



# **Intelligence Community Technical Specification**

---

## **Attribute Practice Compliance Statements for the 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  |
| 1.5 - Dependencies .....                                       | 3  |
| 1.5.1 - Specification Dependencies .....                       | 4  |
| 1.5.2 - Inverse Dependencies .....                             | 5  |
| Chapter 2 - Development Guidance .....                         | 6  |
| 2.1 - UIAS Compliance Statements .....                         | 6  |
| 2.1.1 - Admin Organization .....                               | 6  |
| 2.1.1.1 - Person Entity (PE) Compliance Statements .....       | 6  |
| 2.1.1.2 - Non-Person Entity (NPE) Compliance Statements .....  | 6  |
| 2.1.2 - Audit Routing Organization .....                       | 6  |
| 2.1.2.1 - Person Entity (PE) Compliance Statements .....       | 6  |
| 2.1.2.2 - Non-Person Entity (NPE) Compliance Statements .....  | 7  |
| 2.1.3 - Authority Category .....                               | 7  |
| 2.1.3.1 - Person Entity (PE) Compliance Statements .....       | 7  |
| 2.1.3.2 - Non-Person Entity (NPE) Compliance Statements .....  | 7  |
| 2.1.4 - Authority To Operate (ATO) Status .....                | 7  |
| 2.1.4.1 - Person Entity (PE) Compliance Statements .....       | 7  |
| 2.1.4.2 - Non-Person Entity (NPE) Compliance Statements .....  | 7  |
| 2.1.5 - Authorized IC Person .....                             | 8  |
| 2.1.5.1 - Person Entity (PE) Compliance Statements .....       | 8  |
| 2.1.5.2 - Non-Person Entity (NPE) Compliance Statements .....  | 8  |
| 2.1.6 - Certificate Authority .....                            | 8  |
| 2.1.6.1 - Person Entity (PE) Compliance Statements .....       | 8  |
| 2.1.6.2 - Non-Person Entity (NPE) Compliance Statements .....  | 8  |
| 2.1.7 - Clearance .....                                        | 8  |
| 2.1.7.1 - Person Entity (PE) Compliance Statements .....       | 8  |
| 2.1.7.2 - Non-Person Entity (NPE) Compliance Statements .....  | 9  |
| 2.1.8 - Country of Affiliation .....                           | 9  |
| 2.1.8.1 - Person Entity (PE) Compliance Statements .....       | 9  |
| 2.1.8.2 - Non-Person Entity (NPE) Compliance Statements .....  | 9  |
| 2.1.9 - Digital Identifier .....                               | 9  |
| 2.1.9.1 - Person Entity (PE) Compliance Statements .....       | 9  |
| 2.1.9.2 - Non-Person Entity (NPE) Compliance Statements .....  | 10 |
| 2.1.10 - Duty Organization .....                               | 10 |
| 2.1.10.1 - Person Entity (PE) Compliance Statements .....      | 10 |
| 2.1.10.2 - Non-Person Entity (NPE) Compliance Statements ..... | 10 |
| 2.1.11 - Duty Organization Unit .....                          | 11 |
| 2.1.11.1 - Person Entity (PE) Compliance Statements .....      | 11 |
| 2.1.11.2 - Non-Person Entity (NPE) Compliance Statements ..... | 11 |
| 2.1.12 - Entity Security Mark .....                            | 11 |
| 2.1.12.1 - Person Entity (PE) Compliance Statements .....      | 11 |
| 2.1.12.2 - Non-Person Entity (NPE) Compliance Statements ..... | 11 |

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| 2.1.13 - Entity Type .....                                                  | 11 |
| 2.1.13.1 - Person Entity (PE) Compliance Statements .....                   | 11 |
| 2.1.13.2 - Non-Person Entity (NPE) Compliance Statements .....              | 12 |
| 2.1.14 - Fine Access Control .....                                          | 12 |
| 2.1.14.1 - Person Entity (PE) Compliance Statements .....                   | 12 |
| 2.1.14.2 - Non-Person Entity (NPE) Compliance Statements .....              | 14 |
| 2.1.15 - Group .....                                                        | 16 |
| 2.1.15.1 - Person Entity (PE) Compliance Statements .....                   | 16 |
| 2.1.15.2 - Non-Person Entity (NPE) Compliance Statements .....              | 16 |
| 2.1.16 - Handling Controls .....                                            | 16 |
| 2.1.16.1 - General Rules .....                                              | 16 |
| 2.1.16.2 - DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION<br>(DCNI) .....  | 17 |
| 2.1.16.3 - DISPLAYONLY .....                                                | 18 |
| 2.1.16.4 - DS .....                                                         | 19 |
| 2.1.16.5 - DSEN .....                                                       | 19 |
| 2.1.16.6 - FISA .....                                                       | 19 |
| 2.1.16.7 - FOUO .....                                                       | 20 |
| 2.1.16.8 - IMC .....                                                        | 20 |
| 2.1.16.9 - LES .....                                                        | 20 |
| 2.1.16.10 - LES-NF .....                                                    | 20 |
| 2.1.16.11 - ND .....                                                        | 21 |
| 2.1.16.12 - NF .....                                                        | 22 |
| 2.1.16.13 - OC .....                                                        | 22 |
| 2.1.16.14 - PR .....                                                        | 23 |
| 2.1.16.15 - REL .....                                                       | 23 |
| 2.1.16.16 - REL_ACGU .....                                                  | 24 |
| 2.1.16.17 - REL_FVEY .....                                                  | 24 |
| 2.1.16.18 - REL_TEYE .....                                                  | 25 |
| 2.1.16.19 - RS .....                                                        | 25 |
| 2.1.16.20 - SBU .....                                                       | 25 |
| 2.1.16.21 - SBU-NF .....                                                    | 26 |
| 2.1.16.22 - SSI .....                                                       | 26 |
| 2.1.16.23 - DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION<br>(UCNI) ..... | 27 |
| 2.1.16.24 - USONLY .....                                                    | 27 |
| 2.1.16.25 - USP .....                                                       | 27 |
| 2.1.16.26 - XD .....                                                        | 28 |
| 2.1.16.27 - Constraint Rule Across FDR Handling Controls .....              | 28 |
| 2.1.17 - IC Networks .....                                                  | 29 |
| 2.1.17.1 - Person Entity (PE) Compliance Statements .....                   | 29 |
| 2.1.17.2 - Non-Person Entity (NPE) Compliance Statements .....              | 29 |
| 2.1.18 - Is IC Member .....                                                 | 29 |
| 2.1.18.1 - Person Entity (PE) Compliance Statements .....                   | 29 |
| 2.1.18.2 - Non-Person Entity (NPE) Compliance Statements .....              | 29 |
| 2.1.19 - Lifecycle Status .....                                             | 29 |
| 2.1.19.1 - Person Entity (PE) Compliance Statements .....                   | 29 |
| 2.1.19.2 - Non-Person Entity (NPE) Compliance Statements .....              | 30 |
| 2.1.20 - Originating Network .....                                          | 30 |

