



# **Intelligence Community Technical Specification**

---

## **CVE Encoding Specification for Mission Need**

**Version 2021-NOV**

December 1, 2022

Distribution Notice:

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

# Table of Contents

Chapter 1 - Introduction .....	1
1.1 - Purpose .....	1
1.2 - Scope .....	1
1.3 - Enterprise Need .....	1
1.4 - Conventions .....	2
1.4.1 - XML Namespaces .....	2
1.5 - Dependencies .....	2
1.5.1 - Specification Dependencies .....	2
1.5.2 - Inverse Dependencies .....	5
Chapter 2 - Development Guidance .....	7
2.1 - Relationship to Abstract Data Definition and other encodings .....	7
2.2 - Understanding Access Control .....	7
2.3 - Additional Guidance .....	7
2.3.1 - Usage of the MN Schema .....	7
2.3.2 - Usage of the MN Schematron Library .....	8
Chapter 3 - Constraints .....	9
3.1 - Data Validation Constraint Rules .....	9
3.1.1 - Value Enumeration Constraints .....	9
3.1.2 - Additional Constraints .....	9
3.1.2.1 - CES Constraints .....	9
3.1.3 - Constraint Rules .....	9
3.2 - Data Rendering Constraint Rules .....	9
3.2.1 - Purpose .....	9
3.2.2 - Rendering Constraint Rules .....	10
Appendix A - Feature Summary .....	11
A.1 - MN Feature Summary .....	11
Appendix B - Change History .....	12
B.1 - 2021-NOV Change Summary .....	12
B.2 - 2017-MAYr2019-MAR Change Summary .....	13
B.3 - 2017-MAY Change Summary .....	13
Appendix C - Glossary .....	15
Appendix D - List of Abbreviations .....	16
Appendix E - Bibliography .....	17
Appendix F - Points of Contact .....	19
Appendix G - IC CIO Approval Memo .....	20

# List of Figures

Figure 1 - Related Specifications ..... 4

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 - MN Feature Comparison .....	11
Table 6 - CES Version Identifier History .....	12
Table 7 - Data Encoding Specification 2021-NOV Change Summary .....	12
Table 8 - Data Encoding Specification 2017-MAYr2019-MAR Change Summary .....	13
Table 9 - Data Encoding Specification 2017-MAY Change Summary .....	13

## Chapter 1 - Introduction

### 1.1 - Purpose

This *CVE Encoding Specification for Mission Need* (MN.CES) defines controlled vocabularies for geographic regions and issue categories related to GIMMEE Mission Need Profiles. This Controlled Vocabulary Enumeration Encoding Specification (CES) provides controlled vocabularies that map directly to regions and issues used in Mission Need Profiles for use in CES instance documents, as entity attributes, and by systems making access control decisions.

### 1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML<sup>[2]</sup>) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

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

This CES defines Region and Issue CVEs. It contains common valid Regions and Issues for Access Control.

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

- 500 Series:
  - Intelligence Community Directive (ICD) 500, *Director Of National Intelligence Chief Information Officer* <sup>[3]</sup>
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* <sup>[4]</sup>
  - Intelligence Community Program Guidance (ICPG) 500.2, *Attribute-based Authorization and Access Management* <sup>[5]</sup>
  - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* <sup>[6]</sup>
- Memorandums:

- IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* [\[1\]](#)

## 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 [\[2\]](#).

### 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 Extensible Markup Language (XML) Qualified Name used in any example in this document should be interpreted using the information below.

**Table 1 - XML Namespaces**

Prefix	URI
mn	urn:us:gov:ic:mn
ism	urn:us:gov:ic:ism
xsd	<a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a>

## 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 [\[2\]](#).

### 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
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ <sup>[2]</sup> )	This specification does not depend on a specific version of IC-SF.XML <sup>[2]</sup> ; 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.
Schematron <sup>[7]</sup>	<p>Schematron — International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19757-3:2006 — is a rule-based document schema definition language. In this specification Schematron is a formal language used to express normative business rules, so this reference is normative.</p> <p>The Schematron rules are normative in the sense that they convey criteria that a document MUST adhere to, exactly as English may be used to convey normative criteria. It is not necessary for implementers to use the specific Schematron encoding in this specification. Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification.</p> <p>Note: The Schematron rules in this specification use Transformations (XSLT) 2.0<sup>[8]</sup> query binding.</p>

Name	Dependency Description
<p>XSLT 2.0<sup>[8]</sup> implementation of Schematron<sup>[7]</sup> by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): <a href="http://code.google.com/p/schematron/">http://code.google.com/p/schematron/</a>.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>

