



Intelligence Community Technical Specification

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set

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	2
1.4 - Conventions	3
1.4.1 - XML Namespaces	4
1.4.2 - Multiplicity	4
1.5 - Dependencies	5
1.5.1 - Specification Dependencies	5
1.5.2 - Inverse Dependencies	8
Chapter 2 - Development Guidance	9
2.1 - IC UAAS Federation	9
2.2 - IC Enterprise Identity Attribute Names and Values	10
2.2.1 - Admin Organization	11
2.2.2 - Audit Routing Organization	12
2.2.3 - Authority Category	12
2.2.4 - Authority to Operate Status	13
2.2.5 - Authorized IC Person	14
2.2.6 - Clearance	15
2.2.7 - Country of Affiliation	15
2.2.8 - Digital Identifier	16
2.2.9 - Duty Organization	16
2.2.10 - Duty Organization Unit	18
2.2.11 - Entity Security Mark	18
2.2.12 - Entity Type	19
2.2.13 - Fine Access Controls	19
2.2.14 - Group	20
2.2.15 - Handling Controls	21
2.2.16 - IC Networks	21
2.2.17 - Is IC Member	22
2.2.18 - Life Cycle Status	23
2.2.19 - Region	23
2.2.20 - Role	24
2.2.21 - Topic	24
2.3 - IC Enterprise Environment Attribute Names and Values	25
2.3.1 - Certificate Authority	25
2.3.2 - Originating Network	26
Chapter 3 - Constraints	27
3.1 - Data Validation Constraint Rules	27
3.1.1 - Value Enumeration Constraints	27
3.1.2 - Additional Constraints	27
3.1.2.1 - DES Constraints	27
3.1.3 - Constraint Rules	27
3.2 - Data Rendering Constraint Rules	28
3.2.1 - Purpose	28
3.2.2 - Rendering Constraint Rules	28

Appendix A - Feature Summary	29
A.1 - UIAS.XML Feature Comparison	29
A.1.1 - Features from V2018-APR to V2021-NOV	29
A.1.1.1 - Features Partial and N/A from V2018-APR to V2021-NOV	30
A.1.2 - Features from V2015-AUG to V2018-APR	30
A.1.3 - Features from V3 to V2015-AUG	31
A.1.4 - Features from V1 to V3	31
Appendix B - Change History	32
B.1 - V2021-NOV Change Summary	33
B.2 - V2019-SEP Change Summary	36
B.3 - V2018-APRr2018-NOV Change Summary	36
B.4 - V2018-APR Change Summary	37
B.5 - V2016-SEPr2017-JUL Change Summary	39
B.6 - V2016-SEP Change Summary	40
B.7 - V2015-AUG Change Summary	43
B.8 - V2014-DEC Change Summary	44
B.9 - V3.1 Change Summary	45
B.10 - V3 Change Summary	45
B.11 - V2.1 Change Summary	46
B.12 - V2 Change Summary	46
Appendix C - Glossary	48
Appendix D - List of Abbreviations	51
Appendix E - Bibliography	54
Appendix F - Points of Contact	60
Appendix G - IC CIO Approval Memo	61

List of Figures

Figure 1 - Related Specifications	7
Figure 2 - Inverse Dependency Specifications	8
Figure 3 - UAAS Federation	10

List of Tables

Table 1 - Operational Usage	2
Table 2 - XML Namespaces	4
Table 3 - Definitions of Multiplicities	4
Table 4 - Direct Dependencies	5
Table 5 - Admin Organization	11
Table 6 - Foreign Government adminOrganization Countries	11
Table 7 - AuditRoutingOrganization	12
Table 8 - AuthorityCategory	12
Table 9 - ATO Status	13
Table 10 - AICP	14
Table 11 - Clearance	15
Table 12 - Country of Affiliation	15
Table 13 - Digital Identifier	16
Table 14 - Duty Organization	16
Table 15 - Foreign Government dutyOrganization Countries	17
Table 16 - Duty Organization Unit	18
Table 17 - Entity Security Mark	18
Table 18 - Entity Type	19
Table 19 - Fine Access Controls	19
Table 20 - Group	20
Table 21 - Handling Controls	21
Table 22 - IC Networks	21
Table 23 - Is IC Member	22
Table 24 - Life Cycle Status	23
Table 25 - Region	23
Table 26 - Role	24
Table 27 - Topic	24
Table 28 - Certificate Authority	25
Table 29 - Originating Network	26
Table 30 - Constraint Rules	28
Table 31 - Feature Summary Legend	29
Table 32 - UIAS.XML Feature Comparison V2018-APR to V2021-NOV	29
Table 33 - UIAS.XML Feature Comparison V2018-APR to V2021-NOV	30
Table 34 - UIAS.XML Feature Comparison V2015-AUG to V2018-APR	30
Table 35 - UIAS.XML Feature Comparison V3 to V2015-AUG	31
Table 36 - UIAS.XML Feature Comparison V1 to V3	31
Table 37 - Identifier History	32
Table 38 - Data Encoding Specification V2021-NOV Change Summary	33
Table 39 - Data Encoding Specification V2019-SEP Change Summary	36
Table 40 - V2018-APRr2018-NOV Change History	37
Table 41 - V2018-APR Change History	37
Table 42 - V2016-SEPr2017-JUL Change History	39
Table 43 - V2016-SEP Change History	40
Table 44 - V2015-AUG Change History	44
Table 45 - V2014-DEC Change History	44
Table 46 - V3.1 Change History	45

Table 47 - V3 Change History	45
Table 48 - V2.1 Change History	46
Table 49 - V2 Change History	46

Chapter 1 - Introduction

1.1 - Purpose

This technical specification, *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML), governs the set of Intelligence Community (IC) enterprise Unified Identity Attribute Set (UIAS) and associated values that must be supported by an Attribute Service (AS) participating in the IC's Unified Authorization and Attribute Services (UAAS) capability. The specification is the basis for defining and populating the set of attributes and values that comprise an attribute statement or assertion, e.g., Security Assertion Markup Language (SAML) Attribute Statement as described in the SAML 2.0 Attribute Sharing, *SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, [Encrypted Mode]*^[38], 27 March 2008.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[15]) defines the basic conceptual structure and outlines the core philosophy of IC technical specifications. For convenience, a copy of this framework is included in every package.

This specification is applicable to the IC and access to the information produced by, stored within, or shared throughout the IC's Top Secret (TS/) Sensitive Compartmented Information (SCI) information domain as defined in Intelligence Community Program Guidance (ICPG) 500.2, *Attribute-Based Authorization and Access Management*^[22] Identity attributes defined at the enterprise level within the IC may have relevance outside the scope of the IC; however, prior to applying outside of this defined scope, the models should be closely scrutinized and differences separately documented and assessed for applicability.

This document lists identity attributes, multiplicity and values defined at the enterprise level for entities, both persons and non-person entities (e.g., machines, servers, services, processes, applications, etc.) within the IC information domain required for UAAS exchange in direct support of Intelligence Community Standard (ICS) 500-30, *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*^[27]. In the case that the attribute is not applicable to a type of entity, or if the entity does not have any values listed for the particular attribute, then the attribute is not exchanged as part of the attribute assertion. This document also lists environmental identity attributes, multiplicity and values defined at the enterprise for entities, that may or may not be part of the UAAS exchange.

The primary audience for this document is the implementer and/or administrator who must configure an Attribute Service to meet the requirements for participation in the IC UIAS capability. The audience for this document also includes:

- Those responsible for implementing and managing the capabilities that create, provide, modify, store, exchange, search, display, or further process IC enterprise identity attributes.
- Data stewards for protected resources, who will use this information to develop policies for access control.
- Those responsible for provisioning and maintaining AAS.

This document applies to all IC enterprise identity attributes exchanged amongst UIAS-compliant Attribute Services and capabilities on the IC information domain.

This document identifies the operational usage for each of the identity attributes. These include, but are not limited to ingest, discovery, access, and audit.

Table 1 - Operational Usage

Operational Usage	Definition
Ingest	Enables high-quality data to be brought into the processing environment
Discovery	Enables searching and rapid location of useful data
Access	Enables rule-based access decisions based on law, policy, and mission constraints
Audit	Enables understanding and ability to audit person and non-person participation in key events

In addition to enterprise identity attributes, there are other classes of attributes (such as extended and local) that may be used to further protect resources as appropriate, but they are outside the scope of this document. Those extended and local attributes or attribute values **MUST NOT** conflict with the attributes and values described in this document. Undocumented attribute exchange is supported by UAAS, as described in the AATT CONOPS, *Department of Defense and Intelligence Community Unified Authorization and Attribute Service, Concept of Operations* ^[1], December 8, 2008, Version 1.11. These additional attributes may become enterprise attributes over time, necessitating updates to this document.

IC Enterprise Identity Attributes are assigned per persona. A persona is an electronic identity that is unambiguously associated with a single person or Non-Person Entity (NPE). A single person or NPE may have multiple personas, with each persona being managed by the same or by different organizations (e.g., a Director of National Intelligence (DNI) contractor who is also an Army reservist).

1.3 - Enterprise Need

Defining the set of IC enterprise identity attributes and values for sharing through the IC UAAS supports the opportunity for consistent and assured information sharing across the enterprise. The IC UAAS supports ICS 500-30^[27] to promote on-demand access to information and other resources by IC users and services, and reduces authorization vulnerabilities by strengthening the access control decision process.

Implementers of IC UIAS-compliant attribute services require coordination of identity attribute definitions. This requires the usage of standardized attribute names and values when exchanging attribute assertions (e.g., SAML protocol messages) between systems participating in the IC UIAS.

This technical specification relates to the Attribute Practice Compliance Statement (APCS) used by all agencies and system owners who write the Attribute Practice Statement (APS) required for

each AAS and AS of an IC element and comply with ICS 500-30^[27] as well as operators and resource owners that rely on attributes for authorization decisions. The APCS, published by the IC Chief Information Officer (CIO), contains a compliance statement for each attribute identified in the UIAS.XML technical specification for both Person Entity (PE)s and NPEs that are US owned, controlled, and vetted.

