Intelligence Community Technical Specification

CVE Encoding Specification for US Agency Acronyms

Version 2022-JUL

December 1, 2022

Table of Contents

Chapter 1 - Introduction 1
1.1 - Purpose 1
1.2 - Scope 1
1.3 - Enterprise Need 1
1.4 - Conventions 2
1.4.1 - XML Namespaces 2
1.5 - Dependencies 3
1.5.1 - Specification Dependencies 3
1.5.2 - Inverse Dependencies 5
Chapter 2 - Development Guidance 7
2.1 - List Sources 7
2.2 - Understanding Access Control 8
Chapter 3 - Constraints 9
3.1 - Data Validation Constraint Rules 9
3.1.1 - Purpose 9
3.1.2 - Value Enumeration Constraints 9
3.1.3 - Additional Constraints 9
3.1.3.1 - CES Constraints 9
3.1.4 - Constraint Rules 9
3.2 - Data Rendering Constraint Rules 10
3.2.1 - Purpose 10
3.2.2 - Rendering Constraint Rules 10
Appendix A - Feature Summary 11
A.1 - USAgency Feature Comparison 11
A.1.1 - Features from V2017-MAR to V2022-JUL 11
A.1.2 - Features from V2014-SEP to V2017-MAR 11
A.1.3 - Features from V1 to V2014-SEP 12
Appendix B - Change History 13
B.1 - V2022-JUL Change Summary 13
B.2 - V2021-NOV Change Summary 14
B.3 - V2017-MARr2018-FEB Change Summary 15
B.4 - V2017-MAR Change Summary 16
B.5 - V2016-SEP Change Summary 17
B.6 - V2015-FEB Change Summary 18
B.7 - V2014-SEP Change Summary 19
Appendix C - List of Abbreviations 20
Appendix D - Bibliography 22
Appendix E - Points of Contact 25
Appendix F - IC CIO Approval Memo 26

List of Figures

Figure 1 - Related Specifications 5
Figure 2 - Inverse Dependency Specifications 6

List of Tables

Table 1 - XML Namepaces 2
Table 2 - Dependencies 3
Table 3 - Constraint Rules 10
Table 4 - Feature Summary Legend 11
Table 5 - USAgency Feature comparison V2017-MAR to V2022-JUL 11
Table 6 - USAgency Feature comparison V2014-SEP to V2017-MAR 11
Table 7 - USAgency Feature comparison V1 to V2014-SEP 12
Table 8 - CES Version Identifier History 13
Table 9 - Data Encoding Specification V2022-JUL Change Summary 14
Table 10 - Data Encoding Specification V2021-NOV Change Summary 15
Table 11 - Data Encoding Specification V2017-MARr2018-FEB Change Summary 16
Table 12 - Data Encoding Specification V2017-MAR Change Summary 17
Table 13 - Data Encoding Specification V2016-SEP Change Summary 17
Table 14 - Data Encoding Specification V2015-FEB Change Summary 19
Table 15 - Data Encoding Specification V2014-SEP Change Summary 19

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 Extensible Markup Language (XML) and JavaScript Object Notation (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 18 Intelligence Community (IC) members to the “top”. This list is intended to be used for multiple purposes. For the distribution of Originator Controlled (ORCON) data, it includes a Controlled Vocabulary Enumeration (CVE) for ORCON-USGOV since An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies. (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 Intelligence Community Audit Subcommittee (ICAS) approved list of audit routing organizations. This Controlled Vocabulary Enumeration 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

The *Intelligence Community Technical Specification Framework* (IC-SF.XML[4]) defines the basic conceptual structure and outlines the core philosophy of IC technical specifications. For convenience, a copy of this framework is included in every package.

This specification is applicable to the IC and information produced by, stored, or shared within the IC. This 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 - 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 CES, 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 USAgency CVEs.

- “CVEnumUSAgencyAcronym” contains all valid Executive and Legislative branch acronyms.

- “CVEnumUSGOVAgencyAcronym” contains all valid Executive branch acronyms.

- “CVEnumAuditRoutingOrg” contains all valid Executive and Legislative branch acronyms along with additional audit routing unique organizational acronyms.

