Intelligence Community Technical Specification

CVE Encoding Specification for Role

Version 2021-NOV

December 1, 2022

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

Table of Contents

List of Figures

List of Tables

List of Examples

Chapter 1 - Introduction

1.1 - Purpose

This *CVE Encoding Specification for Role* (ROLE.CES) defines detailed implementation guidance for using Extensible Markup Language (XML) to encode the controlled vocabulary for Role. This Controlled Vocabulary Enumeration Encoding Specification (CES) defines the CES elements and attributes, associated structures and relationships, cardinality requirements, and permissible values for the **`@role`** attribute as defined in the *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML[14]) Technical Specification. ROLE.CES is a set of values to characterize the entity's (person or non-person) authorized position, job or area of responsibility that ties membership to the function that the entity needs to perform the expected task.

1.2 - Scope

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

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

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

The conditions of use and applicability of this technical specification are defined outside of this technical specification. Intelligence Community Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance* [8], defines the Intelligence Community Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

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

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

1.3 - 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 minimize the need to revise 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 CVE 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 Role CVEs. It contains the approved namespaces and associated taxonomies for the **@Role** attribute and the valid values for populating the components of a **@role**.

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* [4]
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* [5]
  - Intelligence Community Program Guidance (ICPG) 500.1, *Digital Identity* [6]
  - ICPG 500.2, *Attribute-based Authorization and Access Management* [7]
  - ICS 500-20, *IC Enterprise Standards Compliance* [8]
  - ICS 500-29, *IC Digital Identifier* [9]
  - ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources* [10]
- 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[3].

1.5 - Dependencies

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

1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in Table 1. 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 1 will be shown in Figure 1; however not all IC CIO specifications listed in Figure 1 may appear in Table 1. Figure 1 is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 1 - Dependencies

Name	Dependency Description
CVE Encoding Specification for US Agency Acronyms (USAgency.CES.V2017-MAR-r2018-FEB+[15])	This specification does not depend on a specific version of USAgency.CES[15]; versions later than version 2017-MAR-r2018-FEB MAY be used. The minimum version was based on the earliest non-retired version; Enterprise Standards Baseline (ESB) 21-2.0 was used for determining the version.
Intelligence Community Specification Framework (IC-SF.XML.V2021-NOV+[3])	This specification does not depend on a specific version of IC-SF.XML[3]; 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[13]	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[16] query binding.

Name	Dependency Description
XSLT 2.0[16] implementation of Schematron[13] 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.

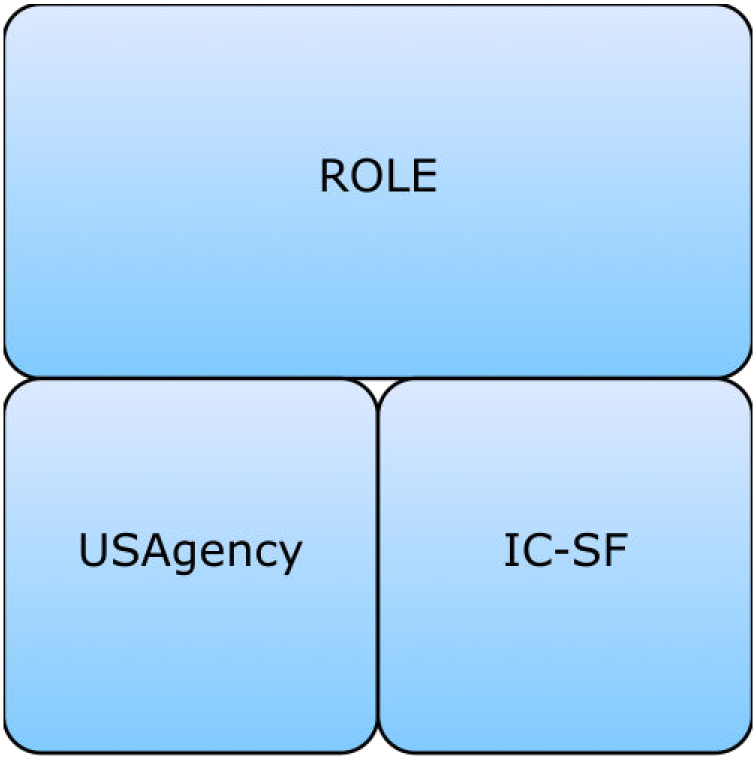

Figure 1 : Related Specifications

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.