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

- 100 Series:
 - Intelligence Community Directive (ICD) 121, *Managing the Intelligence Community Information Environment* ^[16]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[17]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* ^[18]
 - ICPG 500.1, *Digital Identity* ^[21]
 - ICPG 500.2, *Attribute-based Authorization and Access Management* ^[22]
 - ICS 500-20, *IC Enterprise Standards Compliance* ^[24]
 - ICS 500-27, *Collection and Sharing of Audit Data* ^[25]
 - ICS 500-29, *IC Digital Identifier* ^[26]
 - ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources* ^[27]
- 700 Series:
 - ICPG 704.5, *Intelligence Community Security Database Scattered Castles* ^[23]
- Memorandums:
 - OMB Memo - *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* ^[35]
 - OMB Memo - *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* ^[34]
 - IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* ^[10]
- DoD Issuances:
 - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* ^[5]
- Presidential Directives
 - HSPD-12 *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* ^[9]

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^[15].

Several key terms in this document are to be interpreted as defined in ICS 500-30, *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources* ^[27], Appendix B. These terms, with their definitions are defined in the [Appendix C - Glossary](#) and include the following: APS, Attribute, AS, AAS, DN, Integree, NPE, and PE.

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 2 - XML Namespaces

Prefix	URI
uias	urn:us:gov:ic:uias

Additionally within this technical specification there is the notation that some attributes are only applicable to person or non-person entities. These conditional multiplicity values are noted as “P” for persons and “NPE” for non-persons.

1.4.2 - Multiplicity

Throughout this document, references are made to the multiplicity of attributes and parameters. Multiplicity defines the allowed number of occurrences of an attribute value, and whether the attribute is required or optional.

Table [Table 3](#) follow Object Management Group (OMG)'s UML, *Unified Modeling Language* [\[40\]](#) and International Organization for Standardization (ISO) 11179-3, *SO/IEC 11179, Information Technology -- Metadata registries (MDR), Part 3: Registry metamodel and basic attributes* [\[28\]](#).

Table 3 - Definitions of Multiplicities

Multiplicity	Description
[1..1]	Indicates the attribute is mandatory and must contain one and only one value.
[0..1]	Indicates the attribute is optional and may contain at most one value.
[0..*]	Indicates the attribute is optional and may contain any number of values, including none.
[1..*]	Indicates the attribute is mandatory and may contain one or more values.
[0..n]	Indicates the attribute is optional and may contain at most n values, where n is a finite integer. An example in this specification is the multiplicity of auditRoutingOrganization , which is [0..10].
[n..m]	Indicates the attribute is mandatory having at least n values, and may contain at most m values, where n and m are finite integers.

In some cases within this specification, attribute value multiplicity requirements for an attribute will vary depending on whether the entity is a person entity or a non-person entity. In these situations,

multiplicity requirements will be noted with "PE" for person entities, and "NPE" for non-person entities.

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^[15].

1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 4](#). 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 4](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 4](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 4 - Direct Dependencies

Name	Dependency Description
<i>CVE Encoding Specification for Authority Categories</i> (AUTHCAT.CES.V2018-APR+ ^[2])	This specification does not depend on a specific version of AUTHCAT.CES ^[2] ; versions later than version 2018-APR 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.
<i>CVE Encoding Specification for Fine Access Control</i> (FAC.CES.V2019-SEP+ ^[8])	This specification depends only on the set of tokens and associated meanings defined in the FAC.CES ^[8] . This specification does not depend on the schema, business rules, etc. defined for Fine Access Control (FAC) or those of any of FAC's dependencies. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.

Name	Dependency Description
<i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES.V2019-SEP+ ^[14])	This specification depends on the LATEST technically sound, approved version of IC-GENC.CES ^[14] . At the time of this release, the latest version of IC-GENC.CES is 2019-SEP and MUST be used unless a later, technically sound, approved version of IC-GENC.CES has been released. The requirement to use the latest technically sound, approved version is based on authoritative source compliance ^[36] .
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[29])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[29] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[20] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>CVE Encoding Specification for Mission Need</i> (MN.CES.V2017-MAYr2019-MAR+ ^[31])	This specification does not depend on a specific version of MN.CES ^[31] ; versions later than version 2017-MAYr2019-MAR MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.
<i>CVE Encoding Specification for Role</i> (ROLE.CES.V2021-NOV+ ^[37])	This specification does not depend on a specific version of ROLE.CES ^[37] ; versions later than version 2021-NOV MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.
<i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES.V2017-MARr2018-FEB+ ^[41])	This specification does not depend on a specific version of USAgency.CES ^[41] ; versions later than version 2017-MARr2018-FEB MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.
<i>XML Data Encoding Specification for Virtual Coverage</i> (VIRT.XML.V2020-OCT+ ^[42])	This specification does not depend on a specific version of VIRT.XML ^[42] ; versions later than version 2020-OCT MAY be used. The minimum version was based on the earliest non-retired version; ESB 21-2.0 was used for determining the version.

Name	Dependency Description
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[15])	This specification does not depend on a specific version of IC-SF.XML ^[15] ; 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.
SAML Version 2.0 Attribute Sharing Profile for ITU-T standard for public key infrastructures (X.509) Authentication-Based Systems, Version 1.0, [Encrypted Mode] (27 March 2008) ^[38]	Specification for attribute sharing.
Transformations (XSLT) 2.0 ^[43] implementation of Schematron ^[39] 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 <i>behavior</i> 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 <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.

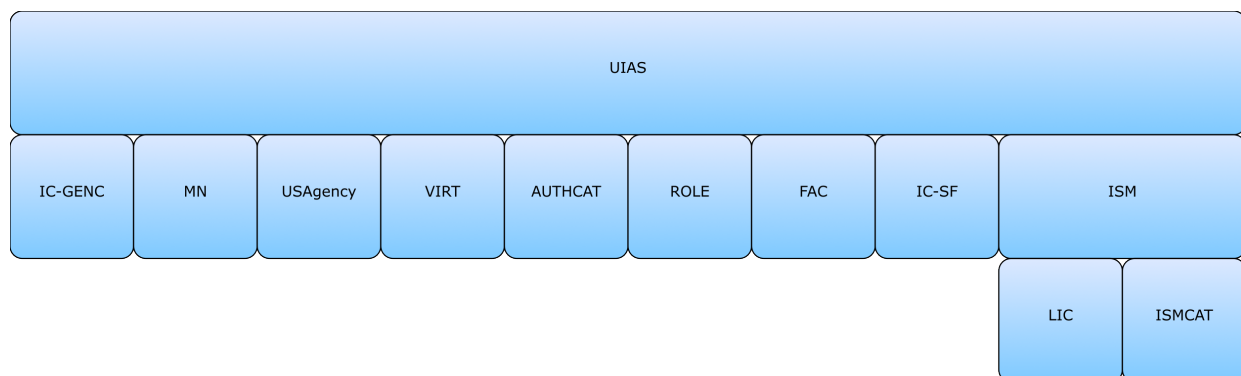


Figure 1 : Related Specifications

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](#).

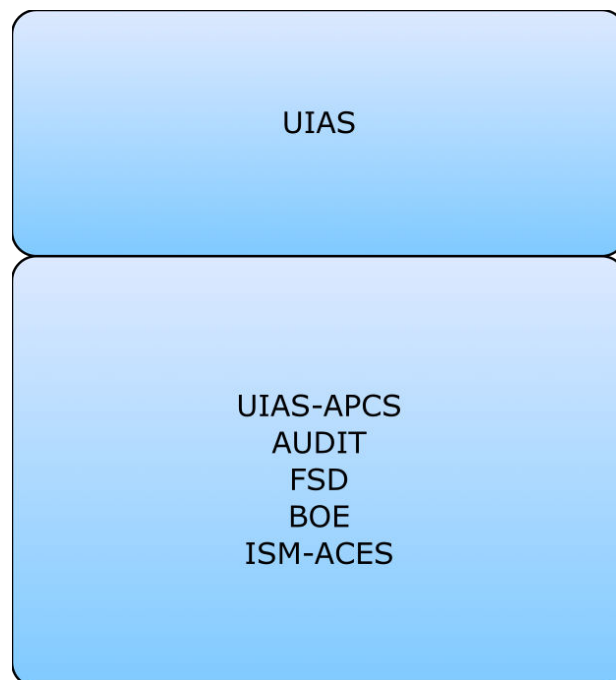


Figure 2 : Inverse Dependency Specifications

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^[15] 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 - IC UAAS Federation

The IC UAAS is a federation of agency-based attribute service providers that exchange attributes in order to support systems employing an Attribute Based Access Control (ABAC) model. The UAAS federation contains six providers, i.e. Central Intelligence Agency (CIA) Central Intelligence Agency (CIA) Virtual Directory Engine – JWICS (VDE-J), Defense Intelligence Agency (DIA) DoDIIS Identity and Authorization Services (DIAS), National Reconnaissance Office (NRO) Identity Access Management Service (IAMS), National Geospatial Intelligence Agency (NGA) GEOAxIS, National Security Agency (NSA) AccessIT!, and National Security Agency (NSA) Intelligence Community Service Operations Group (ICSOG) (Common Services). DoDIIS Identity and Authorization Services (DIAS) supports all military IC elements, e.g., Army, whereas ICSOG (Common Services) support all other IC elements, e.g., Treasury Department.

The UAAS provides an attribute service and most systems employing Attribute Based Access Control (ABAC) leverage the UAAS federation for UIAS.XML attribute retrieval. The UAAS in turn obtains these UIAS.XML attributes from AASs, such as the providers’ agency-based Security and HR based systems, or shared repositories of common concern, for example the IC Full Service Directory (FSD) for HR-related attributes and Scattered Castles (as defined by ICPG 704.5, *Intelligence Community Security Database Scattered Castles*^[23]) for security-related attributes. The UAAS service provider nodes may also provide an authorization service, i.e. a full range of access control rule sets and policy decision points for any system that is configured to offload (outsource) this function. There is a great variety of configurations for systems across the IC that leverage the UAAS for attributes.