USAgency is used for audit routing in *XML Data Encoding Specification for Enterprise Audit Exchange* (AUDIT.XML[1]) and to enable Attribute Based Access Control (ABAC) for ORCON and Exclusive Distribution (EXDIS) Need-To-Know Metadata (NTK) in *XML Data Encoding Specification for Information Security Markings* (ISM.XML[14]).

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

- 200 Series:
  - Intelligence Community Directive (ICD) 208, *Write for Maximum Utility* [5]
  - ICD 209, *Tearline Production and Dissemination* [6]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community’s Responsibility to Provide* [11]
- 500 Series:
  - ICD 500, *Director Of National Intelligence Chief Information Officer* [7]
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [8]
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* [12]
  - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* [13]
- 700 Series:
  - ICD 710, *Classification and Control Markings System* [9]
  - Intelligence Community Program Guidance (ICPG) 710.1, *Application of Dissemination Controls: Originator Control* [10]

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the “Specification Conventions” chapter in the IC-SF.XML[4].

1.4.1 - XML Namespaces

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

Table 1 - XML Namepaces

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

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML[4].

1.5.1 - Specification Dependencies

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

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

Table 2 - Dependencies

Name	Dependency Description
Intelligence Community Specification Framework (IC-SF.XML.V2021-NOV+[4])	This specification does not depend on a specific version of IC-SF.XML[4]; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.

Name	Dependency Description
Schematron[15]	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. The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. Note: The Schematron rules in this specification use Transformations (XSLT) 2.0[17] query binding.
XSLT 2.0[17] implementation of Schematron[15] by Rick Jelliffe (2010-04-14) Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/.	The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the *behavior* of the implementation created by Mr. Jelliffe is normative. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid *if and only if* the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.