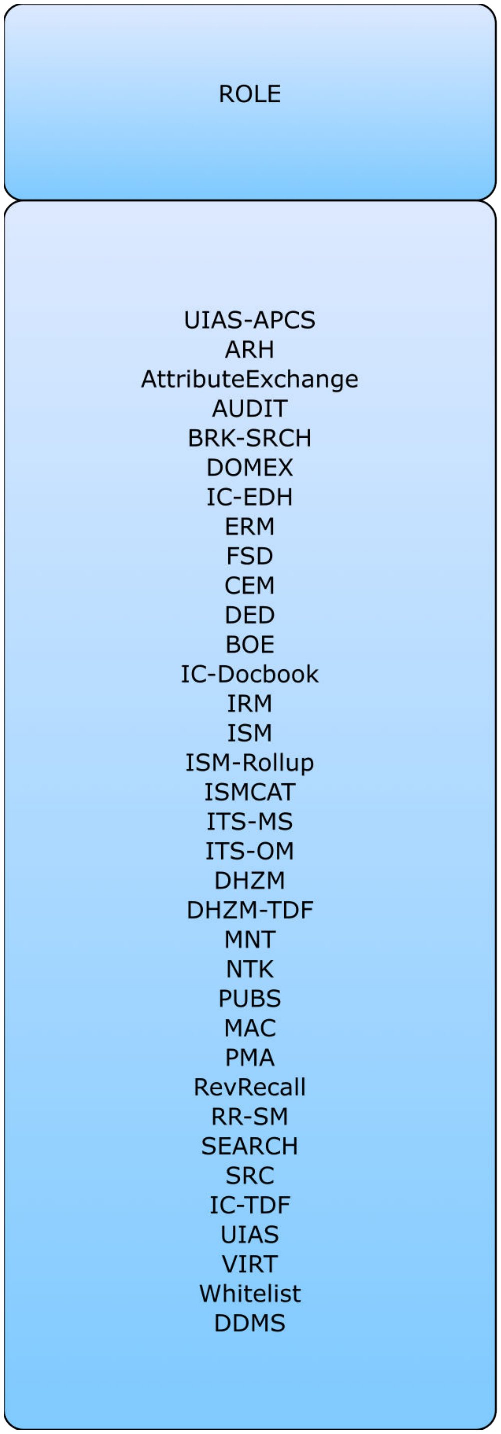

Figure 2 : Inverse Dependency Specifications

Chapter 2 - Development Guidance

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

2.1 - Understanding Access Control

This specification participates in the Data Attribute 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[3] framework document.

The user 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 user attribute component to make accurate, reliable, and automated access control decisions. The Role specification provides a common encoding (e.g., common understanding) and foundation for the UIAS.XML[14] attribute **`@role`**.

2.2 - Relationship to Abstract Data Definition and other encodings

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

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

Chapter 3 - Constraints

3.1 - Role Taxonomy

This section describes the generic format and lexicon for the **`@role`** attribute. This format and lexicon is used to create specific taxonomies for a given namespace and are included in ensuing subsections. While this specification is useful in and of itself, the intended use is to be incorporated into other specifications, in particular, UIAS.XML[14]. For this purpose, **`@role`** is defined by the use of Augmented Backus-Naur Form (ABNF) which are defined in Internet Engineering Task Force (IETF)-Request for Comments (RFC) 5234, *Augmented BNF for Syntax Specifications: ABNF* [12]. The ABNF (See http://tools.ietf.org/pdf/rfc5234.pdf [12]) rules used to specify the format of Role are normative, the corresponding textual descriptions are informative. The remainder of this document is normative. Additionally, the use of keywords defined in IETF-RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels* [11] is considered normative within the scope of the sentence. The following ABNF rules explicitly define the content of ABNF and are used to provide a formal description independent of any particular technology.

