



Intelligence Community Technical Specification

CVE Encoding Specification for Fine Access Control

Version 2022-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	3
1.5.1 - Specification Dependencies	3
1.5.2 - Inverse Dependencies	5
Chapter 2 - Development Guidance	7
2.1 - Understanding Access Control	7
2.2 - Additional Guidance	7
2.2.1 - Usage of the FAC.CES Schema	7
2.2.2 - Usage of the FAC Schematron Library	7
2.2.3 - Use of FAC for SAP Accesses	8
2.2.3.1 - Classification-based Read-ons for DoD SAPs	8
2.2.3.2 - Rules for SAP Values in Fine Access Controls	9
2.2.3.3 - Published and Unpublished SAPs	10
Chapter 3 - Constraints	11
3.1 - “Living” Constraint Rules	11
3.2 - Data Validation Constraint Rules	11
3.2.1 - Value Enumeration Constraints	11
3.2.2 - Additional Constraints	12
3.2.2.1 - CES Constraints	12
3.2.3 - Constraint Rules	12
3.3 - Data Rendering Constraint Rules	12
3.3.1 - Purpose	12
3.3.2 - Rendering Constraint Rules	12
Appendix A - Feature Summary	13
A.1 - FAC Feature Comparison	13
A.1.1 - Features from V2019-MAR to V2022-NOV	13
A.1.2 - Features from V2018-APR to V2019-MAR	14
A.1.3 - Features from V1 to V2018-APR	14
Appendix B - Change History	15
B.1 - V2022-NOV Change Summary	15
B.2 - V2021-NOV Change Summary	16
B.3 - V2019-SEP Change Summary	17
B.4 - V2019-MAR Change Summary	18
B.5 - V2018-NOV Change Summary	18
B.6 - V2018-JUL Change Summary	18
B.7 - V2018-APR Change Summary	19
B.8 - V2014-DEC Change Summary	20
Appendix C - List of Abbreviations	22
Appendix D - Bibliography	24
Appendix E - Points of Contact	27
Appendix F - IC CIO Approval Memo	28

List of Figures

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

List of Tables

Table 1 - XML Namepaces	3
Table 2 - Direct Dependencies	3
Table 3 - Constraint Rules	12
Table 4 - Feature Summary Legend	13
Table 5 - FAC.CES Feature comparison V2019-MAR to V2022-NOV	13
Table 6 - FAC.CES Feature comparison V2018-APR to V2019-MAR	14
Table 7 - FAC.CES Feature comparison V1 to V2018-APR	14
Table 8 - CES Version Identifier History	15
Table 9 - V2022-NOV Change History	16
Table 10 - V2021-NOV Change History	16
Table 11 - V2019-SEP Change History	17
Table 12 - V2019-MAR Change History	18
Table 13 - V2018-NOV Change History	18
Table 14 - V2018-JUL Change History	19
Table 15 - V2018-APR Change History	19
Table 16 - V2014-DEC Change History	21

Chapter 1 - Introduction

1.1 - Purpose

This *CVE Encoding Specification for Fine Access Control* (FAC.CES) defines detailed implementation guidance using several encoding formats including Extensible Markup Language (XML), and JavaScript Object Notation (JSON) to encode Fine Access Control controlled vocabulary. 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^[7]) 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 intelligence; 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* ^[15], 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 remove the need to revision a specification when a CVE was updated, a new type of encoding specification, the CVE Encoding Specification, was created to decouple the vocabulary from the specifications. Each CES contains one or more CVEs and optionally a master schema defining elements and attributes limited to the allowable values and/or any Schematron rules that enforce the vocabulary in specifications that define their own elements or attributes.

This CES defines the fine access control CVE and contains valid values for the *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML^[20]) attribute **@fineAccessControls**. This specification is independent from the UIAS.XML^[20] specification and allows the fine access control values to be revised without revising the UIAS.XML^[20] specification. This CES also defines the fine access control CVE and contains valid values for the *XML Data Encoding Specification for Enterprise Audit Exchange* (AUDIT.XML^[1]) elements with **@name="fineAccessControls"**.