|                                                                |    |
|----------------------------------------------------------------|----|
| 2.1.20.1 - Person Entity (PE) Compliance Statements .....      | 30 |
| 2.1.20.2 - Non-Person Entity (NPE) Compliance Statements ..... | 30 |
| 2.1.21 - Region .....                                          | 30 |
| 2.1.21.1 - Person Entity (PE) Compliance Statements .....      | 30 |
| 2.1.21.2 - Non-Person Entity (NPE) Compliance Statements ..... | 31 |
| 2.1.22 - Role .....                                            | 31 |
| 2.1.22.1 - Person Entity (PE) Compliance Statements .....      | 31 |
| 2.1.22.2 - Non-Person Entity (NPE) Compliance Statements ..... | 31 |
| 2.1.22.3 - Authorized Law Enforcement Personnel (ALEP) .....   | 31 |
| 2.1.23 - Topic .....                                           | 32 |
| 2.1.23.1 - Person Entity (PE) Compliance Statements .....      | 32 |
| 2.1.23.2 - Non-Person Entity (NPE) Compliance Statements ..... | 33 |
| 2.2 - AAS and AS Operation Compliance Statements .....         | 33 |
| 2.2.1 - Attribute Latency .....                                | 33 |
| 2.2.2 - Publish & Subscribe .....                              | 33 |
| 2.2.3 - Attribute Protection .....                             | 34 |
| Appendix A - Feature Summary .....                             | 35 |
| A.1 - UIAS-APCS Feature Summary .....                          | 35 |
| A.1.1 - Features from V2018-DEC to V2021-NOV .....             | 35 |
| A.1.2 - Features from V2016-FEB to V2018-DEC .....             | 35 |
| Appendix B - Change History .....                              | 36 |
| B.1 - V2021-NOV Change Summary .....                           | 36 |
| B.2 - V2019-SEP Change Summary .....                           | 37 |
| B.3 - V2019-MAR Change Summary .....                           | 37 |
| B.4 - V2018-DEC Change Summary .....                           | 38 |
| Appendix C - Glossary .....                                    | 39 |
| Appendix D - List of Abbreviations .....                       | 43 |
| Appendix E - Bibliography .....                                | 46 |
| Appendix F - Points of Contact .....                           | 52 |
| Appendix G - IC CIO Approval Memo .....                        | 53 |

## List of Figures

|                                         |   |
|-----------------------------------------|---|
| Figure 1 - Related Specifications ..... | 4 |
|-----------------------------------------|---|

## List of Tables

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Table 1 - Direct Dependencies .....                                 | 4  |
| Table 2 - Feature Summary Legend .....                              | 35 |
| Table 3 - UIAS-APCS Feature Comparison V2018-DEC to V2021-NOV ..... | 35 |
| Table 4 - UIAS-APCS Feature Comparison V2016-FEB to V2018-DEC ..... | 35 |
| Table 5 - DES Version Identifier History .....                      | 36 |
| Table 6 - V2021-NOV Change History .....                            | 36 |
| Table 7 - V2019-SEP Change History .....                            | 37 |
| Table 8 - V2019-MAR Change History .....                            | 38 |
| Table 9 - V2018-DEC Change History .....                            | 38 |

## Chapter 1 - Introduction

### 1.1 - Purpose

This *Attribute Practice Compliance Statements for the Unified Identity Attribute Set* (UIAS-APCS) provides concise direction to Intelligence Community (IC) elements required by Intelligence Community Standard (ICS) 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control Of Resources* [33], to produce an Attribute Practice Statement (APS) for each Attribute Service (AS) of an IC element. Compliance with an Attribute Practice Compliance Statement (APCS) document ensures interoperability and consistently applied attributes in dynamic Information Technology (IT) environments including the Intelligence Community Information Technology Enterprise (IC ITE). An APCS alleviates the need for each IC element to produce an APS and ensure compliance with ICS 500-30 [33], and *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML [42]).

This UIAS-APCS has a dependency on UIAS.XML [42]. Citations for the Controlled Vocabulary Enumeration (CVE)s are covered in the UIAS.XML [42] technical specification and should be complied with in accordance with the needs and practices of the responding organization, and that such compliance should also designate the reasoning for compliance approach or its variations. The UIAS.XML [42] MUST be consulted in conjunction with this document.

### 1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML [19]) 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.

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to a flexible, scalable and interoperable architecture for use within and across the IC's environments. Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [23] grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA)
- Lead the IC's identification, development, and management of IC enterprise standards
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA
- Certify IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common IT standards, protocols, and interfaces; to establish uniform information security standards; and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces, and to support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service enabled federated enterprise. As the enterprise develops and deploys shared services employing approved

standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse.

IC Enterprise Identity Attributes are assigned per persona. A persona is an electronic identity that is unambiguously associated with a single Person Entity (PE) or Non-Person Entity (NPE). A single PE 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).

The assignment of IC Enterprise Identity Attributes MUST be done in a consistent manner to facilitate interoperability and trust between systems. This document is intended to ensure that the attributes are provisioned in a consistent manner.

This UIAS-APCS is to be used by all agencies and system owners who write the APSs required for each Authoritative Attribute Source (AAS) and AS of an IC element and comply with ICS 500-30<sup>[33]</sup>, as well as operators and resource owners that rely on attributes for authorization decisions. The UIAS-APCS, published by the IC CIO, contains a compliance statement for each attribute identified in the UIAS.XML<sup>[42]</sup> technical specification for NPEs that are US owned, controlled, and vetted and for PEs.

Agencies MUST write variance statements for each AAS to identify where the agency provisioning differs from the compliance statements within this document. In cases where the agency is fully compliant with the compliance statement, the agency MUST state in writing that no variance exists. Reporting will be managed by the IC Identity, Credential, and Access Management Subcommittee (IC ICAM SC), in accordance with the IC ICAM SC Terms of Reference<sup>[20]</sup>, and reported at IC ICAM SC meetings.

## 1.3 - Enterprise Need

As the IC environment evolves, the user base grows with more diverse membership with unique data sources per member entity. The IC's move to a simplified architecture for access control and authorization is predicated on Attribute Based Access Control (ABAC) and an IC Authorization service being trustworthy. This drives an increased need to better understand attribute provisioning and ensure that all IC elements provision and maintain access control and authorization related attributes consistently. This document specifies compliance statements to confirm that enterprise identity attributes are consistent with the attributes defined in the UIAS.XML<sup>[42]</sup> technical specification and that IC elements maintain attributes consistent with Appendix C of ICS 500-30, *Operation of ASs and AAS* <sup>[33]</sup>. Compliance with the ICS 500-30<sup>[33]</sup> will ensure that all IC elements provision and maintain attributes for availability, accuracy, consistency, privacy, confidentiality, and integrity across persona lifecycles.

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

- 100 Series:
  - ICD 121, *Managing the Intelligence Community Information Environment* <sup>[22]</sup>
- 500 Series:
  - ICD 500, *Director Of National Intelligence Chief Information Officer* <sup>[23]</sup>
  - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* <sup>[24]</sup>

- Intelligence Community Program Guidance (ICPG) 500.1, *Digital Identity* [\[27\]](#)
- ICPG 500.2, *Attribute-based Authorization and Access Management* [\[28\]](#)
- ICS 500-20, *IC Enterprise Standards Compliance* [\[30\]](#)
- ICS 500-27, *Collection and Sharing of Audit Data* [\[31\]](#)
- ICS 500-29, *IC Digital Identifier* [\[32\]](#)
- ICS 500-30, *Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources* [\[33\]](#)
- 700 Series:
  - ICPG 704.5, *Intelligence Community Security Database Scattered Castles* [\[29\]](#)
- Memorandums:
  - OMB Memo - *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* [\[40\]](#)
  - IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* [\[13\]](#)
- DoD Issuances:
  - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* [\[6\]](#)
- Presidential Directives
  - HSPD-12 *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* [\[12\]](#)

## 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 [\[19\]](#).

In order to understand the compliance statements in [Section 2.1 - UIAS Compliance Statements](#), readers need familiarity with terms that have specialized meanings in the context of Identity, Credential, and Access Management (ICAM) functions. These terms with their definitions are defined in the [Appendix C - Glossary](#). A key distinction is the difference between the complete value of an entity attribute, contrasted with individual tokens in the attribute. For example, in the attribute `@ism:releasableTo="USA AFG FVEY"`, the tokens are "USA", "AFG" and "FVEY". In contrast, the value of `@ism:releasableTo` is the entire string "USA AFG FVEY".