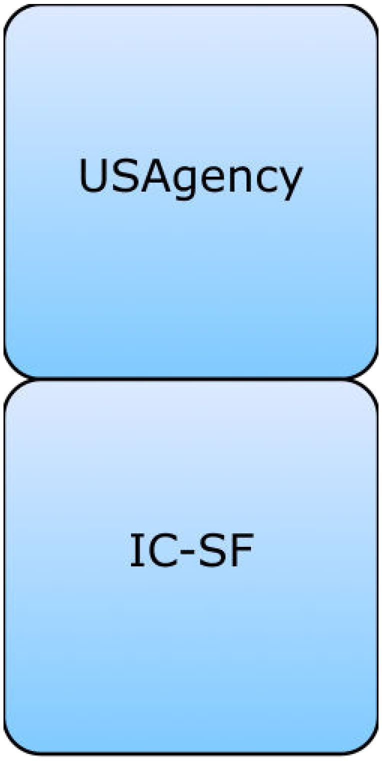

Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

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

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

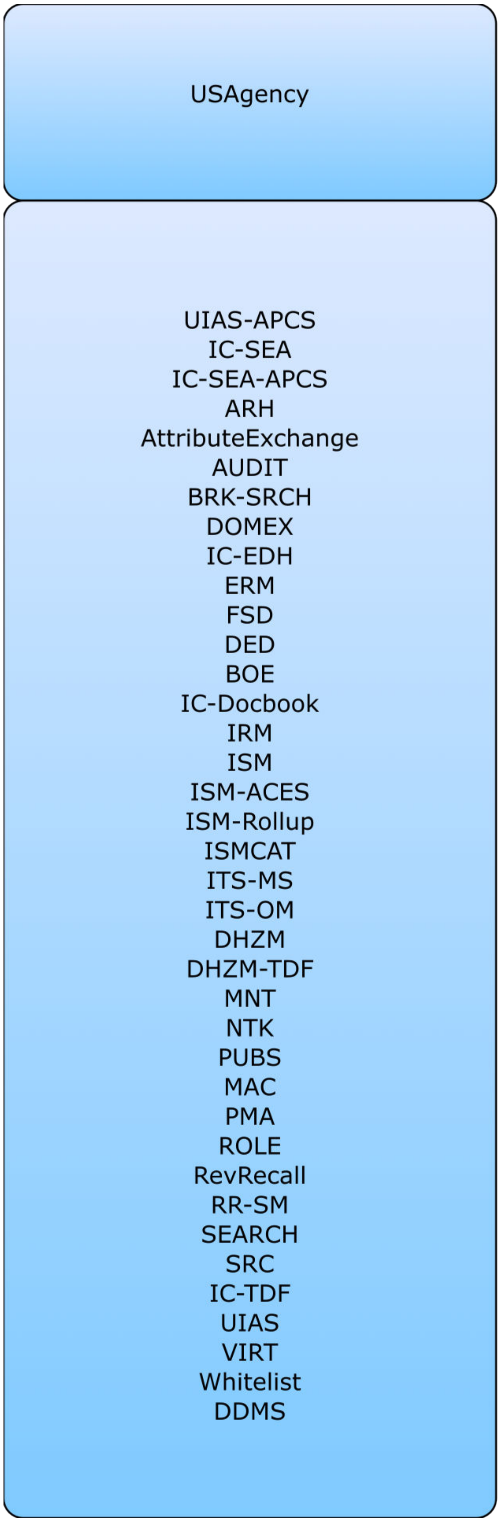

Figure 2 : Inverse Dependency Specifications

Chapter 2 - Development Guidance

2.1 - List Sources

The terms in the United States (US) Agency Acronym CVE list were either obtained directly or derived from the Members of the IC section of the dni.gov website[3] or from the Federal Executive Branch or Federal Legislative Branch sections of the usa.gov website[16] which is referenced 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 [https://www.dni.gov/index.php/what-we-do/members-of-the-ic]
  - Federal Executive Agencies [https://www.usa.gov/branches-of-government]
    - Executive Office of the President (as a single entity)
    - Cabinets (not named individuals)
    - Executive Departments
    - Independent Agencies and Government Corporations
    - Boards, Commissions, and Committees (not Federal Advisory Committees)
    - Quasi-Officials
- Legislative Branch:
  - United States Senate http://www.senate.gov/
    - Committee Offices (including Joint Committees) http://www.senate.gov/pagelayout/committees/d_three_sections_with_teasers/committees_home.htm
    - Offices of Senate-Elected Officers and Officials http://www.senate.gov/pagelayout/senators/a_three_sections_with_teasers/leadership.htm
  - United States House of Representatives http://www.house.gov
    - Committee Offices (including Joint Committees) http://www.house.gov/committees/
    - Officers and Organizations of the House https://www.house.gov/the-house-explained/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

2.2 - Understanding Access Control

This specification participates in the Data Attributes and User/Entity Attributes legs of the access control framework either as a primary specification or as a dependency of a primary specification. For more information, please see the “Components of Access Control Decisions” chapter in the IC-SF.XML[4] framework document.

The data attributes component of the policy framework provides a common understanding of IC metadata to enable precise access control decisions. Without this common understanding the IC Enterprise is missing a crucial data attribute component to make accurate, reliable, and automated access control decisions. The USAgency.CES specification provides a common encoding (e.g., common understanding) and foundation for data attributes specifications that use US agency acronyms.

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

3.1.1 - Purpose

The USAgency.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which 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.

3.1.2 - Value Enumeration Constraints

Several elements and attributes of the USAgency.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 may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

Some CVEs are not available on all networks. A subset CVE will be provided for use on networks not approved for the entire list. If the processing will occur on a network where the entire CVE is not available, the subset CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

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

3.1.3 - Additional Constraints

3.1.3.1 - 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.

3.1.4 - Constraint Rules

The detailed constraint rules for the USAgency.CES schema can be found in a separate document inside the Documents/USAgency 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 “USAgency_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - 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.

3.2.2 - Rendering Constraint Rules

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

Table 3 - Constraint Rules

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

Appendix A Feature Summary

The following table summarizes major features by version for USAgency.CES 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, *Intelligence Community Markings System Register and Manual* [2], the date is often one year after the date of publication. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates.