It is important to note that ABNF strings are case-insensitive, therefore all components of the **`@role`** attribute are case-insensitive. ALPHA is defined to be A-Z / a-z.

Role-Template Format

[1] Role-Template ::= Namespace1*10Concept-Template

[2] Namespace ::= 1*255(ALPHA / DIGIT / "_")

[3] Concept-Template ::= "-" 1*255(ALPHA / DIGIT / "_")

Role Lexicon

The following vocabulary helps explain the meaning of terms used in Role-Template documentation.

A new namespace has to define all of the following terms:

Role-Template (Canonical Role)

A globally unique attribute used to define an entity's allowed actions in an IC system. The **`@role`** attribute is composed of a namespace and one or more concepts. There is no theoretical size limit (length) of the value for a **`@role`**, but maximum lengths have been established for each component of the CVE to avoid practical issues with software implementation and to support interoperability needs.

Namespace

Namespace is the highest level of the taxonomy and identifies the environment for which the **`@role`** attribute value set is created. Valid values for namespace can be found in the CVE, “CVEnumROLENamespace”, included in this specification package. All **`@role`** values SHOULD be UNCLASSIFIED. Each namespace will have an ABNF for the particular pattern that is appropriate for that namespace.

Concept-Template

Concept-Template is a template for the concepts of **`@role`** within a namespace. Each concept MAY have a CVE associated with it. The namespace owner MAY create a taxonomy consisting of up to 10 concepts.

3.1.1 - Approved Namespaces

The following namespaces have been approved for use within the **`@role`** attribute value set:

Table 2 - Approved Namespaces

Namespace	Description
C2S	Commercial Cloud Services (C2S)
ENT	Enterprise
Nebula	Nebula Suite of Services
PAAS	Platform as a Service (PAAS)

3.1.2 - C2S Namespace Taxonomy

This section describes the format and lexicon for the **`@roles`** of the C2S namespace.

C2S Format

```
[4]          C2S ::= "C2S" "-" RoleOrg "-" RoleScope "-" RoleName "-"
                     RoleFunction
[5]      RoleOrg ::= 1*255(ALPHA / DIGIT / "_" )
[6]    RoleScope ::= 1*255(ALPHA / DIGIT / "_" )
[7]     RoleName ::= 1*255(ALPHA / DIGIT / "_" )
[8] RoleFunction ::= 1*64(UPALPHA / DIGIT / "_" )
[9]      UPALPHA ::= %x41-5A ; any US-ASCII uppercase letter "A".."Z"
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in the C2S **`@role`** value documentation, and it may further constrain the set of allowable values:

C2S (Canonical C2S Role)

The C2S **`@Role`** is a globally unique attribute used to define an entity's allowed actions in the C2S system. The value string is composed of the namespace C2S and four concepts: a RoleOrg, a RoleScope, a RoleName and a RoleFunction. Each of these concepts of the taxonomy are separated by a dash (“-”) character.

RoleOrg

The RoleOrg concept of the C2S **`@role`** taxonomy represents the organization or agency for which the **`@role`** is valid. The RoleOrg value of the C2S **`@role`** taxonomy appended with prefix "USA." MUST be one of the values found in the CVE, "CVEnumUSAgencyAcronym" in *CVE Encoding Specification for US Agency Acronyms*(USAgency.CES[15]).

RoleScope

The RoleScope concept of the C2S **@role** taxonomy defines the context for which the given **@role** is valid. The RoleScope could be global or limited to a sub-portion of the IC Information Technology (IT) infrastructure. The RoleScope concept of the C2S **@role** taxonomy MUST contain one of the valid values found in the CVE, "CVEnumROLEC2SScope", included in this specification package.

RoleName

The RoleName concept of the C2S **@role** taxonomy contains the context for the **@role** attribute. Some possible contexts include a mission name, project name, group name, etc. While there are no controlled values for RoleName, the name MUST NOT contain the dash ("-") character and MUST conform to the ABNF above.

RoleFunction

The RoleFunction concept of the C2S **@role** taxonomy indicates the specific function. It is important to note that the C2S RoleFunction concept can contain values described by a regular expression as show in the C2SFormat table above, including the constraint that all alphabetic characters must be upper case. The RoleFunction concept of the C2S **@role** taxonomy MUST contain one of the valid values found in the CVE, "CVEnumROLEC2SFunction", however, service providers can create custom role functions and begin using them immediately.

Example 3.1. Examples of Role for C2S Namespace

- C2S-CIA-Ent-CLZ-S3ONLY
- C2S-CIA-Ent-CIO-NETADMIN
- C2S-NSA-Msn-MissionA-READONLY

3.1.3 - Enterprise Namespace Taxonomy

This section describes the format and lexicon for the **@roles** of Enterprise namespace.

Enterprise Role Format