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* [\[33\]](#), Appendix B. These terms include the following: Attribute, APS, AS, AAS, DN, Integree, NPE, and PE.

## 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 [\[19\]](#).

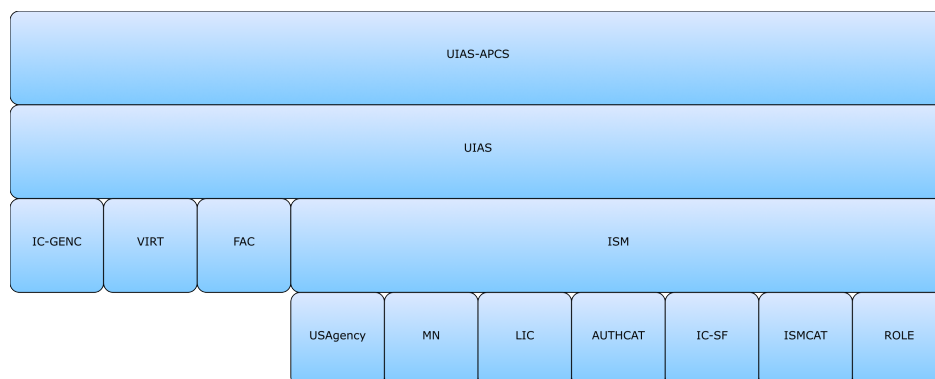
## 1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 1](#). The dependencies listed below are directly referenced in this specification (e.g., Schema, Schematron), and are normative or informative as indicated.

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

**Table 1 - Direct Dependencies**

| Name                                                                                                         | Dependency Description                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Data Encoding Specification for Unified Identity Attribute Set</i> (UIAS.XML.V2019-SEP+ <sup>[42]</sup> ) | This specification does not depend on a specific version of UIAS.XML <sup>[42]</sup> ; versions later than version 2019-SEP MAY be used. The minimum version was based on technical dependencies.                                                                                                                                                                                                                                                    |
| <i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ <sup>[19]</sup> )                | This specification does not depend on a specific version of IC-SF.XML <sup>[19]</sup> ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications. |



**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).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

## Chapter 2 - Development Guidance

For information on the structure and content of the specifications, please see the "Specification Overview" chapter in the IC-SF.XML<sup>[19]</sup> framework document. This chapter is intended to expand upon the common information that the framework specifies providing specific development guidance that is specific to the implementation of this specification.

### 2.1 - UIAS Compliance Statements

#### 2.1.1 - Admin Organization

##### 2.1.1.1 - Person Entity (PE) Compliance Statements

For a token of "MIL" in the **@entityType** attribute, the value for the **@adminOrganization** attribute MUST specify the administrative agency, military branch, or other top-level organization/department that holds a PE's human resource record.

For a token of "GOV" in the **@entityType** attribute, the value for the **@adminOrganization** attribute MUST specify the administrative agency, military branch, or other top-level organization/department that holds a PE's human resource record.

For a token of "CTR" in the **@entityType** attribute, the value for the **@adminOrganization** attribute MUST specify the administrative agency, military branch, or other top-level organization/department that holds the contract which a PE supports.

In support of Second Party Integree (2PI), the value for the **@adminOrganization** attribute MUST represent the home country's administrative agency, military branch, or other top-level organization/department, as defined in *Table 6 - Foreign Government adminOrganization Countries* in UIAS.XML<sup>[42]</sup>.

##### 2.1.1.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@adminOrganization** attribute MUST be the administrative agency, military branch, or other top-level organization/department that owns and maintains the system under which the NPE was created and is the Authorizing Official (AO) for the entity.

NPE's **@adminOrganization** attribute MUST contain a token from the *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES<sup>[43]</sup>) list.

#### 2.1.2 - Audit Routing Organization

##### 2.1.2.1 - Person Entity (PE) Compliance Statements

The tokens in the **auditRoutingOrganization** attribute MUST include any organization(s) beyond the entity's **dutyOrganization** and **adminOrganization** that should receive audit records for the PE, in accordance with ICS 500-27<sup>[31]</sup>.

The list of **auditRoutingOrganization** tokens for a PE MUST be coordinated between the PE's **dutyOrganization** and **adminOrganization**.

## 2.1.2.2 - Non-Person Entity (NPE) Compliance Statements

The tokens in the **auditRoutingOrganization** attribute MUST specify any organization(s) beyond the entity's **dutyOrganization** and **adminOrganization** that should receive audit records for the NPE, in accordance with ICS 500-27<sup>[31]</sup>.

The list of **auditRoutingOrganization** tokens for a NPE MUST be coordinated between the NPE's **dutyOrganization** and **adminOrganization**. Since both the NPE's **dutyOrganization** and **adminOrganization** have a need to track the actions and uses of the NPE, both organizations should be able to specify tokens for the NPE's **auditRoutingOrganization**.

## 2.1.3 - Authority Category

### 2.1.3.1 - Person Entity (PE) Compliance Statements

The tokens in the **authorityCategory** attribute MUST specify the PE's legal, policy, training, mission or other authorities required to access and/or discover protected resources.

The tokens in the **authorityCategory** attribute SHOULD include all of its Authority Categories for which it is authorized. The tokens in the **authorityCategory** attribute MUST be updated by the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed tokens to the enterprise.

### 2.1.3.2 - Non-Person Entity (NPE) Compliance Statements

The tokens in the **authorityCategory** attribute MUST include the NPE's legal, policy, training, mission or other authorities required to access and/or discover protected resources.

The tokens in the **authorityCategory** attribute SHOULD include all of its Authority Categories for which it is authorized.

The tokens in the **authorityCategory** attribute MUST be updated by the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed tokens to the enterprise.

## 2.1.4 - Authority To Operate (ATO) Status

### 2.1.4.1 - Person Entity (PE) Compliance Statements

Not Applicable.

### 2.1.4.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **ATOStatus** attribute for an NPE MUST be "**true**" or "**1**" if the NPE currently has an Authority To Operate (ATO), as authorized by the AO or Designated AO, in accordance with ICD 503, *Intelligence Community Information Technology Systems Security Risk Management* <sup>[25]</sup>.

The value for the **ATOStatus** attribute for an NPE MUST be "**false**" or "**0**" if the NPE does not have an ATO.

The value for the **ATOStatus** attribute for an NPE MUST match what is documented in the NPE's SSP as required by CNSSI 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems* [\[3\]](#).

## 2.1.5 - Authorized IC Person

### 2.1.5.1 - Person Entity (PE) Compliance Statements

Per ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* [\[24\]](#) Appendix A, the value for the **@aICP** attribute MUST be "**true**" or "**1**" if the PE is 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 and has been identified by an IC element head or an Authorized IC Person (AICP) approver who has been designated consistent with the procedures described in IC Memo 2010-0460, *Instructions for Designation of Authorized 704.5 Approvers* [\[17\]](#).

Per ICD 501 [\[24\]](#) Appendix A, the value for the **@aICP** attribute MUST be "**false**" or "**0**" if the PE has not met the requirements defining an AICP in paragraph 2 of ICD 501 [\[24\]](#), Appendix A.