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* ^[8]
 - ICD 209, *Tearline Production and Dissemination* ^[9]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide* ^[14]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[10]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* ^[11]
 - ICS 500-20, *IC Enterprise Standards Compliance* ^[15]
 - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[16]
- 700 Series:
 - ICD 710, *Classification and Control Markings System* ^[12]
 - Intelligence Community Program Guidance (ICPG) 710.1, *Application of Dissemination Controls: Originator Control* ^[13]
- DoD Issuances:
 - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* ^[3]
 - Department of Defense Manual Number 5200.01, *DoD Information Security Program (Vol 1-3)* ^[2]
- IC CIO Directives:
 - *Intelligence Community Markings System Register and Manual* ^[6]

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^[7].

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 Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism
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^[7].

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 - Direct Dependencies

Name	Dependency Description
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[7])	This specification does not depend on a specific version of IC-SF.XML ^[7] ; 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 ^[19]	<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^[21] query binding.</p>
<p>XSLT 2.0^[21] implementation of Schematron^[19] by Rick Jelliffe (2010-04-14)</p> <p>Note: The only available identifying descriptors for this implementation are the implementer's name and date of release. This implementation may be found at the following Uniform Resource Locator (URL): http://code.google.com/p/schematron/.</p>	<p>The International Organization for Standardization does not create nor endorse reference implementations of its standards. For the purposes of this specification the <i>behavior</i> of the implementation created by Mr. Jelliffe is normative.</p> <p>Implementers MAY use any encodings, tools, or languages desired to implement validation schemes for conformance to this specification. To conform to this specification, a validator MUST find a document valid <i>if and only if</i> the Schematron implementation by Mr. Jelliffe would find the document valid according to the Schematron rules in this specification.</p>



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](#).

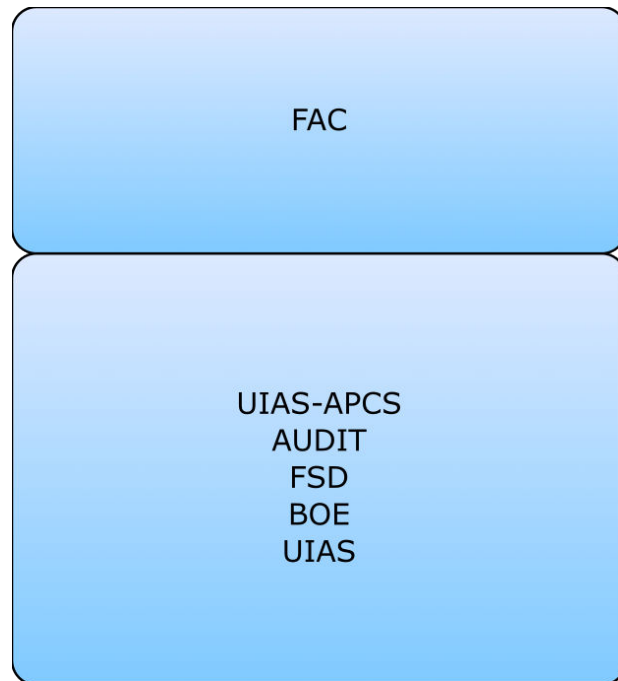


Figure 2 : Inverse Dependency Specifications

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^[7] 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 Entity 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^[7] framework document.

2.2 - 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 fine access control can use the FAC.CES specification: through referencing objects defined in the schema or enforcing the format via running Schematron.

For each of the allowable FAC.CES allowable values, there is a marking metadata attribute that may or may not contain a value. The Marking Metadata attribute can document any information about the FAC.CES value as needed.

2.2.1 - Usage of the FAC.CES Schema

The FAC.CES schema defines an element (**Fac**) and an attribute (**@fac**) that enforces the allowable values as defined in the specification’s CVE (see [Section 3.2.1 - Value Enumeration Constraints](#) for more details). Consumers of the FAC.CES specification should import the FAC schema and reference the element or attribute, depending on what is needed. Note: the names for the element and the attribute are similar because the content is the same, i.e., both limit the value to the FAC.CES CVE, but the expectation on usage is that the consumer would use one or the other. The difference in capitalization is because they follow the IC naming standards, which requires the first letter for elements to be uppercase and the first letter for attributes to be lower case.

2.2.2 - Usage of the FAC Schematron Library

The FAC.CES Schematron library contains an abstract rule that enforces the allowable values as defined in the specification’s CVE (see [Section 3.2.1 - Value Enumeration Constraints](#) for more details). Consumers of the FAC.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 “CVEnumFineAccessControlType” CVE.