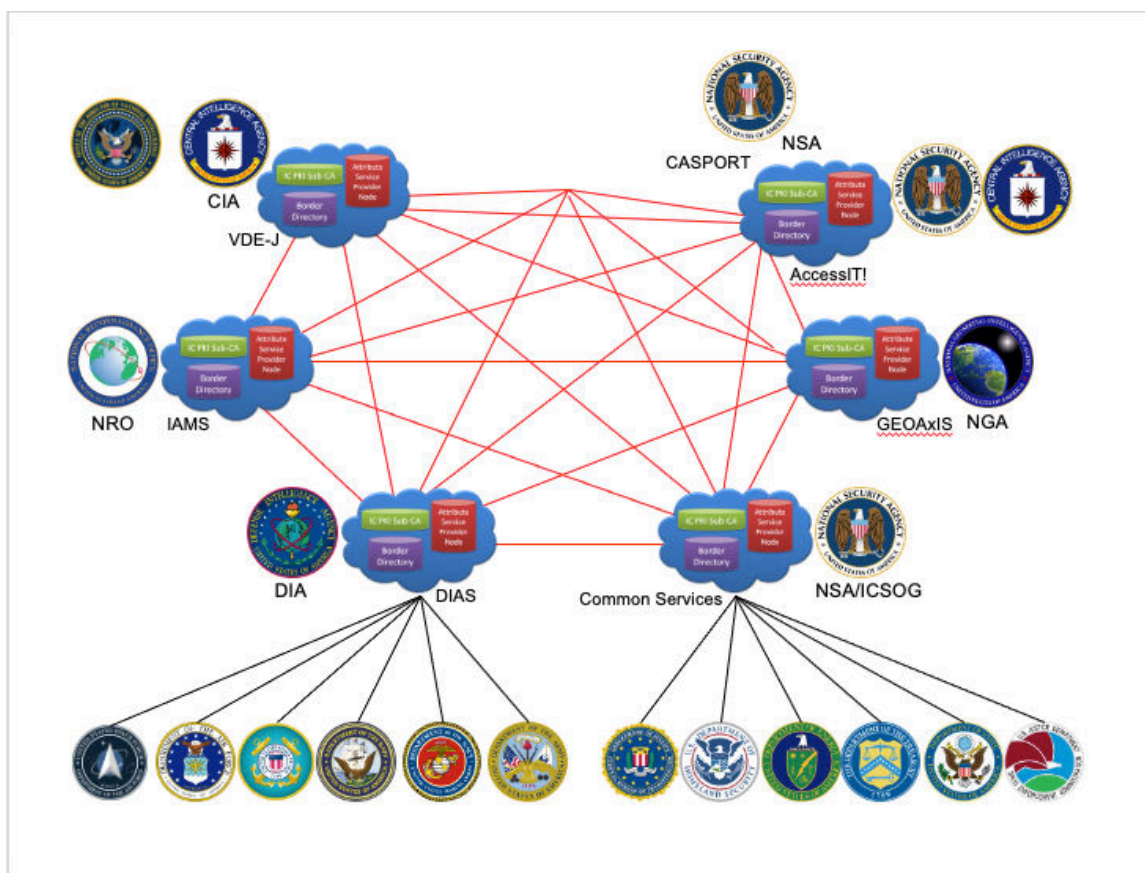


Figure 3 : UAAS Federation

2.2 - IC Enterprise Identity Attribute Names and Values

The attributes as defined in this specification represent the set of IC enterprise identity attributes and associated values that must be supported by an AS participating in the IC's UAAS capability. UAAS exchange requires using these attributes and values for exchange of attributes for both persons and non-person entities, except where indicated in the definition and multiplicity.

All of these attributes may be required within an attribute assertion sent in response to an attribute query originating from another Attribute Service for entity's attributes. In cases where attribute names and values defined below differ in underlying authoritative sources or agency implementations, they must be transformed or derived to match this specification before passing them via the UAAS.

In each of the definitions below, the entity's persona is uniquely identified within the IC information domain (as defined in ICPG 500.1 *Digital Identity*^[21]) by the Distinguished Name (DN) in the Public Key Infrastructure (PKI) issued certificate. Persons or non-person entities (e.g., servers, services, applications, etc.) may have one or more persona.

To ensure trust, where authoritative sources for Allowed Values are cited for specific attributes, the authoritative source must support and work in conjunction with this technical specification and under guidance from designated community governance authorities by managing and governing the Controlled Vocabulary Enumeration (CVE)s for the value set.

2.2.1 - Admin Organization

Table 5 - Admin Organization

Attribute Name	adminOrganization
Definition/Purpose	Reflects the home organization of the entity.
Allowed Values	Summation of two sets: <ul style="list-style-type: none"> Includes values listed in <i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES^[41]), in the CVE "CVEnum-USAgencyAcronym". Values listed in table Table 6
Multiplicity	[1..1]
Example	USA.DIA, USA.FBI, GBR.GCHQ
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:adminOrganization

This attribute specifies the home or administrative organization affiliation with which the entity (person or non-person) is associated. For persons, the administrative organization is the one that maintains their personnel records. For non-person entities, the administrative organization is the one that controls the administration of the NPE when in use.

The **@adminOrganization** attribute may be used for identifying the home or administrative organization of the entity, but may also be used for access control decisions where relevant to the protected resource provider.

Authoritative sources can apply specific internal policies for use of this attribute.

In support of Second Party Integree (2PI) and Second Party Sovereign (2PS), additional values for **@adminOrganization** are needed to identify the entity's top-level foreign government agency and the country of the entity's foreign government agency.

Table 6 - Foreign Government adminOrganization Countries

Value	Definition
AUS.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of Australia (AUS)
CAN.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of Canada (CAN)
GBR.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of the United Kingdom (GBR)
NZL.[A-Za-z0-9_-\.\.]{1,36}	Agencies that are operating under the government of New Zealand (NZL)

The values that appear in the Foreign Government @**adminOrganization** Countries table are Regular Expressions (REGEX), a kind of short-hand description of allowable values for the given field. Allowable values can be interpreted as follows:

- AUS., CAN., GBR., or NZL. indicates the value must begin with one of those sequences.
- {1:36} indicates that 1 to 36 characters can follow the opening sequence.
- [A-Za-z0-9_-\.] indicates the 1 to 36 characters that follows the opening sequence can be upper or lower case alphabetic characters, any digit from 0 to 9, or underscore ('_'), dash ('-'), or period('.') characters.
- Example: New Zealand Government Communications Security Bureau might be represented as NZL.GCSB.

2.2.2 - Audit Routing Organization

Table 7 - AuditRoutingOrganization

Attribute Name	auditRoutingOrganization
Definition/Purpose	This attribute specifies the organization(s) to which Audit Records should be forwarded in addition to the entity's dutyOrganization and adminOrganization .
Allowed Values	Includes values listed in USAgency.CES ^[41] , in the CVE "CVEnumAuditRoutingOrg".
Multiplicity	[0..10]
Examples	USA.CIA, USA.USPACOM, USA.EOP
Operational Usage	Audit
Attribute Identifier	urn:us:gov:ic:uias:auditRoutingOrganization

This attribute specifies the organization(s) to which Audit records will be routed beyond the entity's **adminOrganization** and **dutyOrganization**. Audit software and services **MUST** always route audit records to both the **adminOrganization** and **dutyOrganization**. If the entity has values in **auditRoutingOrganization**, then audit software and services **MUST** also route audit data to the organizations in **auditRoutingOrganization**.

2.2.3 - Authority Category

Table 8 - AuthorityCategory

Attribute Name	authorityCategory
Definition/Purpose	This attribute specifies the authority(ies) under which the entity is authorized to access and/or discover protected resources.

Attribute Name	authorityCategory
Allowed Values	Includes values listed in <i>CVE Encoding Specification for Authority Categories</i> (AUTHCAT.CES ^[2]), in the CVE "CVEnum-AuthCatType".
Multiplicity	[0..*]
Examples	ICD503, FISA_B, EO12333_IA, DODD8530_USA
Operational Usage	Access, Discovery
Attribute Identifier	urn:us:gov:ic:uias:authorityCategory

This attribute specifies the authority under which the entity (person or non-person) is authorized to access and/or discover protected resources.

Authority types can include, but are not limited to, legal, policy, training or mission.

@**authorityCategory** is used for access control decisions to protected resources. If the entity does not have any values listed for the @**authorityCategory** attribute, then the attribute is not exchanged as part of the attribute assertion.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.2.4 - Authority to Operate Status

Table 9 - ATO Status

Attribute Name	ATOStatus
Definition/Purpose	This attribute indicates the authority decision status for the non-person entity.
Allowed Values	Boolean: 0,1,true, false
Multiplicity	Conditional: P = [0..0] NPE = [1..1] Default=false
Example	true
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:ATOStatus

This attribute indicates the authorization decision, formerly known as Authority To Operate (ATO), status for the non-person entity. As defined by ICD 503, *Intelligence Community Information Technology Systems Security Risk Management* ^[19] an authorization decision is approved for operation at a particular level of security in a particular environment, with the established level of risk associated with operating the system. This includes authorization decisions with conditions, which can be derived based upon the approved necessary conditions of the approving authority (e.g., if an Interim Authority to Test has been granted). A value of "**true**" indicates that an

favorable authorization has been granted. A value of **"false"** indicates an authorization has not been granted.

The **@AToStatus** attribute is only applicable for non-person entities. If the UIAS exchange is for a person entity, then the **@AToStatus** attribute is not exchanged as part of the attribute assertion.

The **@AToStatus** attribute should be used in conjunction with the **@lifeCycleStatus** attribute to determine the actual status of the NPE.

2.2.5 - Authorized IC Person

Table 10 - AICP

Attribute Name	aICP
Definition/Purpose	Reflects whether or not the entity is an Authorized IC Person (AICP).
Allowed Values	Boolean: 0,1,true, false
Multiplicity	Conditional: P = [1..1] NPE = [0..0] Default=false
Example	true
Operational Usage	Access, Discovery
Attribute Identifier	urn:us:gov:ic:uias:aICP

AICP is defined by ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* ^[18] as follows:

"A U.S. person employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, has a mission need and an appropriate security clearance for information collected or analysis produced. Authorized IC personnel shall be identified by their IC element head and shall have discovery rights to information collected and analysis produced by all elements of the IC. The term may include contractor personnel."

This attribute is a flag that reflects whether a person has been identified by their IC element head to act as an AICP. Under ICD 501 ^[18], only users employed by, assigned to, or acting on behalf of an IC element may be AICPs.

This is a Boolean attribute that is set to **"false"** by default. Where this attribute is unpopulated, its value shall be treated as **"false"** by the receiving system. **@aICP** will only be set to **"true"** if the **@isICMember** attribute is also set to **"true"**.

The **@aICP** attribute is specific to only U.S. persons and associated personas, and is not applicable to non-person entities, and is used for access control decisions to protected resources. The **@aICP** attribute is not applicable to Second Party Integrees.

If the UIAS is for a non-person entity, then the **@aICP** attribute is not exchanged as part of the attribute assertion.

2.2.6 - Clearance

Table 11 - Clearance

Attribute Name	clearance
Definition/Purpose	Reflects the clearance or classification level of the entity.
Allowed Values	Includes values listed in the CVE for Clearance “CVCEnumUIASCclearance”.
Multiplicity	[1..*]
Examples	TS, Q
Operational Usage	Access, Ingest
Attribute Identifier	urn:us:gov:ic:uias:clearance

This attribute specifies the entity’s highest security clearance level(s) for a person entity, or the highest security classification of information that can be handled by an NPE.