The value for the **@aICP** attribute MUST be provided by one of the community core ICAM services operated and maintained by the Identity, Credential, and Access Management Service Providers (ICAM-SP).

### 2.1.5.2 - Non-Person Entity (NPE) Compliance Statements

Not applicable.

## 2.1.6 - Certificate Authority

### 2.1.6.1 - Person Entity (PE) Compliance Statements

The value for the **@certificateAuthority** attribute MUST reflect the issuing Public Key Infrastructure (PKI) certificate authority for the entity.

### 2.1.6.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@certificateAuthority** attribute MUST reflect the issuing PKI certificate authority for the entity.

## 2.1.7 - Clearance

### 2.1.7.1 - Person Entity (PE) Compliance Statements

The value for the **@clearance** attribute MUST reflect the highest clearance level briefed to the PE.

The value for the "**clearance**" attribute SHOULD match the clearance for the PE obtained from the Scattered Castles as defined by ICPG 704.5, *IC Personnel Security Database Scattered Castles* [\[29\]](#).

## 2.1.7.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@clearance** attribute MUST reflect the highest classification level for which the NPE is authorized.

## 2.1.8 - Country of Affiliation

For both PE and NPE compliance statements, the allowed values for **countryOfAffiliation** are the values listed in IC-GENC.CES[\[18\]](#) in the CVE "CVEnumGENCCountryCode.xml".

### 2.1.8.1 - Person Entity (PE) Compliance Statements

The tokens in the **countryOfAffiliation** attribute MUST include all of the countries for which the PE holds valid citizenships.

The **countryOfAffiliation** attribute MUST only contain tokens that represent the countries for which the PE holds valid citizenships.

In order to provision a PE with the token "**USA**", the PE MUST meet the conditions of being either 1) a natural born citizen or 2) a naturalized citizen of the United States of America. The token "**USA**" is specifically not a valid token for a permanent resident alien (e.g., green card holder) according to E.O. 12968[\[9\]](#).

In order to provision a PE with a token for a foreign government (e.g., "**GBR**") in the **countryOfAffiliation** attribute, the PE MUST satisfy the conditions set by the foreign government for meeting the citizenship requirements for a passport from that government.

### 2.1.8.2 - Non-Person Entity (NPE) Compliance Statements

The tokens in the **countryOfAffiliation** attribute MUST include tokens that represent the countries for organizations that provide control or administration of the NPE.

The **countryOfAffiliation** attribute MUST only contain tokens that represent countries for organizations that provide control or administration of the NPE.

## 2.1.9 - Digital Identifier

### 2.1.9.1 - Person Entity (PE) Compliance Statements

The value for the **@digitalIdentifier** attribute MUST be the PE's Distinguished Name (DN) from the PKI certificate (per ICS 500-29, *Intelligence Community Digital Identifier* [\[32\]](#)).

The value for the **@digitalIdentifier** attribute MUST be unique to the persona associated with the PE's PKI certificate (per ICS 500-29[\[32\]](#)).

The value for the **@digitalIdentifier** attribute MUST be provisioned from authoritative attribute sources (per ICS 500-29<sup>[32]</sup>).

The DN in the entity's **@digitalIdentifier** MUST include at least one of each of the following keywords: C (country name), CN (common name), O (organization name), and OU (organization unit name). Refer to IETF-RFC 4514, *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names* <sup>[34]</sup> and IC PKI Certificate Revocation List (CRL), *Intelligence Community Public Key Infrastructure Certificate and Certificate Revocation List Profiles* <sup>[16]</sup> for further guidance.

## 2.1.9.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@digitalIdentifier** attribute MUST be the NPE's DN from the PKI certificate (per ICS 500-29<sup>[32]</sup>).

The value for the **@digitalIdentifier** attribute MUST be unique to the persona associated with the NPE's PKI certificate (per ICS 500-29<sup>[32]</sup>).

The value for the **@digitalIdentifier** attribute MUST be provisioned from authoritative attribute sources (per ICS 500-29<sup>[32]</sup>).

The DN in the entity's **@digitalIdentifier** MUST include at least one of each of the following keywords: C (country name), CN (common name), O (organization name), and OU (organization unit name). Refer to IETF-RFC 4514<sup>[34]</sup> and IC PKI CRL <sup>[16]</sup> for further guidance.

## 2.1.10 - Duty Organization

### 2.1.10.1 - Person Entity (PE) Compliance Statements

The value for the **@dutyOrganization** attribute MUST specify the administrative agency, military branch, or other top-level organization/department which the PE is representing.

If PE is detailed from his or her home or administrative agency to another agency for a Joint Duty assignment or other rotation, the value for the **@dutyOrganization** attribute MUST be the administrative agency, military branch, or other top-level organization/department holding the PE's interim assignment.

In support of Second Party Integrees, the value for the **@dutyOrganization** attribute MUST represent the U.S. government sponsoring administrative agency, military branch, or other top-level organization/department.

### 2.1.10.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@dutyOrganization** attribute MUST be the administrative agency, military branch, or other top-level organization/department that owns the system under which the NPE was created and is the executive agent official for the entity.

If the NPE has been loaned or transferred from its administrative agency to another agency, or is being operated by another agency, the value for the **@dutyOrganization** attribute MUST be the

administrative agency, military branch, or other top-level organization/department currently holding or operating the NPE.

## 2.1.11 - Duty Organization Unit

### 2.1.11.1 - Person Entity (PE) Compliance Statements

The value for the **@dutyOrganizationUnit** attribute MUST specify the suborganization which the PE is representing. The value for the **@dutyOrganizationUnit** attribute MUST be a suborganization of the agency represented in the PE's **@dutyOrganization**.

If PE is detailed from his or her home or administrative agency to another agency for a Joint Duty assignment or other rotation, the value for the **@dutyOrganizationUnit** attribute MUST be the suborganization holding the PE's interim assignment.

In support of Second Party Integreees, the value for the **@dutyOrganizationUnit** attribute MUST represent the PE's assigned suborganization in the U.S. government sponsoring agency.

### 2.1.11.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@dutyOrganizationUnit** attribute MUST be the suborganization in the agency that owns the system under which the NPE was created and is the executive agent official for the entity.

If the NPE has been loaned or transferred from its administrative agency to another agency, or is being operated by another agency, the value for the **@dutyOrganizationUnit** attribute MUST be the suborganization of the agency currently holding or operating the NPE.

## 2.1.12 - Entity Security Mark

### 2.1.12.1 - Person Entity (PE) Compliance Statements

The security classification value for the **@entitySecurityMark** attribute specifying the classification for the entity's persona MUST be defined for PEs through a joint agreement between the PE **@adminOrganization** and **@dutyOrganization**.

### 2.1.12.2 - Non-Person Entity (NPE) Compliance Statements

The security classification value for the **@entitySecurityMark** attribute specifying the classification for the entity's persona MUST be defined for NPEs through a joint agreement between the NPE **@adminOrganization** and **@dutyOrganization**.

## 2.1.13 - Entity Type

### 2.1.13.1 - Person Entity (PE) Compliance Statements

The value for the **entityType** attribute MUST be "MIL" if the PE is operating as a military service member under this persona.

The value for the **entityType** attribute MUST be **"CTR"** if the PE is operating as a contractor under this persona.

The value for the **entityType** attribute MUST be **GOV** if the PE is operating as a government civilian employee under this persona. Note that **GOV** can be inclusive of Federal, State and Local government officials which is reflected through their **dutyOrganization**.