Table 4 - Feature Summary Legend

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

A.1. USAgency Feature Comparison

A.1.1. Features from V2017-MAR to V2022-JUL

Table 5 - USAgency Feature comparison V2017-MAR to V2022-JUL

Required date	Feature	V2017-MAR	V2017-MARr2018-FEB	V2021-NOV	V2022-JUL
	Treat enforcement of CESVersion as a warning	N	F	F	F
	Add "USA." prefix to all USAgency values	N	N	F	F
	Added "USA.DFC"	N	N	N	F

A.1.2. Features from V2014-SEP to V2017-MAR

Table 6 - USAgency Feature comparison V2014-SEP to V2017-MAR

Required date	Feature	V2014-SEP	V2015-FEB	V2016-SEP	V2017-MAR
	Support ORCON USGov with the USGovAgency CVE	N	N	F	F
	Add CVE auditRoutingOrganization	N	N	F	F
	Add CVE auditRoutingUnique	N	N	F	F

A.1.3. Features from V1 to V2014-SEP

Table 7 - USAgency Feature comparison V1 to V2014-SEP

Required date	Feature	V1	V2014-SEP

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.7 - V2014-SEP Change Summary
2015-FEB	February 2, 2015	Routine revision to technical specification. For details of changes, see Section B.6 - V2015-FEB Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.5 - V2016-SEP Change Summary
2017-MAR	March 13, 2017	Routine revision to technical specification. For details of changes, see Section B.4 - V2017-MAR Change Summary
2017-MARr2018-FEB	February 16, 2018	Routine revision to technical specification. For details of changes, see Section B.3 - V2017-MARr2018-FEB Change Summary
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see Section B.2 - V2021-NOV Change Summary
2022-JUL	July 1, 2022	Routine revision to technical specification. For details of changes, see Section B.1 - V2022-JUL Change Summary

B.1 - V2022-JUL Change Summary

Significant drivers for Version 2022-JUL include:

- Community Change Requests

Table 9 summarizes the changes made to this technical specification from version 2021-NOV to version 2022-JUL.

Table 9 - Data Encoding Specification V2022-JUL Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Added "USA.DFC" which replaces "USA.OPIC". (CR-2022-024)	CVEnum-AuditRoutingOrg.xml updated CVEnum-USAgencyAcronym.xml updated CVEnum-USGOVAgencyAcronym.xml updated Schematron USAgency-ID-00002 added USAgency-ID-00003 added USAgency-ID-00004 added USAgency-ID-00005 added USAgency-ID-00006 added USAgency-ID-00007 added	Systems may need to be updated to handle new/updated values and the change in the code.

B.2 - V2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- Community Change Requests

Table 10 summarizes the changes made to this technical specification from version 2017-MARr2018-FEB to version 2021-NOV.

Table 10 - Data Encoding Specification V2021-NOV Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Change format of foreign partner organizations to match IC-SEA and 5EE. (CR-2019-003)	CVEnum-AuditRoutingOrg.xml updated CVEnum-AuditRoutingUnique.xml updated CVEnum-USAgencyAcronym.xml updated CVEnum-USGOVAgencyAcronym.xml updated	Systems may need to be updated to handle new/updated values.
2	Updated documentation to use the specification framework. (CR-2019-043)	Documentation	No impact to systems.
3	Updated CSV generation to include a column for deprecation date information. (CR-2018-089)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.
4	Updated Schema Guide Implementation Notes to identify the lack of a root node. (CR-2019-128)	Documentation	No impact to systems.
5	Add U.S. Space Force (USSF). (CR-2021-009)	CVEnum-USAgencyAcronym.xml updated	Systems may need to be updated to handle new/updated values.

B.3 - 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.

Table 11 summarizes the changes made to this technical specification from version 2017-MAR to version 2017-MARr2018-FEB.

Table 11 - Data Encoding Specification V2017-MARr2018-FEB Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Correct CESVersion bug from 2017-MAR release by enforcing the CESVersion 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.
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[14] 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.4 - V2017-MAR Change Summary

Significant drivers for Version 2017-MAR include:

- Requirement of White House Military Office for provisioning.

Table 12 summarizes the changes made to this technical specification from version 2016-SEP to version 2017-MAR.

Table 12 - Data Encoding Specification V2017-MAR Change Summary

#	Change	Artifacts changed
1	Added new token, White House Military Office, to the executive branch entities (CR-2017-012)	CVEnumAuditRoutingOrg.xml updated CVEnumUSAgencyAcronym.xml updated CVEnum-USGOVAgencyAcronym.xml updated

B.5 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

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

Table 13 summarizes the changes made to this technical specification from version 2015-FEB to version 2016-SEP.