It contains values from United States (US) National Security Information (NSI) and the Department of Energy (DOE). If an entity has a clearance in more than one of these classification or protection marking systems, the highest security clearance/authorization from each must be listed.

Note: The schema does NOT indicate that an entity holds an “interim” clearance.

The @clearance attribute is used for access control decisions to protected resources.

2.2.7 - Country of Affiliation

Table 12 - Country of Affiliation

Attribute Name	countryOfAffiliation
Definition/Purpose	Reflects the citizenship(s) or affiliation(s) of the entity.
Allowed Values	Includes values listed in <i>CVE Encoding Specification for Geopolitical Entities, Names, and Codes</i> (IC-GENC.CES ^[14]), in the CVE “CVCEnumGENCCountryCode”.
Multiplicity	[1..*]
Examples	GBR, USA
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:countryOfAffiliation

In the case of person entities, this is the identifier of the person entity’s country or countries of citizenship. In the case of non-person entities, this represents the citizenship of the administrator(s) and/or the organization(s) in control of the non-person entity.

The **@countryOfAffiliation** attribute is multi valued, since an entity could possibly have multiple citizenships (e.g., “dual citizenship”) relevant for access control decisions.

2.2.8 - Digital Identifier

Table 13 - Digital Identifier

Attribute Name	digitalIdentifier
Definition/Purpose	Reflects the DN from the entity’s PKI certificate.
Allowed Values	DN from the entity’s PKI certificate.
Multiplicity	[1..1]
Examples	cn=Doe John A jdoe, ou=DNI, o=U.S Government, c=US cn=webserver.dni.ic.gov, ou=DNI, o=U.S. Government, c=US
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:digitalIdentifier

The **@digitalIdentifier** is the representation that uniquely identifies a person or non-person IC entity’s persona. ICS 500-29, *Intelligence Community Digital Identifier* [\[26\]](#) specifies that the IC Digital Identifier (DI) is the DN from the PKI Certificate, and is unique to the persona associated with that certificate.

A *DN* is a string representation that uniquely identifies a subject within a PKI. An UIAS-compliant Attribute Service must use the DN from an entity’s PKI certificate associated with that particular persona as the means for specifying the subject identity in attribute assertion being exchanged between partners in the federation. The PKI Certificate is not the authoritative source for attributes and parsing the certificate should not be used for granting access. The DN is treated as an opaque key to retrieve the associated persona’s attributes.

The DN entry is single valued, but an entity could possibly have multiple DNs, with a unique persona per DN as defined by ICS 500-29 [\[26\]](#).

2.2.9 - Duty Organization

Table 14 - Duty Organization

Attribute Name	dutyOrganization
Definition/Purpose	Reflects the assigned organization of the entity.

Attribute Name	dutyOrganization
Allowed Values	Summation of two sets: <ul style="list-style-type: none"> Includes values listed in <i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES^[41]), in the CVE “CVEnum-USAgencyAcronym”. Values listed in table Table 6
Multiplicity	[1..1]
Example	USA.DNI, GBR.GCHQ
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:dutyOrganization

This attribute specifies the organization which the entity (person or non-person) is representing.

The **@dutyOrganization** attribute may differ from **@adminOrganization** in cases where the entity is detailed from his or her home or administrative agency to another agency for a Joint Duty assignment or other rotation, or the NPE is loaned or transferred from its administrative agency to another agency, or operated by another agency.

In support of 2PI, the **@dutyOrganization** should represent the US government sponsoring agency.

In support of 2PS, the **@dutyOrganization** should represent the non-US government sponsoring agency.

Table 15 - Foreign Government dutyOrganization Countries

Value	Definition
AUS.[A-Za-z0-9_\-\.]{1,36}	Agencies that are operating under the government of Australia (AUS)
CAN.[A-Za-z0-9_\-\.]{1,36}	Agencies that are operating under the government of Canada (CAN)
GBR.[A-Za-z0-9_\-\.]{1,36}	Agencies that are operating under the government of the United Kingdom (GBR)
NZL.[A-Za-z0-9_\-\.]{1,36}	Agencies that are operating under the government of New Zealand (NZL)

The values that appear in the Foreign Government **@dutyOrganization** Countries table are Regular Expressions (REGEX), a kind of short-hand description of allowable values for the given field. Allowable values can be interpreted as follows:

- AUS., CAN., GBR., or NZL. indicates the value must begin with one of those sequences.
- {1:36} indicates that 1 to 36 characters can follow the opening sequence.

- [A-Za-z0-9_-\.] indicates the 1 to 36 characters that follows the opening sequence can be upper or lower case alphabetic characters, any digit from 0 to 9, or underscore ('_'), dash ('-'), or period('.') characters.
- Example: New Zealand Government Communications Security Bureau might be represented as NZL.GCSB.

2.2.10 - Duty Organization Unit

Table 16 - Duty Organization Unit

Attribute Name	dutyOrganizationUnit
Definition/Purpose	Reflects the assigned organization unit structure of the entity.
Allowed Values	Agency defined authoritative organization unit structure of the entity's duty organization separated by colons.
Multiplicity	[0..1]
Example	USA.CIA:CIO:APPS:EASPO
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:dutyOrganizationUnit

This attribute specifies the organization unit structure which the entity (person or non-person) is representing.

2.2.11 - Entity Security Mark

Table 17 - Entity Security Mark

Attribute Name	entitySecurityMark
Definition/Purpose	Classification and handling of the entity's digital identity.
Allowed Values	Includes values listed in the CVE for Security Mark Type "CVEEnumUIASSecurityMarkType".
Multiplicity	[0..1]
Example	SECRET//REL TO USA, AUS, CAN, GBR, NZL
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:entitySecurityMark

This attribute specifies the classification and handling for the entity's (person or non-person) digital identity, and is used for determining if the entity's digital identity can be transmitted to another network or domain. An **@entitySecurityMark** does not specify the classification and handling of the entity's assertion as a whole, and does not presuppose which UIAS.XML attribute values may be transmitted to other networks or domains without additional filtering.

If there is a value in **@entitySecurityMark**, the **@entitySecurityMark** attribute should be used in conjunction with **@icNetworks** attribute to determine if an entity's digital identity and approved subset of attributes should be transmitted to another network or domain.

If no value for **@entitySecurityMark** is present, the attribute is not exchanged as part of the attribute assertion, and the entity's digital identity and approved subset of attributes will not be transmitted to another network or domain.

2.2.12 - Entity Type

Table 18 - Entity Type

Attribute Name	entityType
Definition/Purpose	Reflects the type of the entity.
Allowed Values	Includes values listed in the CVE for Entity Type "CVEnumUIASEntityType".
Multiplicity	[1..1]
Example	GOV
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:entityType

This attribute indicates the type of the entity (person or non-person), and may be used for access control to protected resources. The value of the attribute will indicate if the entity is a person or non-person.

Further clarification of attribute values and their definitions can be found in the CVE.

2.2.13 - Fine Access Controls

Table 19 - Fine Access Controls

Attribute Name	fineAccessControls
Definition/Purpose	Reflects the fine grain access aspects of control systems.
Allowed Values	Includes values listed in <i>CVE Encoding Specification for Fine Access Control</i> (FAC.CES ^[8]), in the CVE "CVEnum-FineAccessControlType". Developers of systems processing SCI or Special Access Program (SAP) from the unpublished register will need to contact the Point of Contact (POC) listed in Appendix F - Points of Contact for guidance as those values may have been omitted from the CVE.

Attribute Name	fineAccessControls
Multiplicity	[1..*]
Examples	HCS, SI, TK
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:fineAccessControl

This attribute includes but is not limited to the values listed under SCI Control Systems and Compartments, Special Access Programs/Special Access Restrictions, Atomic Energy Act (AEA), Department of Defense (DoD) Critical Nuclear Weapons Design Information (CNWDI), North Atlantic Treaty Organization (NATO) read-ons, and DoE compartments which an entity (person or non-person) is authorized to access or process. It also includes the caveats ¹ associated with the clearances, where appropriate. The values in “CVENumFineAccessControl”, in FAC.CES^[8], do not represent all allowed values. For example, there are some allowed Unpublished SCI compartments and subcompartments not included in these resources. Use of these special values requires coordination outside of the UIAS.XML specification.

Note: The schema does NOT indicate that an entity holds an “interim” SCI control.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.2.14 - Group

Table 20 - Group

Attribute Name	group
Definition/Purpose	Indicates the group memberships associated with the entity.
Allowed Values	Values governed by the Identity, Credential, and Access Management (ICAM) Service Provider Entitlement Management Service.
Multiplicity	[0..*]
Examples	To Be Determined (TBD)
Operational Usage	Access, Discovery, Ingest, Audit
Attribute Identifier	urn:us:gov:ic:uias:group

This attribute characterizes the entity’s (person or non-person) authorized group membership that the entity needs to perform an expected task.

The **@group** attribute is used for access control decisions to protected resources. If the entity does not have any values listed for the **@group** attribute, then the attribute is not exchanged as part of the attribute assertion.

¹See IC Markings, *IC Markings System Register and Manual*^[12] for more information.

It is the responsibility of the ICAM Service Provider to govern allowed values and the ICAM Service Provider Entitlement Management Service to manage and expose the values to the enterprise.

2.2.15 - Handling Controls

Table 21 - Handling Controls

Attribute Name	handlingControls
Definition/Purpose	Indicates the set of handling controls that an NPE is authorized to have.
Allowed Values	Includes values listed in the CVE for Handling Controls “CVEnumUIASHandlingControls”.
Multiplicity	Conditional: P = [0..0] NPE = [0..*]
Examples	OC, NF
Operational Usage	Ingest, Audit
Attribute Identifier	urn:us:gov:ic:uias:handlingControls

This attribute characterizes the set of handling controls that an NPE is authorized to have.

If the UIAS assertion is for a person entity, then the **@handlingControls** attribute is not exchanged as part of the attribute assertion.

2.2.16 - IC Networks

Table 22 - IC Networks

Attribute Name	icNetworks
Definition/Purpose	List of other IC networks or domains to which an entity’s digital identifier may be transmitted.
Allowed Values	Includes values listed in <i>XML Data Encoding Specification for Virtual Coverage</i> (VIRT.XML ^[42]), in the CVE “CVEnum-VIRTNetworkName”.
Multiplicity	[0..*]
Example	Allied Collaborative Shared Services (ACSS)
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:icNetworks

This attribute specifies the list of available networks or domains that an entity’s (person or non-person) digital identity may be transmitted to. An **@icNetwork** value does not presuppose which

UIAS.XML attribute values may be transmitted to other networks or domains without additional filtering.