## 2.1.13.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **entityType** attribute MUST be **"SVR"** if the NPE is a server.

The value for the **entityType** attribute MUST be **"SVC"** if the NPE is a service, widget, application, software, etc.

The value for the **entityType** attribute MUST be **"DEV"** if the NPE is an end-point device.

The value for the **entityType** attribute MUST be **"NET"** if the NPE is a network device.

## 2.1.14 - Fine Access Control

### 2.1.14.1 - Person Entity (PE) Compliance Statements

Scattered Castles SHOULD serve as the authoritative repository for the **@fineAccessControls** attribute. Scattered Castles MUST serve as the authoritative repository for verifying and validating an individual's Controlled Access Program, except those exempted by the DNI or PDDNI from storage in Scattered Castle per ICD 906, *Controlled Access Programs* [\[26\]](#).

Scattered Castles, or successor systems, is the authoritative repository for verifying and validating an individual's CAP accesses.

The tokens in the **@fineAccessControls** attribute MUST be the valid tokens that represent all of the applicable following categories:

- Secure Compartmented Information (SCI) Controls:

The entity's **@fineAccessControls** attribute MUST be provisioned with all of the control systems, compartments, and subcompartments from the authoritative source list to which the PE has been authorized access.

The entity's **@fineAccessControls** attribute MUST be provisioned with only the control systems, compartments, and subcompartments to which the PE has been authorized access.

SCI Control tokens MUST include the entire hierarchy of the control systems, compartments, or subcompartments (see below).

- The control systems, compartments, and subcompartments MUST be provisioned as separate tokens. For example, a PE authorized for the SI control system and its Gamma compartment would be provisioned with two tokens, **"SI"** and **"SI-G"**, in the PE's **@fineAccessControls** attribute. A PE authorized for the SI control system, its Gamma compartment and a Gamma subcompartment **"####"** would be provisioned with three

tokens, "**SI**", "**SI-G**" and "**SI-G-####**", in the PE's **@fineAccessControls** attribute.

- Special Access Programs (SAP):

The entity's **@fineAccessControls** attribute MUST be provisioned with all Special Access Program (SAP)s to which the PE has been authorized access.

The entity's **@fineAccessControls** attribute MUST be provisioned with only the SAPs for which the PE has been authorized access.

SAP tokens MUST start with the prefix "**SAR-**" followed by the actual token that designates the SAP.

Each SAP value in **@fineAccessControls** identifies, in the following order (see FAC.CES<sup>[1]</sup>):

1. Identification that a **@fineAccessControls** value is a SAP, signified by the prefix 'SAR-'
2. The agency that owns the SAP, followed by a colon (:)
3. (Optional) Required classification read-on level for the SAP data, for SAPs that have different read-ons for different classification levels, following by a colon (:)
4. The SAP marking value.

In order to facilitate automated access control for SAPs that have different read-ons for different classification, the SAP values in an entity's **@fineAccessControls** attribute MUST be denormalized:

- If a user is granted a TOP SECRET read-on to a hypothetical Department of Defense (DOD) SAP STORMY PETREL, the user MUST have all of the following values in **@fineAccessControls** :
  - "**DOD:TS:STORMY\_\_PETREL**"
  - "**DOD:S:STORMY\_\_PETREL**"
  - "**DOD:C:STORMY\_\_PETREL**".
- If a user is granted a SECRET read-on to a hypothetical DOD SAP STORMY PETREL, the user MUST have all of the following values in **@fineAccessControls** :
  - "**DOD:S:STORMY\_\_PETREL**"
  - "**DOD:C:STORMY\_\_PETREL**".
- If a user is granted a CONFIDENTIAL read-on to a hypothetical DOD SAP STORMY PETREL, the user MUST have the following value in **@fineAccessControls** :
  - "**DOD:C:STORMY\_\_PETREL**".

For a hypothetical DNI SAP BUTTER POPCORN that **does not** require different read-ons for different classification levels, an entity **MUST** have a single **@fineAccessControls** value of **"DNI : BUTTER\_POPCORN"**.

- Atomic Energy Markings:

If the PE is authorized for access to atomic energy information designated as CNWDI, then the token **"CNWDI"** **MUST** be provisioned.

- Alternative Compensatory Control Markings (ACCMs):

The entity's **@fineAccessControls** attribute **MUST** be provisioned with all Alternative Compensatory Control Measures (ACCM)s to which the PE has been authorized access.

The entity's **@fineAccessControls** attribute **MUST** be provisioned with only the ACCMs for which the PE has been authorized access.

ACCM tokens **MUST** start with the prefix **"ACCM - "** followed by the actual token that designates the ACCM.

- North Atlantic Treaty Organization (NATO) Information:

If the PE is briefed into and possesses a read-on for NATO information at the Top Secret level, then the token **"NATO-CTS"** **MUST** be provisioned.

If the PE is briefed into and possesses a read-on for NATO information at the Secret level, then the token **"NATO-NS"** **MUST** be provisioned.

If the PE is briefed into and possesses a read-on for NATO information at the Confidential level, then the token **"NATO-NC"** **MUST** be provisioned.

If the PE is briefed into and possesses a read-on for NATO information at the Restricted level, then the token **"NATO-NR"** **MUST** be provisioned.

If the PE is authorized for access to NATO atomic energy information, then the token **"NATO-ATOMAL"** **MUST** be provisioned.

If the PE is authorized for NATO information designated as BALK, then the token **"NATO-BALK"** **MUST** be provisioned.

If the PE is authorized for NATO information designated as BOHEMIA, then the token **"NATO-BOHEMIA"** **MUST** be provisioned.

## 2.1.14.2 - Non-Person Entity (NPE) Compliance Statements

The tokens in the **@fineAccessControls** attribute **MUST** be authorized for the NPE in its CNSSI 1254<sup>[3]</sup> artifacts including System Security Plan (SSP) and Authorization Decision Document (ADD).

The tokens in the **@fineAccessControls** attribute **MUST** be the valid tokens that represent all of the applicable following categories:

- Secure Compartmented Information (SCI) Controls:

The entity's **@fineAccessControls** attribute MUST be provisioned with all of the control systems, compartments, and subcompartments from the authoritative source list that the NPE has been authorized to store/process.

The entity's **@fineAccessControls** attribute MUST be provisioned with only the control systems, compartments, and subcompartments that the NPE has been authorized to store/process.

SCI Control tokens MUST include the entire hierarchy of the control systems, compartments, or subcompartments (see below).

- The control systems, compartments, and subcompartments MUST be provisioned as separate tokens. For example, a NPE authorized for the SI control system and its Gamma compartment would be provisioned with two tokens, "**SI**" and "**SI-G**", in the NPE's **@fineAccessControls** attribute. A NPE authorized for the SI control system, its Gamma compartment and a Gamma subcompartment "####" would be provisioned with three tokens, "**SI**", "**SI-G**" and "**SI-G-####**", in the NPE's **@fineAccessControls** attribute.

- Special Access Programs (SAP):

The entity's **@fineAccessControls** attribute MUST be provisioned with all SAPs to which the NPE has been authorized to store/process.

The entity's **@fineAccessControls** attribute MUST be provisioned with only the SAPs for which the NPE has been authorized to store/process.

SAP tokens MUST start with the prefix "**SAP-**" followed by the actual tokens that designates the SAP.

- Atomic Energy Markings:

If the NPE is authorized for storage/processing of atomic energy information designated as CNWDI, then the token "**CNWDI**" MUST be provisioned.