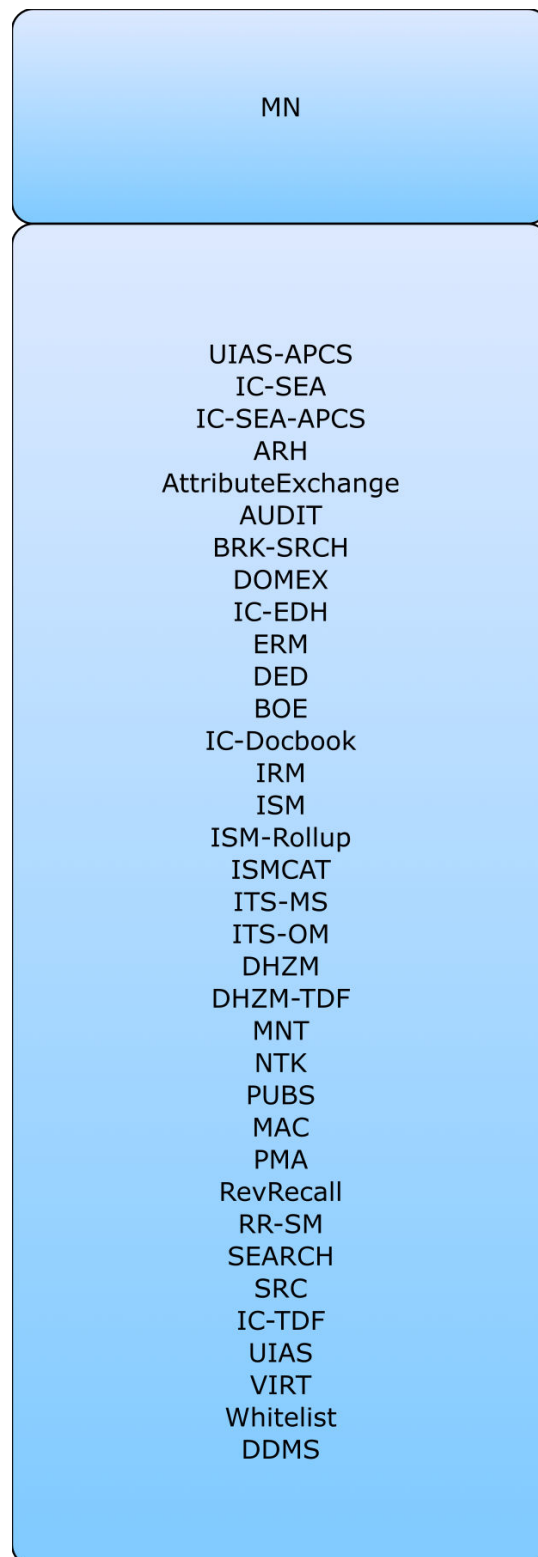


**Figure 1 : Related Specifications**

## 1.5.2 - Inverse Dependencies

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

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



**Figure 2 : Inverse Dependency Specifications**

## Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the “Specification Overview” chapter in the IC-SF.XML<sup>[2]</sup> framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

### 2.1 - Relationship to Abstract Data Definition and other encodings

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

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

### 2.2 - Understanding Access Control

This specification participates in the Data Attributes leg 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<sup>[2]</sup> framework document.

### 2.3 - Additional Guidance

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

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

#### 2.3.1 - Usage of the MN Schema

The MN.CES schema defines elements (**Region** and **Issue**) and attributes (**@mn:region** and **@mn:issue**) that enforce the allowable values as defined in the specification’s CVEs (see [Section 3.1.1 - Value Enumeration Constraints](#) for more details). Consumers of the MN.CES specification should import the MN schema and reference elements or attributes, depending on what is needed. Note: the names for the elements and the attributes are similar because the content is the same, i.e., both limit values to those in MN CVEs. The expectation is that the consumer use one or the

other. The difference in capitalization follows the IC naming standard, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

## 2.3.2 - Usage of the MN Schematron Library

The MN.CES Schematron library contains an abstract rule that enforces the allowable values as defined in the specification's CVE (see [Section 3.1.1 - Value Enumeration Constraints](#) for more details). Consumers of the MN.CES specification should include the abstract rule and define an implementation for it. This allows for the consumer to define the context that triggers the rule and the value that should be matched against the MN CVEs.

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

## Chapter 3 - Constraints

### 3.1 - Data Validation Constraint Rules

The MN.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which MN.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. For more information, please see the “Data Validation Constraint Rules” chapter in the IC-SF.XML<sup>[2]</sup> framework document.

#### 3.1.1 - Value Enumeration Constraints

Several elements and attributes of the MN.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.

#### 3.1.2 - Additional Constraints

##### 3.1.2.1 - CES Constraints

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

#### 3.1.3 - Constraint Rules

The detailed constraint rules for the MN.CES schema can be found in a separate document inside the Documents/MN directory, in the “MN\_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 “MN\_Rules.pdf” file as well.

### 3.2 - Data Rendering Constraint Rules

#### 3.2.1 - Purpose

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

by individuals not familiar with the details of the MN.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 MN.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 this specification.