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

2.2.3 - Use of FAC for SAP Accesses

This release of FAC incorporates Department of Defense (DOD) Special Access Program Control Office (SAPCO) guidance on how accesses to Special Access Program (SAP)s are handled. This section documents SAPCO guidance and contrasts it with differing guidance in the IC Markings Register, *Intelligence Community Markings System Register and Manual* ^[6]. Efforts are underway to reconcile differing guidance documents, but these efforts are not yet completed. This release of FAC adheres to multiple, differing guidance documents on SAPs in order to support multiple customers. This release of FAC adapts handling of SAPs based on the owner of a SAP and on whether data's Information Security Markings (ISM) metadata indicates `@ism:compliesWith` contains "USIC", "USDOD", or both.

In the discussion below, hypothetical SAP markings are used for illustration. Following the IC Markings Register, *Intelligence Community Markings System Register and Manual* ^[6] section on SAPs, the hypothetical SAP BUTTER POPCORN and other hypothetical SAP markings are used for illustration.

2.2.3.1 - Classification-based Read-ons for DoD SAPs

The IC Markings Register, *Intelligence Community Markings System Register and Manual* ^[6], indicates that users are granted a single access level for each SAP. Information from DOD's SAPCO indicates that, for SAP's owned by DOD and possibly some SAPs owned by other agencies, SAP read-ons are granted at different classification levels. A user who is granted Top Secret (TS) access to a SAP is authorized to see information classified at the TS level or below for that SAP. In contrast, a user who is granted SECRET access to a SAP is authorized to see information classified only at the SECRET or CONFIDENTIAL levels for that SAP.

The classification banner for a resource that contains SAP data does not explicitly identify the classification level read-on required to access the resource's SAP data. For example, if there is a hypothetical DOD SAP STORMY_PETREL that requires different read-ons at different classification levels, then a document marked TOP SECRET//SAR-STORMY_PETREL may contain STORMY_PETREL data that is at the TS level, or alternatively it may contain STORMY_PETREL data that only requires a SECRET or even CONFIDENTIAL read-on to STORMY_PETREL. The banner in both cases is the same, and therefore does not provide sufficient information to determine whether a user needs a TOP SECRET read-on to STORMY_PETREL, a SECRET read-on to STORMY_PETREL, or just a CONFIDENTIAL read-on to STORMY_PETREL.

Executive Order (EO) 13526, *Executive Order 13526 – Classified National Security Information* ^[5], Section 4.3, states “ (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. ” Since creation of SAPs is owned by several different agencies, there may not always be deconfliction of SAP markings across agencies. It is therefore important to retain metadata information about the owner of a SAP in data that is marked with one or more SAPs, especially to support automated access control.

To address these challenges, SAP read-on values in the FAC controlled vocabulary for Fine Access Controls (CVCEnumFineAccessControlType) identify, in the following order:

1. Identification that a FAC value is a SAP, signified by initial characters of 'SAR-'
2. The agency that owns the SAP
3. (Optional) The required classification read-on level for the SAP data, for SAPs that have different read-ons for different classification levels
4. The SAP marking value.

The owning agency, any required classification read-on level, and marking value are separated by colons (:). In addition, since some SAPs contain spaces (e.g., a hypothetical Director of National Intelligence (DNI) SAP BUTTER POPCORN), the value in FAC replaces a space with an underscore and becomes "SAR-DNI: BUTTER_POPCORN". Finally, SAPs may contain underscores; in these markings, the underscores will be duplicated in the FAC controlled vocabulary entry for the SAP (e.g., a FAC attribute value that contains "SAR-DOD: S: STORMY__PETREL" for a DOD SAP marking of STORMY_PETREL).

For a hypothetical DOD SAP STORMY_PETREL that has read-ons at different classification levels, a user with a TOP SECRET read-on to this SAP would have a FAC value of "SAR-DOD: TS: STORMY__PETREL", with a double underscore.

In order to facilitate automated access control for SAPs that have different read-ons for different classification levels, the SAP values in an entity's Fine Access Controls in UIAS.XML^[20] will be denormalized. If a user is granted a TOP SECRET read-on to a hypothetical DOD SAP STORMY_PETREL, the user will have all of the following values in Fine Access Controls:

- "SAR-DOD: TS: STORMY__PETREL"
- "SAR-DOD: S: STORMY__PETREL"
- "SAR-DOD: C: STORMY__PETREL".