- Alternative Compensatory Control Markings (ACCMs):

The entity's **@fineAccessControls** attribute MUST be provisioned with all ACCMs to which the NPE has been authorized to store/process.

The entity's **@fineAccessControls** attribute MUST be provisioned with only the ACCMs for which the NPE has been authorized to store/process.

ACCM tokens MUST start with the prefix "**ACCM-**" followed by the actual token that designates the ACCM.

- NATO Information:

If the NPE is authorized to store/process NATO information at the Top Secret level, then the token "**NATO-CTS**" MUST be provisioned.

If the NPE is authorized to store/process NATO information at the Secret level, then the token **"NATO-NS"** MUST be provisioned.

If the NPE is authorized to store/process NATO information at the Confidential level, then the token **"NATO-NC"** MUST be provisioned.

If the NPE is authorized to store/process NATO information at the Restricted level, information, then the token **"NATO-NR"** MUST be provisioned.

If the NPE is authorized to store/process NATO atomic energy information, then the token **"NATO-ATOMAL"** MUST be provisioned.

If the NPE is authorized to store/process NATO information designated as BALK, then the token **"NATO-BALK"** MUST be provisioned.

If the NPE is authorized to store/process NATO information designated as BOHEMIA, then the token **"NATO-BOHEMIA"** MUST be provisioned.

## 2.1.15 - Group

### 2.1.15.1 - Person Entity (PE) Compliance Statements

The token(s) in the **group** attribute MUST include the entity's authorized group assignments (e.g., based on the entity's position, job, or area of responsibility) needed to determine the protected resources the entity may access.

The token(s) in the **group** attribute MUST be provided by one of the community core ICAM services operated and maintained by the ICAM-SP.

### 2.1.15.2 - Non-Person Entity (NPE) Compliance Statements

The token(s) in the **group** attribute MUST include the NPE's authorized group assignments (based on scope or function) needed to determine the protected resources the entity may access.

The token(s) in the **group** attribute MUST be provided by one of the community core ICAM services operated and maintained by the ICAM-SP.

## 2.1.16 - Handling Controls

### 2.1.16.1 - General Rules

The **handlingControls** attribute defines restrictions on the handling of data that go beyond the data's classification or compartmentalization attributes.

1. In general, tokens in an NPE's **handlingControls** attribute MUST be tokens that the NPE has been authorized to handle as documented in the NPE's Committee on National Security Systems Instruction (CNSSI) 1254<sup>[3]</sup> artifacts including System Security Plan (SSP) and/or Authorization Decision Document.

2. The IC element that operates and maintains the NPE MUST define all the token(s) for the NPE's **handlingControls** attribute.
3. An NPE MUST implement applicable access control rules documented in ISM.ACES<sup>[35]</sup>, for each token in the NPE's **handlingControls** attribute.
4. An NPE MUST implement applicable access control rules documented in ISM.ACES<sup>[35]</sup>, for all Need-To-Know entries that are required based on a **handlingControls** marking in data's Information Security Markings (ISM) attributes.
5. An NPE MUST meet auditing requirements as specified in ICS 500-27<sup>[31]</sup> regarding data marked with **handlingControls**.
  - An NPE MUST generate auditing records that document all the Handling Control markings on data in the AUDIT.XML<sup>[1]</sup> **ClassificationContent** of the Resource.
6. An NPE MUST disseminate data to another NPE only if the receiving NPE meets the **handlingControls** requirements for the data being sent.

When there is an enterprise AS or AAS available that has been authorized by the IC ICAM SC, the **handlingControls** tokens for an NPE that operates in IC Information Environment (IC IE) SHOULD be made available from the enterprise AS or AAS.

The **handlingControls** tokens for an NPE MAY be provided by an AS or AAS of the IC element that owns or operates the NPE.

Any exchange of BOE.XML<sup>[2]</sup> for an NPE SHOULD contain all the **handlingControls** tokens for the NPE.

## 2.1.16.2 - DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (DCNI)

An NPE is authorized to have the DCNI Handling Control if it meets **ALL** of the following requirements as documented in ISM.ACES<sup>[35]</sup>:

1. For DCNI data that is not marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE MUST meet all of these requirements:
  - The NPE MUST restrict access to the data to entities that have both **adminOrganization** and **dutyOrganization** in "[**USAgencyList**]", and
  - The NPE MUST restrict access to the data to entities that:
    - a. Have **dutyOrganization** that is not "**SLT**", or
    - b. Have **dutyOrganization** that is "**SLT**", and also have **entityType** that contains one of "**GOV**", "**MIL**", "**SVR**", "**SVC**", "**DEV**", "**NET**" (i.e., contractors are not authorized).
2. For DCNI data that is marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE:

- MUST be capable of using an entity's **countryOfAffiliation** and **adminOrganization** attributes to enforce the ISM.ACES<sup>[35]</sup> access rules for any and all of "REL", "EYES" or "DISPLAYONLY" markings that appear on the data.
- SHOULD have **handlingControls** that contains "REL".

### 2.1.16.3 - DISPLAYONLY

The DISPLAYONLY marking restricts access to data by PEs that are citizens of and work for the DISPLAYONLY list of countries/international organizations. DISPLAYONLY PEs are authorized to view the DISPLAYONLY data, but they are not authorized to create or store a physical copy of the data for retention, regardless of medium.

An NPE is authorized to have the DISPLAYONLY Handling Control if it meets **ALL** of the following requirements:

1. The NPE MUST prevent DISPLAYONLY entities from creating any physical copy of the data, regardless of medium.
2. The NPE MUST satisfy one of the following two conditions:
  - a. The NPE is authorized to allow DISPLAYONLY entities to view the data, because the NPE is capable of using dynamic digital rights management (DRM) or similar technology to prevent DISPLAYONLY entities from creating a physical copy of DISPLAYONLY data that they view.
  - or
  - b. If the NPE is not capable of preventing an entity from creating physical copies of DISPLAYONLY data once it has allowed the entity to view the document, then the NPE MUST prevent DISPLAYONLY entities from viewing the DISPLAYONLY data.
3. The NPE MUST implement the ISM.ACES<sup>[35]</sup> rule that applies REL access rules to a country/international organization that appears in both REL and DISPLAYONLY markings on a data resource.
  - If DISPLAYONLY and REL markings appear on the same data and both markings include one or more tetragraphs, and if there is a country/tetragraph that is a member of both a DISPLAYONLY tetragraph and a REL tetragraph on the same data, then the access rules for REL supersede the rules for DISPLAYONLY for that country/tetragraph.
  - Note this is not a roll-up rule but instead is a rule that applies when DISPLAYONLY and REL appear on the same data (same portion or same document banner). As an example, if a document is marked SECRET//REL TO USA, FVEY/DISPLAYONLY GMIF, then the document is REL TO AUS because AUS is a member of both FVEY and GMIF.

## 2.1.16.4 - DS

An NPE is authorized to have the "**DS**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** restrict access to DS data to entities that have an organizational affiliation with the U.S. Federal government as documented in ISM.ACES<sup>[35]</sup>.
2. The NPE **MUST** restrict access to DS data to PEs who are U.S. citizens.
3. The NPE **MUST** display/print DS caveat notices when displaying or printing DS data.