```
[10]          ENT ::= "ENT" "-" RoleOrg "-" RoleName
[11]      RoleOrg ::= 1*255(ALPHA / DIGIT / "_" )
[12]     RoleName ::= 1*255(ALPHA / DIGIT / "_" )
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in Enterprise **`@role`** value documentation, and it may further constrain the set of allowable values:

Enterprise (Canonical Enterprise Role)

The Enterprise Role is a globally unique attribute used to define a Person Entity's data access restrictions . The value string is composed of the namespace Enterprise and two concepts: a RoleOrg and a RoleName. Each of these concepts of the taxonomy are separated by a dash (“-”) character.

RoleOrg

The RoleOrg concept of the Authorized Law Enforcement Personnel (ALEP) **`@role`** taxonomy represents the organization or agency for which the **`@role`** is valid. The RoleOrg value of the ALEP **`@role`** taxonomy appended with prefix "USA." MUST be one of the values found in the CVE, “CVEnumUSAgencyAcronym” in *CVE Encoding Specification for US Agency Acronyms*(USAgency.CES[15]).

RoleName

The Role concept of the Enterprise **`@role`** taxonomy MUST contain a valid value found in the CVE, “CVEnumROLEEnterpriseRole”, included in this specification package.

Example 3.2. Example of Role for Enterprise Namespace

- ENT-FBI-ALEP

3.1.4 - Nebula Namespace Taxonomy

This section describes the format and lexicon for the **`@roles`** of Nebula namespace.

Nebula Format

```
[13]      Nebula ::= "Nebula-CIA-" NamedRole
[14]   NamedRole ::= 1*255(ALPHA / DIGIT / "_" )
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in Nebula **`@role`** value documentation, and it may further constrain the set of allowable values:

Nebula (Canonical Nebula Role)

The Nebula Role is a globally unique attribute used to define an Non-Person Entity’s allowed actions in the Nebula system. The value string is composed of the namespace Nebula and 1 concept: a NamedRole. Each element in the Nebula namespace is separated by a dash (“-”) character.

NamedRole

The NamedRole concept of the Nebula **@role** taxonomy MUST contain one of the valid values found in the CVE, “CVEnumROLENebulaNamedRole”, included in this specification package.

Example 3.3. Examples of Role for Nebula Namespace

- Nebula-CIA-Proxy
- Nebula-CIA-Bulk

3.1.5 - PAAS Namespace Taxonomy

This section describes the format and lexicon for the **@role**s of the PAAS namespace.

PAAS Format