The **@icNetworks** should be used in conjunction with the **@entitySecurityMark** attribute to determine if an entity's digital identity and approved subset of attributes should be transmitted to another network or domain.

If no values for **@icNetworks** are present, the attribute is not exchanged as part of the attribute assertion, and the entity's digital identity and approved subset of attributes will not be transmitted to another network or domain.

2.2.17 - Is IC Member

Table 23 - Is IC Member

Attribute Name	isICMember
Definition/Purpose	Reflects whether or not the entity is a member of the Intelligence Community.
Allowed Values	Boolean: 0,1,true, false
Multiplicity	[1..1]
Example	true
Operational Usage	Access
Attribute Identifier	urn:us:gov:ic:uias:isICMember

This attribute is a flag that reflects whether the entity (person or non-person) is a member of the IC as defined by Executive Order (E.O.) 12333 *Executive Order 12333 - United States Intelligence Activities, as Amended* [\[7\]](#).

This is a Boolean attribute that will be set to **"false"** by default. Where this attribute is unpopulated, its value shall be treated as **"false"**.

Each organization will make the determination as to which of its personas will have a **"true"** value for this attribute. This process will be documented by the organization and approved by the organization's senior leadership and general counsel following Executive Order 12333 [\[7\]](#), where an IC member is "a person employed by, assigned or detailed to, or acting for an element within the IC." This includes non-person entities owned by, assigned or detailed to, or acting for an element within the IC.

An **@isICMember** attribute value of **"true"** is a prerequisite for determining an entity's **@aICP** value to be **"true"**.

The **@isICMember** attribute is used for access control decisions to protected resources for both persons and non-persons.

2.2.18 - Life Cycle Status

Table 24 - Life Cycle Status

Attribute Name	lifeCycleStatus
Definition/Purpose	Indicates the life cycle phase in which the entity is operating.
Allowed Values	Includes values listed in the XML CVE for Life Cycle Status “CVCEnumUIASLifeCycleStatus”.
Multiplicity	Conditional: P = [0..0] NPE = [1..1]
Example	DEV
Operational Usage	Access, Audit, Ingest
Attribute Identifier	urn:us:gov:ic:uias:lifeCycleStatus

This attribute indicates the life cycle phase in which the entity is operating, and may be used for access control to protected resources. This attribute is only applicable for NPEs.

The **@lifeCycleStatus** attribute should be used in conjunction with the **@ATOStatus** attribute to determine the actual status of the NPE.

If the UIAS assertion is for a person entity, then the **@lifeCycleStatus** attribute is not exchanged as part of the attribute assertion.

2.2.19 - Region

Table 25 - Region

Attribute Name	region
Definition/Purpose	Indicates the individual countries or larger sub-regions such as geographical areas of combatant command Area of Responsibility (AOR)s, Area of Interest (AOI)s or State and Non-State Actor(s).
Allowed Values	Includes values listed in <i>XML CVE Encoding Specification for Mission Need</i> (MN.CES ^[31]), in the CVE “CVCEnumMNRegion”.
Multiplicity	[0..*]
Examples	ANAN, AFce, AFea, ASea, EUce
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:region

This attribute specifies the entity's (person or non-person) need-to-know for access to protected resources, such as individual countries or larger sub-regions such as geographical areas of combatant command, AORs, AOIs, or State and Non-State Actor(s).

The **@region** attribute is used for access control decisions to protected resources. If the entity does not have any values listed for the **@region** attribute, then the attribute is not exchanged as part of the assertion. If the entity does have a value listed for the **@region** attribute, then there MUST be at least 2 values, one of which MUST be ANAN.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.2.20 - Role

Table 26 - Role

Attribute Name	role
Definition/Purpose	Indicates the position, job or area of responsibility associated with the entity.
Allowed Values	The allowed values follow the Namespace Taxonomies are defined in <i>CVE Encoding Specification for Role</i> (ROLE.CES ^[37])
Multiplicity	[0..*]
Examples	C2S-CIA-Ent-CIO-NETADMIN, C2S-NSA-Msn-MissionA-READONLY, Nebula-CIA-Proxy, ENT-FBI-ALEP
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:role

This attribute characterizes 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.

The **@role** attribute is used for access control decisions to protected resources. If the entity does not have any values listed for the **@role** attribute, then the attribute is not exchanged as part of the attribute assertion.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.2.21 - Topic

Table 27 - Topic

Attribute Name	topic
Definition/Purpose	Indicates the particular intelligence subject area.

Attribute Name	topic
Allowed Values	Includes values listed in MN.CES ^[31] , in the CVE “CVEnumMNIssue”.
Multiplicity	[0..*]
Examples	ANY, HREL, HLTH, Common Name (CN), DI, IC
Operational Usage	Access, Discovery, Ingest
Attribute Identifier	urn:us:gov:ic:uias:topic

This attribute specifies the entity’s (person or non-person) need-to-know for access to protected resources, such as particular intelligence subject area.

The `@topic` attribute is used for access control decisions to protected resources. If the entity does not have any values listed for the `@topic` attribute, then the attribute is not exchanged as part of the attribute assertion. If the entity does have a value listed for the `@topic` attribute, then there MUST be at least 2 values, one of which MUST be ANY.

It is the responsibility of the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.

2.3 - IC Enterprise Environment Attribute Names and Values

The attributes, as defined in this section, represent the set of IC enterprise environment attributes and associated values that may or may not be supported by an AS participating in the IC’s UAAS capability. These attributes may be derived at runtime, and not stored by an AS.

2.3.1 - Certificate Authority

Table 28 - Certificate Authority

Attribute Name	certificateAuthority
Definition/Purpose	Reflects the issuing PKI certificate authority for the entity.
Allowed Values	ICPKI, CADPKI Values listed in the XML CVE for Certificate Authority “CVEnumUIASCertificateAuthority”.
Multiplicity	[0..1]
Example	ICPKI, CADPKI
Operational Usage	Access, Audit
Attribute Identifier	urn:us:gov:ic:uias:certificateAuthority

This provides broader and more explicit support for entities (persons and non-persons) of different Certificate Authority (CA)s including the support of policies requiring discrimination of 2PI (or US operating under 2PI constraints) and US users. By allowing Cryptologic Agencies Domain (CAD)

PKI entities (persons and non-persons) access to Intelligence Community Information Technology Enterprise (IC ITE) resources on Joint Worldwide Intelligence Communications System (JWICS), information resources need to recognize this certificate authority distinctly to enforce the appropriate access controls. This will become more important as the use of trust chains broadens to give more system components support beyond IC PKI.

2.3.2 - Originating Network

Table 29 - Originating Network

Attribute Name	originatingNetwork
Definition/Purpose	Reflects the network or domain that the entity's identity originates from.
Allowed Values	Includes values listed in VIRT.XML ^[42] , in the CVE "CVEEnumVIRTNetworkName".
Multiplicity	[0..1]
Examples	NSANET
Operational Usage	Access, Audit, Discovery
Attribute Identifier	urn:us:gov:ic:uias:originatingNetwork

This attribute indicates which network an entity (person and non-person) originates from. Security protections and accreditations vary across environments, especially with regard to foreign nationals and 2PIs sitting within those environments. By allowing 2PIs to access resources on JWICS information resources need to recognize the originating network to enforce the appropriate access controls.

Chapter 3 - Constraints

3.1 - Data Validation Constraint Rules

The UIAS.XML schema defines the data elements, attributes, cardinalities and parent-child relationships for which XML 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^[15] framework document.

3.1.1 - Value Enumeration Constraints

Several elements and attributes of the UIAS.XML 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 in the constraint rules since the excluded values would be excluded from use on the lower network.

Developers of systems processing SCI or SAP from the unpublished Register will need to contact the POC listed in [Appendix F - 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.

3.1.2 - Additional Constraints

3.1.2.1 - DES Constraints

The Data Encoding Specification (DES) version is specified through attributes on an element. The schema constrains the values of these attributes. The `@DESVersion` attribute enables systems processing an instance document to be certain which set of constraint rules, schema, CVEs and business rules are intended by the author to be used.

3.1.3 - Constraint Rules

The detailed constraint rules for the UIAS.XML schema can be found in a separate document inside the Schematron/UIAS directory, in the “UIAS_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 “UIAS_Rules.pdf” file.

3.2 - Data Rendering Constraint Rules

3.2.1 - Purpose

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

Table 30 - 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 UIAS.XML. 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 Markings^[12] has an implementation date of one year after issuance).

Table 31 - 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. UIAS.XML Feature Comparison

A.1.1. Features from V2018-APR to V2021-NOV

Table 32 - UIAS.XML Feature Comparison V2018-APR to V2021-NOV

Required date	Feature	V2018-APR	V2018-APRr2018-NOV	V2019-SEP	V2021-NOV
	@countryOfAffiliation uses ISMCAT.CES ^[30]	F	F	N/A	N/A
	Use ISMCAT.CES ^[30] for country codes and tetragraphs	F	F	N/A	N/A
Sep 2019	@countryOfAffiliation uses IC-GENC.CES ^[14]	N	N	F	F
	Added rule to check that every SCI token in Fine Access Controls with a "-" also has the token with out the last "-xxx".	N	N	F	F
Nov 2021	Addition of ALEP Role to ROLE Attribute	N	N	N	F
	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE	N	N	N	F
	Add two new dissemination controls to UIAS handlingControls CVE.	N	N	N	F
	Incorporate DOD Special Access Program Control Office (SAPCO) guidance on SAPs	N	N	N	F
	Extract ROLE from UIAS to become a standalone CVE again.	N	N	N	F
	Federating ANAN and ANY values for Topic and Region Attributes.	N	N	N	F

Required date	Feature	V2018-APR	V2018-APRr2018-NOV	V2019-SEP	V2021-NOV
	Modify UAAS Diagram in DES to bring it up-to-date	N	N	N	F
	Changed RAW-FISA to RAWFISA	N	N	N	F

A.1.1.1. Features Partial and N/A from V2018-APR to V2021-NOV

Table 33 - UIAS.XML Feature Comparison V2018-APR to V2021-NOV

Required date	Feature	V2018-APR	V2018-APRr2018-NOV	V2019-SEP	V2021-NOV
	@countryOfAffiliation uses ISMCAT.CES ^[30]	F	F	N/A	N/A
	Use ISMCAT.CES ^[30] for country codes and tetragraphs	F	F	N/A	N/A