## 2.1.16.5 - DSEN

An NPE is authorized to have the "**DSEN**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** restrict PE access to DSEN data to:
  - PEs that have a **dutyOrganization** in the U.S. Federal government.
  - or**
  - PEs that are not contractors (**entityType** is not "**CTR**") and that have **dutyOrganization** = "**SLT**".
2. The NPE **MUST** restrict access to DSEN data to PEs that have **countryOfAffiliation** containing the token "**USA**" and that have **adminOrganization** from the **USAgencyList**.
3. The NPE **MUST** restrict access to DSEN data to NPEs that have **handlingControls** that contain the token "**DSEN**".
4. The NPE **MUST** display/print the DSEN caveat notice when displaying or printing DSEN data.

## 2.1.16.6 - FISA

An NPE is authorized to have the "**FISA**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** restrict access to UNCLASSIFIED FISA data to entities that are affiliated with a U.S. Federal, State, Local or Tribal government organization as documented in ISM.ACES<sup>[35]</sup>.
2. The NPE **MUST** be capable of meeting automatic purge requirements that may be levied by FISA orders.
3. The NPE **MUST** display/print FISA caveat notices when displaying or printing FISA data.

## 2.1.16.7 - FOUO

An NPE is authorized to have the FOUO Handling Control if it meets **ALL** of the following requirements as documented in ISM.ACES<sup>[35]</sup>:

1. For FOUO data that is not marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE **MUST** restrict access to the data to entities that have both **adminOrganization** and **dutyOrganization** in "**[USAgencyList]**".
2. For FOUO data that is marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE:
  - **MUST** be capable of using an entity's **countryOfAffiliation** and **adminOrganization** attributes to enforce the ISM.ACES<sup>[35]</sup> access rules for any and all of "**REL**", "**EYES**" or "**DISPLAYONLY**" markings that appear on the data.
  - **SHOULD** have **handlingControls** that contains "**REL**".

## 2.1.16.8 - IMC

An NPE is authorized to have the IMC Handling Control if it meets **ALL** of the following requirements:

1. An NPE **MUST** be granted prior written approval by the Sensitive Analytical Techniques (SAT) Panel Chair, in order to process data marked IMC (*IC Markings System Register and Manual*<sup>[15]</sup>).
2. The NPE **MUST** display/print IMC caveat notices when displaying or printing IMC data.

## 2.1.16.9 - LES

An NPE is authorized to have the "**LES**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** restrict access to LES data based on an entity's organizational affiliation as documented in ISM.ACES<sup>[35]</sup>.
2. The NPE **MUST** take into account any Foreign Disclosure & Release (FDR) markings on data that is marked LES, as documented in ISM.ACES<sup>[35]</sup>.
3. The NPE **MUST** display/print LES caveat notices when displaying or printing LES data.

## 2.1.16.10 - LES-NF

An NPE is authorized to have the "**LES-NF**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** have the token "**LES**" in the NPE's **handlingControls** attribute.
2. The NPE's **countryOfAffiliation** attribute **MUST** contain the token "**USA**" and only the token "**USA**".

3. The NPE's **adminOrganization** attribute MUST be in the **USAgency** list.
4. The NPE MUST be capable of ensuring that only entities with the token **"USA"** in **countryOfAffiliation** and **adminOrganization** in **USAgency** are given access to LES-NF data, by satisfying one of the following requirements:
  - a. The NPE's **handlingControls** attribute contains the token **"NF"**, signifying that the NPE is capable of enforcing access based on the **"NF"** marking.  
or
  - b. The NPE's **handlingControls** attribute contains the token **"USONLY"**, signifying that only US citizens are allowed on the NPE.  
or
  - c. The NPE's **handlingControls** attribute contains the token **"REL"**, signifying that the NPE is capable of enforcing all access rules relating to all the FDR markings (NF, REL, EYES Only, DISPLAYONLY, LES-NF and SBU-NF).

## 2.1.16.11 - ND

An NPE is authorized to have the **"ND"** Handling Control if it meets **ALL** of the following requirements:

1. The NPE MUST have been granted formal approval from the Department of State to process ND data.
2. The NPE MUST prevent further dissemination of data marked ND beyond the original addressee(s) unless so approved by the Executive Secretary of the U.S. Department of State.
  - a. The NPE MUST be capable of restricting access to ND data by one or both of the following two rules:
    - i. The NPE MUST be capable of restricting access to ND data by processing "ND-NTK.XML" following the rules documented in the ISM.ACES<sup>[35]</sup>.  
or
    - ii. The NPE MUST be capable of using metadata on the resource that is logically equivalent to "ND-NTK.XML" and applying the access rules documented for ND-NTK in the ISM.ACES<sup>[35]</sup>.
3. Since data marked ND must also be marked NF, then the NPE MUST be capable of ensuring that only entities with the token **"USA"** in **countryOfAffiliation** and **adminOrganization** in the **USAgency** list are given access to ND data, by satisfying one of the following requirements:
  - a. The NPE's **handlingControls** attribute contains the token **"NF"**, signifying that the NPE is capable of enforcing access based on the **"NF"** marking.

or

- b. The NPE's **handlingControls** attribute contains the token "**USONLY**", signifying that only US citizens are allowed on the NPE.

or

- c. The NPE's **handlingControls** attribute contains the token "**REL**", signifying that the NPE is capable of enforcing all access rules relating to all the FDR markings (NF, REL, EYES Only, DISPLAYONLY, LES-NF and SBU-NF).

## 2.1.16.12 - NF

An NPE is authorized to have the NF Handling Control if it meets **ALL** of the following requirements:

1. The NPE's **countryOfAffiliation** attribute MUST contain the token "**USA**" and only the token "**USA**".
2. The NPE's **adminOrganization** attribute MUST be in the **USAgencyList**.
3. The NPE MUST be capable of ensuring that only entities with the token "**USA**" in **countryOfAffiliation** and **adminOrganization** in the **USAgency** list are given access to NF data.

## 2.1.16.13 - OC

An NPE is authorized to have the "**OC**" **handlingControls** attribute if it meets **ALL** of the following requirements:

1. The NPE MUST be capable of dynamically determining if entities are eligible for access to the data based on the entity's **dutyOrganization** value and matching it to one of the following:
    - The authorized distribution list tagged on the data.
- or
- Need-To-Know Metadata (NTK) tags on the data that conform to the "**OC-NTK**" profile in ISM.XML<sup>[36]</sup>.
  2. The NPE MUST be capable of restricting access to OC data by one or both of the following two rules:
    - a. The NPE MUST be capable of restricting access to OC data by processing "OC-NTK.XML" following the rules documented in ISM.ACES<sup>[35]</sup>.

or

- b. The NPE MUST be capable of using metadata on the resource that is logically equivalent to "OC-NTK.XML" and applying the access rules documented for "**OC-NTK**" in ISM.ACES<sup>[35]</sup>.

## 2.1.16.14 - PR

The NPE MUST be authorized as capable of restricting access to PR data to those who are authorized and have completed appropriate non-disclosure agreements (NDAs) required for access to the data.

The NPE MUST be capable of restricting access to PR data by one or both of the following two rules:

1. The NPE MUST be capable of restricting access to PR data by processing "PR-NTK.XML" following the rules documented in ISM.ACES<sup>[35]</sup>.
- or
2. The NPE MUST be capable of using metadata on the resource that is logically equivalent to "PR-NTK.XML" and applying the access rules documented for "**PROPIN-NTK**" in ISM.ACES<sup>[35]</sup>.

## 2.1.16.15 - REL

The NPE MUST be authorized as capable of enforcing proper dynamic access control based on foreign disclosure and releasability restrictions tagged on the data. This means the NPE is capable of properly interpreting and processing all releasability markings (i.e., REL TO, NF, EYES Only, DISPLAY ONLY, LES-NF, SBU-NF).