For a hypothetical DNI SAP BUTTER POPCORN that does not require different read-ons for different classification levels, an entity would have a single Fine Access Control value of "SAR-DNI: BUTTER_POPCORN".

2.2.3.2 - Rules for SAP Values in Fine Access Controls

In order to ensure that SAP values in FAC follow the patterns documented in the previous section, the SAP values MUST follow the logical pattern, Augmented Backus-Naur Form (ABNF) and Path Language (XPath) regular expression shown below: *Introducing Regular Expressions*^[18]

Logical pattern: SAR-[SAP Authority]:[Optional Classification Level]:[SAP Marking]

SAP ABNF Format

[1] SAP ::= "SAR" "-" "SAPAuthority" ":" OptionalClassification ":" SAPMarking

[2] SAPAuthority : := 3*255(ALPHA)

[3]OptionalClassif : := 0*1("TS" / "S" / "C")
ication

[4] SAPMarking : := 1*255(ALPHA / DIGIT / "_" / "." / "-")

XPath regular expression: ^SAR-[A-Z]{3,}((C|S|TS):){0,1}[A-Za-z0-9._-]{1,}\$

Since FAC is a CES, the Schematron rules that validate SAP values against the regular expression are applied in the Technical Specifications that use FAC, i.e., in UIAS.XML^[20] and AUDIT.XML^[1].

The [A-Z]{3,} portion of the above regular expression provides a general character constraint on the allowed SAP values. EO 13526, *Executive Order 13526 – Classified National Security Information* ^[5], Section 4.3, lists the agencies that are authorized to establish special access programs. These agencies (STATE, DOD, DOE, DHS, AG, and DNI) are the **only** agencies currently authorized to define SAPs. Therefore, the values of the [A-Z]{3,} portion of the SAP regular expression MUST be limited to these six agencies. This version of FAC contains an internal controlled vocabulary, CVEnumFACSARAuthorities, that lists the allowed values for the [A-Z]{3,} portion of the SAP regular expression. Both UIAS.XML^[20] and AUDIT.XML^[1] contain Schematron rules that validate SAP values to constrain the [A-Z]{3,} portion to be one of the values in CVEnumFACSARAuthorities.

2.2.3.3 - Published and Unpublished SAPs

Currently, no SAP markings are published in the IC Markings, *Intelligence Community Markings System Register and Manual* ^[6].

Developers of systems processing SAP from the unpublished Register will need to contact the Point of Contact (POC) listed in [Appendix E - Points of Contact](#) for guidance on how to add unpublished SAPs to “CVEnumFineAccessControlType”.

All SAP values, published or unpublished, MUST conform to the regular expression defined in the preceding section.

Chapter 3 - Constraints

3.1 - “Living” Constraint Rules

These constraint rules are a “living” rule set. The constraint rules provided are a valid starter set and do not attempt to address the full scope of security marking business rules addressed by authoritative security marking guidance, specifically Classification and Control Markings as defined by ICD 710, *Intelligence Community Directive 710* ^[12] implemented in the IC Markings, *Intelligence Community Markings System Register and Manual* ^[6], Information Security Oversight Office (ISOO) 32 Code of Federal Regulations (CFR) Parts 2001 and 2004, *Classified National Security Information (Directive No. 1); Final Rule* ^[17], 22 September 2003, E.O. 13526, *Executive Order 13526 – Classified National Security Information* ^[5], and E.O. 12829, *Executive Order 12829 – National Industrial Security Program, as Amended* ^[4]. These rules will be expanded and modified as the model matures, the IC Markings System Register and Manual ^[6] is modified to reflect IC security marking implementation changes, and as applicable security marking policies change.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

3.2 - Data Validation Constraint Rules

The FAC.CES schema defines the data elements, attributes, cardinalities and parent-child relationships for which FAC.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 ^[7] framework document.

3.2.1 - Value Enumeration Constraints

Several elements and attributes of the FAC.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. An appropriate CVE will be provided for use on networks where the list may be reduced or expanded as necessary. If the processing will occur on a network where the provided CVE is not appropriate, the differentiated CVE may be substituted in the constraint rules since the excluded values would be excluded from use on the lower network.