A.1.2. Features from V2015-AUG to V2018-APR

Table 34 - UIAS.XML Feature Comparison V2015-AUG to V2018-APR

Required date	Feature	V2015-AUG	V2016-SEP	V2016-SEPr2017-JUL	V2018-APR
	Reference @authorityCategory and @fineAccessControl	F	F	F	N
	@countryOfAffiliation uses ISMCAT.CES ^[30]	N	F	F	F
	Support for @dutyOrganizationUnit	N	F	F	F
	Support for @handlingControls	N	F	F	F
	Schematron Rules	N	F	F	F
	XSD Schema	N	F	F	F
	Support for @auditRoutingOrganization	N	F	F	F
	Use ISMCAT.CES ^[30] for country codes and tetragraphs	N	F	F	F
Dec 2017	Align with 2016-DEC IC Marking System Register and Manual.	N	N	F	F
	CSV and JSON CVE formats	N	N	F	F
Nov 2018	Add allowed value reference for @entitySecurityMark	N	N	N	F
	RelaxNG xml and compact formats	N	N	N	F
	Support for 2 new Handling Controls	N	N	N	F

A.1.3. Features from V3 to V2015-AUG

Table 35 - UIAS.XML Feature Comparison V3 to V2015-AUG

Required date	Feature	V3	V3.1	V2014-DEC	V2015-AUG
	Reference @authorityCategory and @fineAccessControl	N	F	F	F
	Reference @role	N	N	F	F
	Second-party Integree	N	N	F	F
	Clarified definition of GOV in support of State, Local, and Tribal Governments (SLT)	N	N	F	F
	Environment Attributes	N	N	F	F
	Support for @Group	N	N	N	F
	Support for Attribute IDs Uniform Resource Name (URN)	N	N	N	F
	Updated allowed value reference for @region	N	N	N	F
	Updated allowed value reference for @topic	N	N	N	F
	@originatingNetwork uses VIRT.XML ^[42]	N	N	N	F
	@icNetworks uses VIRT.XML ^[42]	N	N	N	F

A.1.4. Features from V1 to V3

Table 36 - UIAS.XML Feature Comparison V1 to V3

Required date	Feature	V1	V2	V2.1	V3
	Non-Person Entities	N	F	F	F
	ICAM	N	N	F	F
Dec 2013	Five-Eyes Enterprise (5EE) Safeguarding Initiatives	N	N	N	F

Appendix B Change History

[Table 37](#) summarizes the version identifier history for this technical specification.

Table 37 - Identifier History

Version	Date	Purpose
1	December 14, 2011	Initial Release
2	July 17, 2012	Updated to incorporate required attributes for Non-Person Entities and IC Smart Data in support of the IC ITE
2.1	August 16, 2013	Updated controlled vocabularies and definitions in support of the IC ITE ICAM Service Provider
3	September 3, 2013	Updated to include @entitySecurityMark and @icNetworks in support of 5EE Safeguarding Initiatives
3.1	March 14, 2014	Updated controlled vocabulary pointers for @authorityCategory and @fineAccessControl ; clarified operational usage
2014-DEC	December 22, 2014	Updated controlled vocabulary pointers for role ; reassigned NATO from @clearance to @fineAccessControl ; Support 2PI; Remove 'US federal' from GOV definition in @entityType ; added two new attributes: @certificateAuthority , @originatingNetwork
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see Section B.7 - V2015-AUG Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.6 - V2016-SEP Change Summary
2016-SEPr2017-JUL	July 21, 2017	Routine revision to technical specification. For details of changes, see Section B.5 - V2016-SEPr2017-JUL Change Summary
2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see Section B.4 - V2018-APR Change Summary
2018-APRr2018-NOV	November 26, 2018	Routine revision to technical specification. For details of changes, see Section B.3 - V2018-APRr2018-NOV Change Summary

Version	Date	Purpose
2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see Section B.2 - V2019-SEP Change Summary
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:

- Technical Integration Committee Next Generation (TIC NG)
- IC Marking System Register and Manual 30 August 2019^[1]
- Community Change Requests

[Table 38](#) summarizes the changes made to this technical specification from version 2019-SEP to version 2021-NOV.

Table 38 - Data Encoding Specification V2021-NOV Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Addition of ALEP Role to ROLE Attribute. (CR-2019-013)	Documentation Schematron UIAS-ID-00069 added	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. ICAM systems and software services need to be updated to accommodate the changes.
2	Change format of UIAS foreign partner organizations to match IC-SEA and 5EE (CR-2019-003)	Documentation Schema Schematron UIAS-ID-00053 modified	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. ICAM systems and software services need to be updated to accommodate the changes.

#	Change	Artifacts changed	Compatibility Notes
3	Extract ROLE from UIAS to become a standalone CVE again. (CR-2019-054)	Documentation CVE CVerenum-UIASC2SFunction deleted CVerenumUIASC2SScope deleted CVerenum-UIASNebulaNamedRole deleted CVerenum-UIASPAASFunction deleted CVerenum-UIASPAASScope deleted CVerenum-UIASRoleNamespace deleted Schematron UIAS-ID-00007 modified UIAS-ID-00050 modified UIAS-ID-00070 added	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Corrected sub-compartment to subcompartment. (CR-2019-164).	Documentation	No impact to systems.
5	Federating ANAN and ANY values for Topic and Region attributes. (CR-2019-141).	Documentation Schematron UIAS-ID-00071 added UIAS-ID-00072 added	Data generation and ingestion systems need to be updated to accommodate the changes.

#	Change	Artifacts changed	Compatibility Notes
6	Changed RAW-FISA to RAWFISA. (CR-2020-031).	Documentation CVE CVerenum-UIASHandlingControls modified	Data generation and ingestion systems need to be updated to accommodate the changes.
7	Added DESVersion warning enforcement rules (CR-2021-001)	Schematron UIAS-ID-00073 added UIAS-ID-00074 added UIAS-ID-00075 added UIAS-ID-00076 added UIAS-ID-00077 added UIAS-ID-00078 added UIAS-ID-00079 added	No impact to systems.
8	Add UCNI and DCNI to UIAS CVE for handlingControls (CR-2021-006)	Documentation CVE CVerenum-UIASHandlingControls.xml added	Data generation and ingestion systems need to be updated to accommodate the changes.
9	Modify handling of SAP accesses to support DOD SAPCO rules. (CR-2021-024)	Documentation Schematron UIAS-ID-00080 added UIAS-ID-00081 added	Systems need to be updated to accommodate this change
10	Removed the ACSS PKIC from the UIAS CVE (CR-2021-021)	Documentation CVE CVerenum-UIASCertificateAuthority	Systems need to be updated to accommodate this change
11	Revised UAAS Diagram in DES to add CASPORT (CR-2021-023)	Documentation Diagram 3	Systems need to be updated to accommodate this change

B.2 - V2019-SEP Change Summary

Significant drivers for version 2019-SEP include:

- TIC NG
- Community Change Requests

[Table 39](#) summarizes the changes made to this technical specification from version 2018-APRr2018-NOV to version 2019-SEP.

Table 39 - Data Encoding Specification V2019-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated documentation to use the specification framework. Removed the Dependency Over Time table. (CR-2019-042)	Documentation	No impact to systems.
2	Updated multiplicity to match UML format. (CR-2019-050)	Documentation	No impact to systems.
3	Added rule to check that every SCI token in Fine Access Controls with a "-" also has the token without the last "-xxx". (CR-2019-065)	Schematron UIAS-ID-00068 added UIAS_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Changed countryOfAffiliation to use IC-GENC country codes. (CR-2018-132)	Documentation Schema	Minimal impact to systems. Same tokens, new isolated source.
5	Updated auditRoutingOrganization multiplicity and values. (CR-2018-140)	Documentation	No impact to systems.
6	Identify the lack of a root node in the Schema Guide. (CR-2019-110)	Documentation	No impact to systems.

B.3 - V2018-APRr2018-NOV Change Summary

Significant drivers for Version 2018-APRr2018-NOV include:

- Community Change Requests

[Table 40](#) summarizes the changes made to this technical specification from Version 2018-APR to Version 2018-APRr2018-NOV.

Table 40 - V2018-APRr2018-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Update HandlingControls CVE for 2 new dissemination controls. (CR-2018-135)	CVE	Data generation and ingestion systems need to be updated to accommodate the changes to Dissemination controls.
2	Update UIAS Allowed Values for ATOSStatus, isICMember and aICP to align with Schema 0,1, true, false. (CR-2018-129)	Documentation updated	Systems using Schema valid values need not change.
3	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.
4	Correct schema for DESVersion (CR-2018-145)	Schema	Systems using revisions in DESVersion will properly function.
5	Correct definition for @entitySecurityMark to reference the digital identity vs digital identifier. (CR-2018-138)	Documentation updated	Systems who used @entitySecurityMark only for the identifier and not the entire identity may need to be updated.

B.4 - V2018-APR Change Summary

Significant drivers for Version 2018-APR include:

- Community Change Requests

[Table 41](#) summarizes the changes made to this technical specification from Version 2016-SEPr2017-JUL to Version 2018-APR.

Table 41 - V2018-APR Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Create CVEUIASSecurityMarkType CVE and updated entitySecurityMark to be restricted to the values of the CVE. (CR-2017-017)	Schema CVE CVEnum-sUIASSecurityMark-Type.xml	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Create RelaxNG CVE Fragments for UIAS. (CR-2017-187)	CVEs	No impact to systems.

#	Change	Artifacts Changed	Compatibility Notes
3	Added DESVersion warning enforcement rule and updated schema version restriction to align with version and revision strategy. Added Revision Constraints section to DES. (CR-2017-096)	Documentation Schema Schematron UIAS-ID-00067 added UIAS_XML.sch modified	Data generation and ingestion systems need to be updated to accommodate the changes.
4	Remove FAC from UIAS to allow the addition as many formerly unpublished register values to FAC as possible. (CR-2017-143)	Controlled Vocabulary Enumeration Encoding Specification (CES) CVE FAC	Data generation and ingestion systems need to be updated to use the modified version string.
5	Remove AUTHCAT from UIAS to allow it to update faster as needed for the new NTK profile that uses AUTHCAT. (CR-2016-005), (CR-2017-159)	CES CVE AUTHCAT	Data generation and ingestion systems need to be updated to use the modified version string.
6	Modified cardinality rendering. (CR-2016-078)	CVEs	No impact to existing systems, documentation rendering change only.
7	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.
8	Added schema PDF. (CR-2018-032)	Documentation	No impact to systems.
9	Added ISM.XML ^[29] attributes to Schematron files to mark up the documentation. (CR-2017-317)	Schematron	No impact to systems.
10	Updated dependency over time table to more accurately represent the specifications involved. (CR-2017-283)	Documentation	No impact to systems.
11	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.