```
[15]          PAAS ::= "PAAS" "-" RoleOrg "-" RoleScope "-" RoleName "-"
                       RoleFunction
[16]       RoleOrg ::= 1*255(ALPHA / DIGIT / "_" )
[17]     RoleScope ::= 1*255(ALPHA / DIGIT / "_" )
[18]      RoleName ::= 1*255(ALPHA / DIGIT / "_" )
[19]  RoleFunction ::= 1*64(UPALPHA / DIGIT / "_" )
[20]       UPALPHA ::= %x41-5A ; any US-ASCII uppercase letter "A".."Z"
```

Role Lexicon

The following vocabulary helps explain the meaning of terms used in the PAAS **@role** value documentation, and it may further constrain the set of allowable values:

PAAS (Canonical PAAS Role)

The PAAS Role is a globally unique attribute used to define an entity's allowed actions in the PAAS system. The value string is composed of the namespace PAAS and four concepts: a RoleOrg, a RoleScope, a RoleName and a RoleFunction. Each of these concepts of the taxonomy are separated by a dash (“-”) character.

RoleOrg

The RoleOrg concept of the PAAS **@role** taxonomy represents the organization or agency for which the **@role** is valid. The RoleOrg value of the PAAS **@role** taxonomy appended with prefix "USA." MUST be one of the values found in the CVE, “CVEnumUSAgencyAcronym” in *CVE Encoding Specification for US Agency Acronyms*(USAgency.CES[15]).

RoleScope

The RoleScope concept of the PAAS **`@role`** taxonomy defines the context for which the given **`@role`** is valid. The RoleScope could be global or limited to a sub-portion of the IC IT infrastructure. The RoleScope concept of the PAAS **`@role`** taxonomy MUST contain one of the valid values found in the CVE, “CVEnumROLEPAASScope”, included in this specification package.

RoleName

The RoleName concept of the PAAS **`@role`** taxonomy contains the context for the **`@role`** attribute. Some possible contexts include a mission name, project name, group name, etc. While there are no controlled values for RoleName, the name MUST NOT contain the dash (“-”) character and MUST conform to the ABNF above.

RoleFunction

The RoleFunction concept of the PAAS **`@role`** taxonomy indicates the specific function. It is important to note that the PAAS RoleFunction concept can contain values described by a regular expression as show in the PAASFormat table above, including the constraint that all alphabetic characters must be upper case. The RoleFunction concept of the PAAS **`@role`** taxonomy MUST contain one of the valid values found in the CVE, “CVEnumROLEPAASFunction”, however, service providers can create custom role functions and begin using them immediately.

Example 3.4. Examples of Role for PAAS Namespace

- PAAS-CIA-Ent-CLZ-S3ONLY
- PAAS-CIA-Ent-CIO-NETADMIN
- PAAS-NSA-Msn-MissionA-READONLY

3.2 - Value Enumeration Constraints

Several elements and attributes of the ROLE.CES model use CVEs to define the data allowed in the element or attribute. In some cases the specific CVE is specified via an attribute, which may include a default CVE. Further, in some of the cases where the CVE can be specified, the attribute may restrict the list of CVEs allowed and some may allow for the author to specify their own CVE. For each of these, the value must be in the specified external CVE or the default CVE.

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

A failure of validation against a CVE SHALL be considered an Error.

3.3 - Additional Constraints

3.3.1 - DES Constraints

The Data Encoding Specification (DES) or CES version is specified through attributes on the root element. The schema constrains the values of these attributes. The DES or 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.

3.4 - Constraint Rules

The detailed constraint rules for the ROLE.CES schema can be found in a separate document inside the Documents/ROLE directory, in the “ROLE_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 “ROLE_Rules.pdf” file as well.

Appendix A Feature Summary

The following tables summarize major features by version for ROLE.CES. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g., The IC Marking System Register and Manual[2] has an implementation date of one year after issuance).

Table 3 - 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. ROLE Feature Summary

Table 4 - ROLE Feature comparison

Required date	Feature	V1	V2014-DEC	V2021-NOV
7 July 2014	C2S taxonomy and permissible values	F	F	F
	Nebula namespace	N	F	F
	Updated C2S namespace RoleFunction to be all upper case	N	F	F
	Added new RoleFunction to C2S namespace	N	F	F
	PAAS namespace	N	N	F
	Made ROLE its own separate specification.	N	N	F
	Add Enterprise namespace with value ALEP	N	N	F
	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE	N	N	F

Appendix B Change History

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

Table 5 - CES Version Identifier History

Version	Date	Purpose
1	May 7, 2014	Initial Release
2014-DEC	December 4, 2014	Update C2S Namespace and add Nebula Namespace
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see Section B.1 - V2021-NOV Change Summary

B.1 - V2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- Community Change Requests

The following table summarizes the changes made to 2014-DEC in developing 2021-NOV.

