8310.01

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

[4] FSD

Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD)*.
Available online Intelink-TS at: <http://go.ic.gov/iZiePDW>
Available online Intelink-U at: <https://w3id.org/ic/standards/FSD>
Available online at: <https://w3id.org/ic/standards/public>

[5] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: <http://go.ic.gov/4X6TOc1>

[6] IC Markings

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

[7] IC MEMBERS

Director of National Intelligence. *Members of the IC*.
Available online at: <https://www.dni.gov/index.php/what-we-do/members-of-the-ic>

[8] IC-ID.XML

Office of the Director of National Intelligence. *Text and XML Data Encoding Specification for Intelligence Community Identifier (IC-ID.XML)*.
Available online Intelink-TS at: <http://go.ic.gov/mQ4IUDk>
Available online Intelink-U at: <https://w3id.org/ic/standards/IC-ID>

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

[9] 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

[10] 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>

[11] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <http://go.ic.gov/5Ot5sbK>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[12] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <http://go.ic.gov/GG61roi>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[13] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[14] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <http://go.ic.gov/0d147Ee>

Available online at: <http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf>

[15] 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>

[16] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <http://go.ic.gov/sLKNq3N>

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[17] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <http://go.ic.gov/cWyv9nw>

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[18] 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>

[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: <http://go.ic.gov/3oipfOY>

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

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

[20] Jelliffe

Richard Alan Jelliffe. *FAQ. Frequently Asked Questions: Is Schematron tied to XSLT 1.0?*.

Available online at: <http://www.schematron.com>

[21] Oxygen

SyncRO Soft. *<oXygen/> XML Editor*.

Available online at: <http://www.oxygenxml.com/>

[22] 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/>

[23] 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>

[24] 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: <http://go.ic.gov/H8RwEw8>

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

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

[25] USA.GOV

USA.gov. United States of America Government

Available online at: <http://www.usa.gov>

[26] 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>

[27] 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>

[28] 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>

[29] 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/>

[30] XSLT2

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

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

Appendix E Points of Contact

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

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

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

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

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

Appendix F IC CIO Approval Memo

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

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

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.^[16]