#	Change	Artifacts Changed	Compatibility Notes
12	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.5 - V2016-SEPr2017-JUL Change Summary

Significant drivers for Version 2016-SEPr2017-JUL include:

- Community Change Requests
- Alignment with December 2016 IC Marking System Register and Manual^[13]

[Table 42](#) summarizes the changes made to this technical specification from Version 2016-SEP to Version 2016-SEPr2017-JUL.

Table 42 - V2016-SEPr2017-JUL Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Moving ECRU and NONBOOK as subcompartments under SI and handling the removal of ENDSEAL (CR-2015-097)	CVEs CVEUIASFineAccessControl.xml modified CVEnum-sUIASFineAccessControl.xml modified	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Added inverse dependency section and definitions for Dependencies and Inverse Dependencies. (CR-2017-125)	Documentation	No impact to systems.
3	Create JSON version of CVEs in ISM (CR-2017-068)	CVEs	No impact to systems.
4	Create CSV version of CVEs in ISM (CR-2017-046)	CVEs	No impact to systems.
5	Added @id and @role to all sch:rule elements, in support of commercial tools warnings and errors and to support open source unit testing frameworks. (CR-2017-216)	All non-abstract Schematron rules modified	No impact to existing systems. Additional capabilities.
6	Update the version numbering prose to reflect the existence of Revisions. (CR-2017-237)	Documentation	No impact to systems.

#	Change	Artifacts Changed	Compatibility Notes
7	Remove UIAS orphan abstract rule file, TypeConstraintPatterns.sch, since it is not referenced by any rules. (CR-2017-261)	Schematron TypeConstraintPatterns removed.	No impact to systems.
8	Modified cardinality rendering. (CR-2016-078)	CVEs	No impact to existing systems, documentation rendering change only.

B.6 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests

[Table 43](#) summarizes the changes made to this technical specification from Version 2015-AUG to Version 2016-SEP.

Table 43 - V2016-SEP Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Updated @countryOfAffiliation (CR-2015-102)	DES Schema Schematron UIAS-ID-00065 added.	CVE updated to reference ISMCAT ^[30] "CVerenum-ISMCAATResponsibleEntity"
2	Added @dutyOrganizationUnit (CR-2015-071)	DES Schema	Added new attribute
3	Added @handlingControls (CR-2015-037)	CVE CVerenum-UIASHandlingControls Schema DES	Added new attribute

#	Change	Artifacts Changed	Compatibility Notes
4	Added Schematron rules (CR-2015-034)	Schematron added UIAS-ID-00001 added. UIAS-ID-00004 added. UIAS-ID-00005 added. UIAS-ID-00006 added. UIAS-ID-00007 added. UIAS-ID-00008 added. UIAS-ID-00009 added. UIAS-ID-00011 added. UIAS-ID-00012 added. UIAS-ID-00014 added. UIAS-ID-00016 added. UIAS-ID-00019 added. UIAS-ID-00021 added. UIAS-ID-00022 added. UIAS-ID-00023 added. UIAS-ID-00024 added. UIAS-ID-00025 added. UIAS-ID-00026 added. UIAS-ID-00028 added. UIAS-ID-00030 added. UIAS-ID-00036 added. UIAS-ID-00047 added. UIAS-ID-00050 added. UIAS-ID-00051 added. UIAS-ID-00052 added.	Systems implementing UIAS MUST exchange information valid to the Schematron.

#	Change	Artifacts Changed	Compatibility Notes
		UIAS-ID-00053 added. UIAS-ID-00056 added. UIAS-ID-00057 added. UIAS-ID-00065 added. UIAS-ID-00066 added.	
5	Added schema (CR-2015-034, CR-2016-016)	UIAS XSD Schema added	Systems implementing UIAS MUST exchange information valid to the schema.
6	Added PAAS to CVEnum-UIASRoleNamespace and created CVEnumUIASPAASScope, CVEnumUIASPAASFunction (CR-2015-110)	CVE CVEnum-UIASRoleNamespace updated. CVEnumUIASPAASScope added. CVEnumUIASPAASFunction added.	CVE value added and new CVEs created.
7	Added @auditRoutingOrganization (CR-2016-001, CR-2016-014)	DES Schema	Added new required attribute
8	Incorporated ROLE and AUTHCAT CVEs into UIAS (CR-2016-013)	CVE CVEnum-UIASAuthorityCategory added CVEnum-UIASRoleNamespace added	CVEs are now internal to UIAS

#	Change	Artifacts Changed	Compatibility Notes
9	Added Clearance, CertificateAuthority, EntityType, Non-Person EntityType, FineAccessControls, and LifecycleStatus CVEs into UIAS (CR-2015-015, CR-2015-016, CR-2015-034)	CVE CVEnum-UIASCertificateAuthority added CVEnumUIASClearance added CVEnumUIASEntityType-added CVEnum-UIASFineAccessControl added CVEnum-UIASLifecycleStatus added CVEnum-UIASNonPersonEntityType added CVEnum-UIASPersonEntityType-added	CVEs internal to UIAS now control corresponding attribute values.
10	Updated schema to make all Elements begin with capital letters to be consistent with Naming and Design Rules (CR-2015-034, CR-2016-016)	Schema	Systems need to be updated to accommodate this change.
11	Updated CVE to reflect removal of KDK and the moving of its subcompartments under TK (CR-2016-024)	CVE CVEnum-UIASFineAccessControl updated	Systems need to be updated to accommodate this change.
12	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.7 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests

- Alignment with standalone CVE specifications

[Table 44](#) summarizes the changes made to this technical specification from Version 2014-DEC to Version 2015-AUG.

Table 44 - V2015-AUG Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Added @group	@group	Added new attribute
2	Added attribute ID	DES	Added Attribute ID URN for all attributes
3	Updated @region	@region	CVE updated to reference MN.CES ^[31] CEnumMNRegion
4	Updated @topic	@topic	CVE updated to reference MN.CES ^[31] CEnumMNIssue
5	Updated @originatingNetwork	@originatingNetwork	CVE updated to reference VIRT.XML ^[42] .
6	Updated @icNetworks	@icNetworks	CVE updated to reference VIRT.XML ^[42] .

B.8 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Clarified definition of GOV in support of SLT
- Add CVE for @role
- Move NATO to CVE FAC
- Add support for 2PI
- Added Authoritative Attribute Source for specific attributes

[Table 45](#) summarizes the changes made to this technical specification from Version 3.1 to Version 2014-DEC.

Table 45 - V2014-DEC Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Implemented new versioning scheme.	DES	Changed versioning scheme from version number (e.g., V3) to version YYYY-MMM (e.g, 2014-DEC).
2	Updated @role.	@role	CVE for @role values added.

#	Change	Artifacts Changed	Compatibility Notes
3	Updated attribute @clearance.	@clearance	Remove NATO from attribute @clearance.
4	Updated @adminOrganization.	@adminOrganization	Added support for 2PI.
5	Updated @entityType.	@entityType	Removed 'US federal' in definition of GOV in entityType.
6	Added new attribute @certificateAuthority.	@certificateAuthority	Added new environment attribute.
7	Added new attribute @originatingNetwork.	@originatingNetwork	Added new environment attribute.

B.9 - V3.1 Change Summary

Significant drivers for Version 3.1 include:

- Add CVEs for @authorityCategory and @fineAccessControl

[Table 46](#) summarizes the changes made to this technical specification from Version 3 to Version 3.1.

Table 46 - V3.1 Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Updated @authorityCategory.	@authorityCategory	Updated CVE.
2	Updated @clearance.	@clearance	Clarified definition.
3	Updated @fineAccessControl.	@fineAccessControl	Updated CVE.
4	Updated @icNetworks.	@icNetworks	Updated CVE.

B.10 - V3 Change Summary

Significant drivers for Version 3 include:

- Provide for safeguards

[Table 47](#) summarizes the changes made to this technical specification from Version 2.1 to Version 3.

Table 47 - V3 Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Added new attribute.	@entitySecurityMark	Added new attribute.

#	Change	Artifacts Changed	Compatibility Notes
2	Added new attribute.	@icNetworks	Added new attribute.

B.11 - V2.1 Change Summary

Significant drivers for Version 2.1 include:

- Provide updated CVEs for @adminOrganization and @dutyOrganization

[Table 48](#) summarizes the changes made to this technical specification from Version 2 to Version 2.1.

Table 48 - V2.1 Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Updated @adminOrganization.	@adminOrganization	Updated CVE and clarified definition.
2	Updated @authorityCategory.	@authorityCategory	Clarified definition.
3	Updated @ATOSStatus.	@ATOSStatus	Clarified definition.
4	Updated @clearance.	@clearance	Clarified definition.
5	Updated @dutyOrganization.	@dutyOrganization	Updated CVE and clarified definition.
6	Updated @entityType.	@entityType	Clarified definition.
7	Updated @lifeCycleStatus.	@lifeCycleStatus	Clarified definition.
8	Updated @region.	@region	Clarified definition.
9	Updated @role.	@role	Clarified definition.
10	Updated @topic.	@topic	Clarified definition.

B.12 - V2 Change Summary

Significant drivers for Version 2 include:

- The addition of attributes to provide Fine-Grain Access Control

[Table 49](#) summarizes the changes made to this technical specification from to Version 1 to Version 2.

Table 49 - V2 Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Added new attribute.	@adminOrganization	Added new attribute.
2	None	@aICP	No change.

#	Change	Artifacts Changed	Compatibility Notes
3	Added new attribute.	@ATOSStatus	Added new attribute.
4	Added new attribute.	@authorityCategory	Added new attribute.
5	Updated @clearance.	@clearance	Updated definition to include NPEs, NATO and DoE clearances.
6	Updated @countryOfAffiliation.	@countryOfAffiliation	Updated attribute name and definition to apply to NPEs.
7	Updated @digitalIdentifier.	@digitalIdentifier	Updated DistinguishedName attribute name and definition to apply to NPEs.
8	Updated @dutyOrganization.	@dutyOrganization	Updated Organization attribute name and definition to apply to NPEs.
9	Updated @entityType.	@entityType	Updated Employee Type attribute name and definition to apply to NPEs.
10	Updated @fineAccessControls.	@fineAccessControls	Updated sciControls attribute name and definition to apply to NPEs.
11	Updated @isICMember.	@isICMember	Updated definition to include NPEs.
12	Added new attribute.	@lifeCycleStatus	Added new attribute.
13	Added new attribute.	@region	Added new attribute.
14	Added new attribute.	@role	Added new attribute.
15	Added new attribute.	@topic	Added new attribute.