Table 13 - Data Encoding Specification V2016-SEP Change Summary

#	Change	Artifacts changed
1	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
2	auditRoutingOrganization CVE added to support routing of enterprise audit records. (CR-2015-018)	CVEnumAuditRoutingOrg.xml added

#	Change	Artifacts changed
3	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
4	Documentation cleanup. (CR-2015-031, CR-2015-111)	USAgency.xsd updated CVEnumUSAgencyAcronym.xml updated
5	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
6	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation

B.6 - V2015-FEB Change Summary

Significant drivers for Version 2015-FEB include:

- Office of Legislative Affairs requirements for provisioning users

Table 14 summarizes the changes made to this technical specification from version 2014-SEP to version 2015-FEB.

Table 14 - Data Encoding Specification V2015-FEB Change Summary

#	Change	Artifacts changed
1	Added tokens for the following legislative branch entities: • Committee Offices (House and Senate) • Offices of Senate-Elected Officers and Officials • Offices and Organizations of the House	CVEnumUSAgencyAcronym.xml

B.7 - V2014-SEP Change Summary

Significant drivers for Version 2014-SEP include:

- Alignment with Marking System Register and Manual 31 December 2013[2]

- Community Coding request to remove the '&' special characters

Table 15 summarizes the changes made to this technical specification from version V1 to version 2014-SEP.

Table 15 - Data Encoding Specification V2014-SEP Change Summary

#	Change	Artifacts changed
1	Updated code ONCE to ONCIX.	CVEnumUSAgencyAcronym.xml
2	Corrected code USPC to USCP.	CVEnumUSAgencyAcronym.xml
3	Replaced ampersands with underscores in CVE values (H-E&C, H-T&I, H-W&M, and S-R&A)	CVEnumUSAgencyAcronym.xml
4	Corrected ISMCATCESVersion to replace 12 with 2.	CVEnumUSAgencyAcronym.xml

Appendix C List of Abbreviations

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

ABAC	Attribute Based Access Control
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
EXDIS	Exclusive Distribution
IC	Intelligence Community
ICAS	Intelligence Community Audit Subcommittee
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
NTK	Need-To-Know Metadata
OC-USGOV	An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies.
ORCON	Originator Controlled
URL	Uniform Resource Locator
US	United States
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

XSLT	XSL Transformations

Appendix D Bibliography

[1] AUDIT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Audit Exchange (AUDIT.XML)*.
Available online Intelink-TS at: https://go.ic.gov/Og5CcLk (case sensitive – Oscar golf 5 Charlie charlie Lima kilo)
Available online Intelink-U at: https://w3id.org/ic/standards/AUDIT

[2] 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: https://go.ic.gov/tGXkwGO (case sensitive – tango Golf Xray kilo whiskey Golf Oscar)
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings

[3] 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

[4] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.
Available online Intelink-TS at: https://go.ic.gov/pNFyuVg (case sensitive – papa November Foxtrot yankee uniform Victor golf)
Available online Intelink-U at: https://w3id.org/ic/standards/IC-SF
Available online at: https://w3id.org/ic/standards/public

[5] 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

[6] 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

[7] 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

[8] 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

[9] ICD 710
Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.
Available online Intelink-TS at: https://go.ic.gov/oSj9K7O (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)
Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[10] 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: https://go.ic.gov/fdyoyIS (case sensitive – foxtrot delta yankee oscar yankee India Sierra)
Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf

[11] 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

[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] 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

[15] Schematron
International Organization for Standardization (ISO). *Information technology -- Document Schema Definition Language (DSDL) -- Part 3: Rule-based validation -- Schematron*. ISO/IEC 19757-3:2006.
ISO Spec Available online at: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
StyleSheets for compiling Available online at: http://code.google.com/p/schematron/

[16] USA.GOV
USA.gov. United States of America Government
Available online at: http://www.usa.gov

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

Appendix E Points of Contact

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

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

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

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

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

Appendix F IC CIO Approval Memo

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

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

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20[12].