Developers of systems processing Sensitive Compartmented Information or data related to Special Access Programs from the unpublished register will need to contact the point of contact listed in [Appendix E - Points of Contact](#) for guidance as those values may have been omitted from the CVE.

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

3.2.2 - Additional Constraints

3.2.2.1 - 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.

3.2.3 - Constraint Rules

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

3.3 - Data Rendering Constraint Rules

3.3.1 - Purpose

Rendering rules define constraints on the rendering and display of FAC.CES documents. The intent is to inform the development of systems capable of rendering or displaying FAC.CES data for use by individuals not familiar with the details of the FAC.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.

3.3.2 - Rendering Constraint Rules

The following table contains the information for the FAC.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 tables summarize major features by version for FAC.CES. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, 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^[6] has an implementation date of one year after issuance).

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. FAC Feature Comparison

A.1.1. Features from V2019-MAR to V2022-NOV

Table 5 - FAC.CES Feature comparison V2019-MAR to V2022-NOV

Required date	Feature	V2019-MAR	V2019-SEP	V2021-NOV	V2022-NOV
	Support for hierarchical SCIs	N	F	F	F
	Support for HCS-X	N	F	F	F
	Align with the August 2019 version of the IC Markings Register and Manual	N	N	F	F
	Update to have 4 values for NATO	N	N	F	F
	Incorporate DOD SAPCO guidance on SAPs	N	N	F	F
	SAP values in the CVE have a "SAR-" prefix	N	N	N	F
	Correction to one SAP value	N	N	N	F

A.1.2. Features from V2018-APR to V2019-MAR

Table 6 - FAC.CES Feature comparison V2018-APR to V2019-MAR

Required date	Feature	V2018-APR	V2018-JUL	V2018-NOV	V2019-MAR
	Support for KLM	N	F	F	F
	Support for KLM-R and one other control system	N	N	F	F
	Support for FBI fine access controls	N	N	N	F

A.1.3. Features from V1 to V2018-APR

Table 7 - FAC.CES Feature comparison V1 to V2018-APR

Required date	Feature	V1	V2014-DEC	V2018-APR
	Support for HCS-O and HCS-P	N	F	F
	Support for formerly unpublished SCI compartments and subcompartments	N	N	F

Appendix B Change History

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

Table 8 - CES Version Identifier History

Version	Date	Purpose
1	March 14, 2014	Initial Release
2014-DEC	December 4, 2014	Support for HCS-O and HCS-P Section B.8 - V2014-DEC Change Summary
2018-APR	April 20, 2018	Support for unpublished SCI compartments and subcompartments Section B.7 - V2018-APR Change Summary
2018-JUL	July 31, 2018	Routine revision to technical specification. For details of changes, see Section B.6 - V2018-JUL Change Summary
2018-NOV	November 26, 2018	Routine revision to technical specification. For details of changes, see Section B.5 - V2018-NOV Change Summary
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see Section B.4 - V2019-MAR Change Summary
2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see Section B.3 - V2019-SEP 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-NOV	November 29, 2022	Routine revision to technical specification. For details of changes, see Section B.1 - V2022-NOV Change Summary

B.1 - V2022-NOV Change Summary

Significant drivers for version 2022-NOV include:

- Technical Integration Committee Next Generation (TIC NG)
- Classification Marking Implementation Working Group (CMIWG)
- ODNI Special Programs

[Table 9](#) summarizes the changes made to this technical specification from version 2021-NOV to version 2022-NOV.

Table 9 - V2022-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Correct one SCI in CVEnum-FineAccessControlType- (CR-2022-028)	CVEnum-FineAccessControl-Type.xml modified	Data systems must change their representation of this SCI.
2	Modify SAP values in CVEnum-FineAccessControlType to have a "SAR-" prefix (CR-2022-029)	Documentation modified CVEnum-FineAccessControl-Type.xml modified	Data systems must change their representation of SARs.

B.2 - V2021-NOV Change Summary

Significant drivers for version 2021-NOV include:

- TIC NG
- CMIWG
- ODNI Special Programs

[Table 10](#) summarizes the changes made to this technical specification from version 2019-SEP to version 2021-NOV.