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. MN Feature Summary

Table 5 - MN Feature Comparison

Required date	Feature	V2015-AUG	V2017-MAY	V2017-MAYr2019-MAR	V2021-NOV
	Defines the allowable values for Regions	F	F	F	F
	Defines the allowable values for Issues	F	F	F	F
	Added ANAN value for Regions and ANY value for Issue	N	N	N	F

## Appendix B Change History

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

**Table 6 - CES Version Identifier History**

Version	Date	Purpose
2015-AUG	August 13, 2015	Initial Release
2017-MAY	May 22, 2017	Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - 2017-MAY Change Summary</a>
2017-MAYr2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - 2017-MAYr2019-MAR Change Summary</a>
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - 2021-NOV Change Summary</a>

### B.1 - 2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- Add ANAN and ANY to MN to satisfy a need from the Identity, Credential, and Access Management (ICAM) Service Provider (SP).

The following table summarizes the changes made to 2017-MAYr2019-MAR in developing 2021-NOV.

**Table 7 - Data Encoding Specification 2021-NOV Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Updated documentation to use the specification framework. (CR-2019-037)	Documentation	No impact to systems.
2	Update chapters for consistency with other specifications. (CR-2019-094)	Documentation	No impact to systems.
3	Remove XML from CES Titles. (CR-2019-046)	Documentation	No impact to systems.
4	Identify the lack of a root node in the Schema Guide. (CR-2019-123)	Documentation	No impact to systems.

#	Change	Artifacts Changed	Compatibility Notes
5	Created schematron rule to check current CESVersion (CR-2017-090, CR-2017-228, CR-2017-311)	Schema Schematron MN-ID-00001 added	Data generation and ingestion systems need to be updated to accommodate the changes.
6	Added ANAN for Regions and ANY for Issue (CR-2019-141)	CVE CVerenumMNIssue modified CVerenumMNRegion modified	Systems need to be updated to accommodate this change.

## B.2 - 2017-MAYr2019-MAR Change Summary

Significant drivers for Version 2017-MAYr2019-MAR include:

- Correct bad value of specVersion in MN CVEs from 2017-MAY release.

The following table summarizes the changes made to 2017-MAY in developing 2019-MAR revision, 2017-MAYr2019-MAR.

**Table 8 - Data Encoding Specification 2017-MAYr2019-MAR Change Summary**

#	Change	Artifacts Changed	Compatibility Notes
1	Correct value of specVersion attribute in CVE files. (CR-2019-009)	CVE CVerenumMNIssue CVerenumMNRegion	Systems may need to be updated to handle new/updated values.

## B.3 - 2017-MAY Change Summary

Significant drivers for Version 2017-MAY include:

- DDII updates to values as of 2017-05-18.

The following table summarizes the changes made to 2015-AUG in developing 2017-MAY.

**Table 9 - Data Encoding Specification 2017-MAY Change Summary**

#	Change	Artifacts Changed
	Updated values based on DDII information. (CR-2017-019)	CVE CVerenumMNIssue

#	Change	Artifacts Changed
	Removed Standalone and Convenience packages section. (CR-2017-128)	DES
	Added inverse dependency section along with hard and soft inverse dependency descriptions. (CR-2017-119)	DES

## Appendix C Glossary

This appendix lists terms, definitions and sources of the definitions for terms used in this document.

### ANAN

A token in the `@mn:region` attribute as listed in “CVerenumMNRegion”. The token was added in an effort to move complexity from the ABAC system to the subject provisioning system by denormalizing the Region list. **"ANAN"** on a resource requires any region to be provisioned on the subject. This could be inferred by the presence of a region, but by adding the explicit value **"ANAN"** to the subject, we now have a simple string match.

On a resource when **"ANAN"** is selected, it is the most permissive while still requiring some provisioning of "any" region.

The subject provisioning system **MUST** provision **"ANAN"** when the user has at least one region. When any region is provisioned **"ANAN"** must be selected also and cannot be the only region selected.

### ANY

A token in the `@mn:issue` attribute as listed in “CVerenumMNIssue”. The token was added in an effort to move complexity from the ABAC system to the subject provisioning system by denormalizing the Issue list. **"ANY"** on a resource requires any issue to be provisioned on the subject. This could be inferred by the presence of an issue, but by adding the explicit value **"ANY"** to the subject, we now have a simple string match.

On a resource when **"ANY"** is selected, it is the most permissive while still requiring some provisioning of "any" issue.

The subject provisioning system **MUST** provision **"ANY"** when the user has at least one issue. When any issue is provisioned **"ANY"** must be selected also and cannot be the only issue selected.

## Appendix D List of Abbreviations

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

ABAC	Attribute Based Access Control
ADD	Abstract Data Definition
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

## Appendix E Bibliography

[1] IC CIO Memo 2018-081

Intelligence Community Chief Information Officer. *IC CIO Memo 2018-081: Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness*. 26 November 2018.

[2] 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>

[3] 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](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

[4] 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](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

[5] ICPG 500.2

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

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

Available online at: [http://www.dni.gov/files/documents/ICPG/icpg\\_500\\_2.pdf](http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf)

[6] 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>

[7] 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/>

[8] 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 F 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](mailto:ic-standards-support@odni.gov).

## Appendix G 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<sup>[6]</sup>.