Table 6 - Data Encoding Specification 2021-NOV Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE (CR-2019-003)	Documentation Schema	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. Identity, Credential, and Access Management (ICAM) systems and software services need to be updated to accommodate the changes.
2	Updated documentation to use the specification framework. (CR-2019-039)	Documentation	No impact to systems.

#	Change	Artifacts changed	Compatibility Notes
3	Extract ROLE from UIAS to become a standalone CVE again and also added ROLE schema and schematron. (CR-2019-054)	Documentation CVEs CVEnum-ROLEC2SFunction added CVEnum-ROLEC2SScope added CVEnum-ROLENamespace added CVEnum-ROLENebulaNamedRole added CVEnum-ROLEPAASFunction added CVEnum-ROLEPAASScope added Schema Schematron ROLE-ID-00001 added ROLE-ID-00002 added	No impact to systems.
4	Removed XML from the title. (CR-2019-049)	Documentation	No impact to systems.
5	Add Enterprise namespace with value ALEP. (CR-2019-013)	CVE CVEnum-ROLEEnterpriseRole added Schema	Data generation and ingestion systems need to be updated to use the additional namespace.

B.2 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Added new namespace for Nebula

- Updated C2S namespace

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

Table 7 - V2014-DEC Change History

#	Change	Artifacts changed	Compatibility Notes
1	Changed CESVersion to represent the year and month of release. Also allowed for extension of specification by adding a ‘-’ followed by a string to denote a custom implementation.	CES	Data generation and ingestion systems need to be updated to use the modified version string.
2	Added new namespace for Nebula.	CVE Nebula	Data generation and ingestion systems need to be updated to use the additional namespace.
3	Added new RoleFunction value.	CES	Data generation and ingestion systems need to be updated to use the additional value.
4	Updated RoleFunction to be in all upper case.	CES	Data generation and ingestion systems need to be updated to use the modified values.

Appendix C List of Abbreviations

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

ABNF	Augmented Backus-Naur Form
ADD	Abstract Data Definition
ALEP	Authorized Law Enforcement Personnel
C2S	Commercial Cloud Services
CES	Controlled Vocabulary Enumeration Encoding Specification
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
ESB	Enterprise Standards Baseline
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
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
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
PAAS	Platform as a Service
RFC	Request for Comments
URL	Uniform Resource Locator
XML	Extensible Markup Language

XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix D 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 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-SF.XML

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

[4] ICD 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

[5] 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

[6] ICPG 500.1

Deputy Director of National Intelligence for Policy, Plans, and Requirements. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 7 May 2010.
Available online Intelink-TS at: https://go.ic.gov/kEqL6Dh (case sensitive – kilo Echo quebec Lima 6 Delta hotel)

[7] 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

[8] 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

[9] ICS 500-29
Director of National Intelligence Chief Information Officer. *Intelligence Community Digital Identifier*. Intelligence Community Standard 500-29. 12 July 2012.
Available online Intelink-TS at: https://go.ic.gov/ObgTCPJ (case sensitive – Oscar bravo golf Tango Charlie Papa Juliet)

[10] ICS 500-30
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*. Intelligence Community Standard 500-30. 24 April 2014.
Available online Intelink-TS at: https://go.ic.gov/lqk775v (case sensitive – lima quebec kilo 7 7 5 victor)

[11] 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

[12] IETF-RFC 5234
Internet Engineering Task Force. *Augmented BNF for Syntax Specifications: ABNF*. January 2008.
Available online at: http://tools.ietf.org/html/rfc5234

[13] 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/

[14] UIAS.XML
Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.
Available online Intelink-TS at: https://go.ic.gov/xQK4AX1 (case sensitive – xray Quebec Kilo 4 Alpha Xray 1)
Available online Intelink-U at: https://w3id.org/ic/standards/UIAS
Available online at: https://w3id.org/ic/standards/public

[15] USAgency.CES

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

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

Appendix E Points of Contact

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

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

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

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

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

Appendix F IC CIO Approval Memo

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

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

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC ESB as defined in ICS 500-20[8].