Table 10 - V2021-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Corrected sub-compartment to subcompartment. (CR-2019-172)	Documentation	No impact to systems.
2	Updated DoD 5200.1 citations to 5200.01. (CR-2020-033)	Documentation	No impact to systems.
3	Modified for August 2019 Register and Manual: Changes to SCI Controls: BUR and MVL. Added BUR-DTP. (CR-2020-043)	CVEnum-FineAccessControl-Type.xml modified	Systems need to be updated to accommodate this change
4	Update to have 4 values for NATO (CR-2020-005)	CVEnum-FineAccessControl-Type.xml modified	Systems need to be updated to accommodate this change

#	Change	Artifacts Changed	Compatibility Notes
5	Modify handling of SAP accesses to support DOD SAPCO rules. (CR-2021-024)	Documentation CVerenum-FineAccessControl-Type.xml modified CVerenum-FACSARAuthorities.xml added	Systems need to be updated to accommodate this change

B.3 - V2019-SEP Change Summary

Significant drivers for version 2019-SEP include:

- TIC NG
- CMIWG
- ODNI Special Programs

[Table 11](#) summarizes the changes made to this technical specification from version 2019-MAR to version 2019-SEP.

Table 11 - V2019-SEP Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Modified FAC CVEs to support hierarchical Sensitive Compartmented Information (SCI)s. (CR-2019-016).	CVE	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	Add HCS-X to SCIcontrols (CR-2019-078)	CVerenum-FineAccessControlType	Systems need to be updated to accommodate this change.
3	Update SCIcontrols per ODNI Special Programs (CR-2019-090)	CVerenum-FineAccessControlType	Systems need to be updated to accommodate this change.
4	Update chapters for consistency with other specifications. (CR-2019-095).	Documentation	No impact to systems.
5	Identify the lack of a root node in the Schema Guide. (CR-2019-110)	Documentation	No impact to systems.

B.4 - V2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- CMIWG

The following table summarizes the changes made to 2018-NOV in developing 2019-MAR.

Table 12 - V2019-MAR Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Added FBI access values. (CR-2018-136)	CVE	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Updated documentation to use the specification framework. (CR-2018-126)	Documentation	No impact to systems.

B.5 - V2018-NOV Change Summary

Significant drivers for Version 2018-NOV include:

- CMIWG

The following table summarizes the changes made to 2018-JUL in developing 2018-NOV.

Table 13 - V2018-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Add KLM-R and a new control system to FAC. (CR-2018-137)	CVE CVEEnum- FineAccessControl- Type.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.
2	Fix validity of JSON-LD CVEs. (CR-2018-143)	CVE	Data generation and ingestion systems using JSON need to be updated to accommodate the changes.

B.6 - V2018-JUL Change Summary

Significant drivers for Version 2018-JUL include:

- Community Change Requests

The following table summarizes the changes made to 2018-APR in developing 2018-JUL.

Table 14 - V2018-JUL Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Add KLM to FAC. (CR-2018-109)	CVE CVerenum- FineAccessControl- Type.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes.

B.7 - V2018-APR Change Summary

FAC.CES was retired and merged into the UIAS specification with UIAS version 2016-SEP. FAC.CES is re-established and removed from UIAS in the 2018-APR versions of FAC.CES and UIAS. Any changes that occurred to the Fine Access Control CVE while it was a part of UIAS will not be included in the FAC change history, but instead are listed in the UIAS change history.

Significant drivers for Version 2018-APR include:

- Support for a limited set of unpublished SCI compartments and subcompartments.

The following table summarizes the changes made to this technical specification from Version 2014-DEC to Version 2018-APR.

Table 15 - V2018-APR Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Remove FAC from UIAS to allow the addition of as many formerly unpublished register values to FAC as possible. (CR-2017-143)	All	Data generation and ingestion systems need to be updated to use the modified version string.
2	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-278)	Documentation	No impact to systems.
3	Update prose to align with current specifications. Change e-mail address to ic-standards-support@iarpa.gov. (CR-2017-285)	Documentation	No impact to systems.
4	Update the version numbering EBNF to reflect the existence of Revisions. (CR-2017-243)	Documentation	No impact to systems.
5	Create RelaxNG CVE Fragments for FAC. (CR-2017-190)	CVEs	No impact to systems.
6	Create JSON version of CVEs in FAC (CR-2017-288)	CVEs	No impact to systems.