Appendix C Glossary

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

ANAN	<p>A token in the <code>@mn:region</code> attribute as listed in “CVCEnumMNRegion”. 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.</p> <p>On a resource when "ANAN" is selected, it is the most permissive while still requiring some provisioning of "any" region.</p> <p>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.</p>
ANY	<p>A token in the <code>@mn:issue</code> attribute as listed in “CVCEnumMNIssue”. 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.</p> <p>On a resource when "ANY" is selected, it is the most permissive while still requiring some provisioning of "any" issue.</p> <p>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.</p>
attribute	<p>A distinct characteristic of an object. In the context of ICAM standards for PE and NPE entities, an attribute captures characteristics of PEs and NPEs.</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> [27].</p>
Attribute Practice Statement (APS)	<p>A document stating the operational guidelines and practices to which an owning organization agrees to adhere to, assuring the quality and level of service for each IC AAS and IC AS provided (Based on NIST SP 800-205 Attribute Considerations for Access Control Systems).</p>

	Source: NIST SP 800-205, <i>Attribute Considerations for Access Control Systems</i> [33] .
Attribute Service (AS)	<p>A service that provides a common access point to accurate and current attributes obtained from one or more AAS.</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> [27].</p>
Authoritative Attribute Source (AAS)	<p>The official source that originates and maintains the attributes of entities.</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> [27].</p>
audit	<ol style="list-style-type: none"> 1. Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. <p>Source: Committee on National Security Systems Instruction (CNSSI) 4009, <i>National Information Assurance (IA) Glossary</i> [4].</p> <ol style="list-style-type: none"> 2. Provides authorized personnel with the ability to review and examine any action that can potentially cause access to, generation of, or affect the release of classified or sensitive information. <p>Source: Intelligence Community Standard (ICS) 500-27, <i>Intelligence Community Standard for Collection and Sharing of Audit Data</i> [25]</p>
Distinguished Name (DN)	<p>A unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service.</p> <p>Source: CNSS Instruction 4009, <i>National Information Assurance (IA) Glossary</i> [4].</p>
Entity	<p>An individual (person), organization, device, or process.</p> <p>Source: NIST 800-56Br1, <i>Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1</i> [32].</p>
Non-Person Entity (NPE)	Entity related to Information Technology (IT), e.g., hardware objects (physical entities/devices) and software objects (virtual/logical entities).

Source: ICS 500-30, *Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources* [\[27\]](#).

Person Entity (PE)

A human Entity that is the Owner of a PKI certificate (NIST SP 800-56Br1). A human entity that is the Name or Role Subscriber in a PKI certificate (CNSSI 1300).

Source: NIST SP 800-56Br1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1* [\[32\]](#).

Source: CNSSI 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25* [\[3\]](#)

Second Party Integree

Second Party Integree means:

1. A Second Party citizen who is employed by a Second Party Government who works in support of a USG objective at a USG organization, under the supervision and direction of USG personnel within a USG facility or Second Party facility with a co-utilization agreement
2. A Second Party citizen who works under a USG contract, in support of a USG objective at a USG organization, under the supervision and direction of USG personnel within a USG facility or Second Party facility with a co-utilization agreement.

Individuals who act on behalf of a Second Party in a representational capacity are not Second Party Integrees.

Sources:

1. DNI Executive Correspondence 2016-00816, *Second Party Integree Access to the IC Information Environment* [\[6\]](#).

Appendix D List of Abbreviations

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

2PI	Second Party Integree
2PS	Second Party Sovereign
5EE	Five-Eyes Enterprise
AAS	Authoritative Attribute Source
ABAC	Attribute Based Access Control
ACSS	Allied Collaborative Shared Services
AEA	Atomic Energy Act
AICP	Authorized IC Person
AOI	Area of Interest
AOR	Area of Responsibility
APCS	Attribute Practice Compliance Statement
APS	Attribute Practice Statement
AS	Attribute Service
ATO	Authority To Operate
CA	Certificate Authority
CAD	Cryptologic Agencies Domain
CES	Controlled Vocabulary Enumeration Encoding Specification
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CN	Common Name
CNWDI	Critical Nuclear Weapons Design Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DI	Digital Identifier
DIAS	DoDIIS Identity and Authorization Services

DN	Distinguished Name
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
E.O.	Executive Order
ESB	Enterprise Standards Baseline
FAC	Fine Access Control
FSD	Full Service Directory
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
IC ITE	Intelligence Community Information Technology Enterprise
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JWICS	Joint Worldwide Intelligence Communications System
NATO	North Atlantic Treaty Organization
NPE	Non-Person Entity
NSA	National Security Agency
NSI	National Security Information
OMG	Object Management Group
PE	Person Entity
PKI	Public Key Infrastructure
POC	Point of Contact

SAML	Security Assertion Markup Language
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SCI	Sensitive Compartmented Information
SLT	State, Local, and Tribal Governments
TBD	To Be Determined
TIC NG	Technical Integration Committee Next Generation
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
X.509	ITU-T standard for public key infrastructures
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformations

Appendix E Bibliography

[1] AATT CONOPS

Department of Defense / Intelligence Community. *Unified Authorization and Attribute Service, Concept of Operations*. Version 1.11. 8 December 2008.

Available online Intelink-TS at: <https://go.ic.gov/un85ruo> (case sensitive – uniform november 8 5 romeo uniform oscar)

[2] AUTHCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Authority Category (AUTHCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/JIMIYN5> (case sensitive – Juliet India Mike lima Yankee November 5)

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

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

[3] CNSSI 1300

Committee on National Security Systems. *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25*. 1300. December 2014.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[4] CNSSI 4009

Committee on National Security Systems. *National Information Assurance (IA) Glossary*. 4009. 6 April 2015.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[5] 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>

[6] ES 2016-00816

ODNI. *Second Party Integree Access to the IC Information Environment*. ES 2016-00816. 30 December 2016.

[7] E.O. 12333

The White House. *Executive Order 12333 - United States Intelligence Activities, as Amended*. Federal Register, Vol. 46, No. 235. 4 December 1981.

Available online at: <http://www.archives.gov/federal-register/codification/executive-order/12333.html>

[8] FAC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Fine Access Control (FAC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/uZz5l7T> (case sensitive – uniform Zulu zulu 5 India 7 Tango)

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

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

[9] HSPD-12

Office of Management and Budget. *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*.

Available online at: <https://www.dhs.gov/homeland-security-presidential-directive-12>

[10] 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.

[11] IC Markings AUG 2019

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 30 Aug 2019.

Available online Intelink-TS at: <https://go.ic.gov/gbMr5fv> (case sensitive – golf bravo Mike romeo 5 foxtrot victor)

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

[12] 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>

[13] IC Markings DEC 2016

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2016.

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>

[14] IC-GENC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Geopolitical Entities, Names, and Codes (IC-GENC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/Tuxrlnu> (case sensitive – Tango uniform xray romeo India november uniform)

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

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

[15] 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>

[16] ICD 121

Office of the Director of National Intelligence. *Managing the Intelligence Community Information Environment*. Intelligence Community Directive 121. 19 January 2017.
Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20206.pdf>

[17] 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

[18] 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

[19] ICD 503

Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management*. Intelligence Community Directive 503. 21 July 2015.
Available online Intelink-TS at: <https://go.ic.gov/Ru5XGc9> (case sensitive – Romeo uniform 5 Xray Golf charlie 9)
Available online at: <http://www.dni.gov/files/documents/ICD/ICD503.pdf>

[20] 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

[21] 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)

[22] 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

[23] ICPG 704.5

Deputy Directory of National Intelligence for Policy, Plans and Requirements. *IC Personnel Security Database Scattered Castle*. Intelligence Community Policy Guidance 704.5. 25 February 2020.

Available online Intelink-TS at: <https://go.ic.gov/MT7zPzY> (case sensitive – Mike Tango 7 zulu Papa zulu Yankee)

Available online at: https://www.dni.gov/files/documents/ICPG/02-25-20_ODNI_ICPG_IC_Personnel_Security_Database_Scattered_Castles_20-00078_U.pdf

[24] 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>

[25] ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <https://go.ic.gov/Jznuy0x> (case sensitive – Juliet zulu november uniform yankee 0 xray)

[26] 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)

[27] 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)

[28] ISO 11179-3

International Organization for Standardization (ISO). *ISO/IEC 11179, Information Technology -- Metadata registries (MDR), Part 3: Registry metamodel and basic attributes*.

Available online at: <https://www.iso.org/standard/50340.html>

[29] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)

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

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

[30] ISMCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/mL5WA9> (case sensitive – mike Lima Foxtrot 5 Whiskey Alpha 9)

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

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

[31] MN.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Mission Need (MN.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/ndd7V1R> (case sensitive – november delta delta 7 Victor 1 Romeo)

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

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

[32] NIST 800-56Br1

National Institute of Standards and Technology. *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. Revision 1. September 2014.

Available online at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf>

[33] NIST SP 800-205

National Institute of Standards and Technology. *Attribute Considerations for Access Control Systems*. Special Publication 800-205. June 2019.

Available online at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf>

[34] OMB Memo M-11-11

Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

Available online at: <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>

[35] OMB Memo M-19-17

Enabling Mission Delivery through Improved Identity, Credential, and Access Management.

Available online at: <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>

[36] Public Law 80-242

Secretary of the Interior. *Public Law 242-80th Congress*. 1947-07-25.

Available online at: https://geonames.usgs.gov/docs/pubs/Public_Law_242.pdf

[37] ROLE.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Role (ROLE.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/GknYELv> (case sensitive – Golf kilo november Yankee Echo Lima victor)

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

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

[38] SAML 2.0 Attribute Sharing

OASIS Security Services Technical Committee. *SAML 2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, [Encrypted Mode]*. 27 March 2008.

Available online at: <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.html>

[39] 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/>

[40] UML

Object Management Group (OMG). *Unified Modeling Language*. 6 December 2017.

Available online at: <https://www.omg.org/spec/UML/2.5.1/PDF/changebar>

[41] 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>

[42] VIRT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Virtual Coverage (VIRT.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/BljGxq> (case sensitive – Bravo India lima juliet Golf xray quebec)

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

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

[43] 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 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 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^[24].