#	Change	Artifacts Changed	Compatibility Notes
7	Create CSV version of CVEs in FAC (CR-2017-289)	CVEs	No impact to systems.
8	Updated CESVersion attribute to generic regex in the schema and created schematron rule to check current CESVersion (CR-2017-340)	Schema Schematron FAC-ID-00001 added	Data generation and ingestion systems need to be updated to accommodate the changes.
9	The schema change logs will no longer be maintained as of the 2018-APR release. The existing change logs will only serve as legacy information. For changes to schema as of and after 2018-APR, reference the change history in the CES.	Schema	No impact to systems.
10	Added schema PDF. (CR-2018-032)	Documentation	No impact to systems.
11	Rename short name to FAC.CES from FAC.XML since there are multiple non XML formats included. Updated Purpose section to be less XML centric. (CR-2018-040)	Documentation	No impact to systems.
12	Updated section on Understanding Access Control to more accurately represent all of the specifications that participate in access control decisions. (CR-2018-071)	Documentation	No impact to systems.
13	Updated CSV generation to include a column for deprecation date information. (CR-2018-091)	CSV	Systems using CSVs no longer have to look to the XML or JSON for the deprecation date information.

B.8 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- HCS-O/P transition

The following table summarizes the changes made to this technical specification from Version 1 to Version 2014-DEC.

Table 16 - V2014-DEC Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Changed CES Version 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 Schema	Data generation and ingestion systems need to be updated to use the modified version string.
2	Added HCS-O and HCS-P.	CVE FAC	Data generation, ingestion systems need to be updated to handle HCS's transition to HCS-O and HCS-P.
3	Updated HCS and CNWDI Hierarchies.	CVE FAC	None.

Appendix C List of Abbreviations

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

ABNF	Augmented Backus-Naur Form
CES	Controlled Vocabulary Enumeration Encoding Specification
CFR	Code of Federal Regulations
CMIWG	Classification Marking Implementation Working Group
CVE	Controlled Vocabulary Enumeration
DNI	Director of National Intelligence
DOD	Department of Defense
E.O.	Executive Order
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
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard
IEC	International Electrotechnical Commission
ISM	Information Security Markings
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSON	JavaScript Object Notation
POC	Point of Contact
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SCI	Sensitive Compartmented Information

TIC NG	Technical Integration Committee Next Generation
TS	Top Secret
URL	Uniform Resource Locator
XML	Extensible Markup Language
XPath	XML Path 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] DoD Manual 5200.01

Under Secretary of Defense for Intelligence. *DoD Information Security Program (Vol 1-3):*. 5200.01. February 24, 2012.

Vol 1 Available online at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol1.pdf

Vol 2 Available online at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol2.pdf

Vol 3 Available online at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol3.pdf

Vol 4 was replaced by DoDI 5200.48

[3] DoD Manual 5205.07

Under Secretary of Defense for Intelligence. *Special Access Program (SAP) Security Manual: Marking (Vol 4)*. 5205.07. October 10, 2013.

Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520507-V4p.pdf?ver=2020-09-09-110203-730>

[4] E.O. 12829

The White House. *Executive Order 12829 – National Industrial Security Program, as Amended*. Federal Register, Vol. 58, No. 240. 14 December 1993.

Available online at: <https://www.archives.gov/isoo/policy-documents/eo-12829-with-eo-13691-amendments.html>

[5] E.O. 13526

The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.

Available online at: <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>

[6] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.

Available online Intelink-TS at: <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>

[7] 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>

[8] 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

[9] 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>

[10] 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

[11] 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

[12] 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

[13] 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/fdyoylS> (case sensitive – foxtrot delta yankee oscar yankee India Sierra)

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

[14] 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>

[15] 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>

[16] 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>

[17] ISOO 32 CFR Parts 2001 and 2004

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information (Directive No. 1); Final Rule*. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 28, No. 183. 22 September 2003.

Available online at: <https://www.gpo.gov/fdsys/pkg/FR-2003-09-22/pdf/03-24047.pdf>

[18] RegularExpressions

Michael Fitzgerald. O'Reilly Media, Inc.. *Introducing Regular Expressions*.

Available online at: <https://www.oreilly.com/library/view/introducing-regular-expressions/9781449338879/ch01.html>

[19] 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/>

[20] 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>

[21] XSLT2

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

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

Appendix E Points of Contact

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

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

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

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

E-mail: ic-standards-support@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^[15].