An NPE is authorized to have the "**REL**" Handling Control if it meets **ALL** of the following requirements:

1. The NPE MUST be capable of using an entity's **countryOfAffiliation** and **adminOrganization** attributes to enforce the ISM.ACES<sup>[35]</sup> access rules for **ALL** of the following markings:
  - a. REL
  - b. NF
  - c. EYES
  - d. DISPLAYONLY
  - e. LES-NF
  - f. SBU-NF
2. The NPE MUST satisfy the requirements in Section 2.1.14 of this document, for all of the following **handlingControls**: "**REL**", "**NF**", "**DISPLAYONLY**", "**LES-NF**", and "**SBU-NF**".

## 2.1.16.16 - REL\_ACGU

The REL\_ACGU Handling Control is used for NPEs that are NOT capable of appropriately processing releasability markings on data, but that:

- Restrict access to entities that have one of "AUS", "CAN", "GBR", or "USA" in their **@countryOfAffiliation** attribute and that have an appropriate **@adminOrganization** for their country,  
  
and
- Only handle data that is at least releasable to all the ACGU countries. A data resource in the NPE MAY be releasable to the ACGU countries plus other countries, but MUST be releasable to all the ACGU countries.

An NPE is authorized to have the REL\_ACGU Handling Control if it meets **ALL** of the following requirements:

1. The NPE or its surrounding environment MUST ONLY grant access to entities whose **@countryOfAffiliation** is one of the ACGU members ("USA", "AUS", "CAN", "GBR"), and whose **@dutyOrganization** is in the **USAgency** list for U.S. entities or matches the non-US organizational pattern (e.g., "CAN\_\*") for non-US entities from one of the ACGU countries.
2. The NPE only processes data that is, at a minimum, REL to ACGU expressed either as the tetragraph ACGU or as the complete list of countries: "AUS", "CAN", "GBR", "USA".

## 2.1.16.17 - REL\_FVEY

The REL\_FVEY Handling Control is used for NPEs that are NOT capable of appropriately processing releasability markings on data, but that:

- Restrict access to entities that have one of "AUS", "CAN", "GBR", "NZL", or "USA" in their **@countryOfAffiliation** attribute and that have an appropriate **@adminOrganization** for their country,  
  
and
- Only handle data that is at least releasable to all the FVEY countries. A data resource in the NPE MAY be releasable to the FVEY countries plus other countries, but MUST be releasable to all the FVEY countries.

An NPE is authorized to have the REL\_FVEY Handling Control if it meets **ALL** of the following requirements:

1. The NPE or its surrounding environment MUST ONLY grant access to entities whose **@countryOfAffiliation** is one of the FVEY members ("USA", "AUS", "CAN", "GBR"), and whose **@dutyOrganization** is in the **USAgency** list for U.S. entities or matches the non-US organizational pattern (e.g., "CAN\_\*") for non-US entities from one of the FVEY countries.

2. The NPE only processes data that is, at a minimum, REL to FVEY expressed either as the tetragraph ACGU or as the complete list of countries: "**AUS**", "**CAN**", "**GBR**", "**NZL**", "**USA**".

## 2.1.16.18 - REL\_TEYE

The REL\_TEYE Handling Control is used for NPEs that are NOT capable of appropriately processing releasability markings on data, but that:

- Restrict access to entities that have one of "**AUS**", "**GBR**", or "**USA**" in their **@countryOfAffiliation** attribute and that have an appropriate **@adminOrganization** for their country,  
  
and
- Only handle data that is at least releasable to all the TEYE countries. A data resource in the NPE MAY be releasable to the TEYE countries plus other countries, but MUST be releasable to all the TEYE countries.

An NPE is authorized to have the REL\_TEYE Handling Control if it meets **ALL** of the following requirements:

1. The NPE or its surrounding environment MUST ONLY grant access to entities whose **@countryOfAffiliation** is one of the TEYE members ("**USA**", "**AUS**", "**GBR**"), and whose **@dutyOrganization** is in the **USAgency** list for U.S. entities or matches the non-US organizational pattern (e.g., "**GBR\_\***") for non-US entities from one of the TEYE countries.
2. The NPE only processes data that is, at a minimum, REL to TEYE expressed either as the tetragraph TEYE or as the complete list of countries: "**AUS**", "**GBR**", "**USA**".

## 2.1.16.19 - RS

There are no rules currently for provisioning PEs or NPEs with the token "**RS**" in the **handlingControls** attribute, because the RS marking has no impact on access control according to the ISM.ACES<sup>[35]</sup>.

## 2.1.16.20 - SBU

As documented in the ISM.ACES<sup>[35]</sup>, the SBU marking on a resource restricts access to PEs with organizational affiliation to the U.S. Federal Government. This rule applies to U.S. citizens only. Since SBU can co-occur with REL markings, the rule is conditional on U.S. citizenship. Since there is no controlled vocabulary for foreign partner organizations at this time, there is no SBU rule relating to foreign partner PEs.

An NPE is authorized to have the SBU Handling Control if it meets **ALL** of the following requirements as documented in ISM.ACES<sup>[35]</sup>:

1. For SBU data that is not marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE MUST meet all of these requirements:

- The NPE MUST restrict access to the data to entities that have both **adminOrganization** and **dutyOrganization** in "[USAgencyList]", and
  - The NPE MUST restrict access to the data to entities that have **dutyOrganization** that is not "SLT".
2. For SBU data that is marked with "REL", "EYES" or "DISPLAYONLY", the NPE:
- MUST be capable of using an entity's **countryOfAffiliation** and **adminOrganization** attributes to enforce the ISM.ACES<sup>[35]</sup> access rules for any and all of "REL", "EYES" or "DISPLAYONLY" markings that appear on the data.
  - SHOULD have **handlingControls** that contains "REL".

## 2.1.16.21 - SBU-NF

As documented in the ISM.ACES<sup>[35]</sup>, the "SBU - NF" marking on a resource restricts access to entities with **countryAffiliation** equal to "USA" and organizational affiliation to the U.S. Federal Government.

An NPE is authorized to have the "SBU" Handling Control if **ALL** of the following rules are satisfied:

1. The NPE's **countryOfAffiliation** attribute MUST contain the token "USA" and only the token "USA".
2. The NPE's **adminOrganization** MUST be in the **USAgency** list.
3. The NPE's **handlingControls** attribute MUST contain either "NF" or "USONLY" or "REL".
4. The NPE MUST allow an entity to access a resource marked "SBU - NF" only if all of the following conditions are satisfied:
  - a. The entity's **adminOrganization** MUST be from the **USAgency** list.
  - and
  - b. The entity's **dutyOrganization** MUST NOT equal "SLT".

## 2.1.16.22 - SSI

An NPE is authorized to have the "SSI" Handling Control if it meets **ALL** of the following requirements:

1. The NPE MUST allow an entity to access a resource marked SSI if and only if the entity meets the clearance requirements documented for SSI in ISM.ACES<sup>[35]</sup>.
2. The NPE MUST display/print SSI caveat notices when displaying or printing SSI data.

## 2.1.16.23 - DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)

An NPE is authorized to have the UCNI Handling Control if it meets **ALL** of the following requirements as documented in ISM.ACES<sup>[35]</sup>:

1. For UCNI data that is not marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE **MUST** meet all of these requirements:
  - The NPE **MUST** restrict access to the data to entities that have both **adminOrganization** and **dutyOrganization** in "**[USAgencyList]**", and
  - The NPE **MUST** restrict access to the data to entities that:
    - a. Have **dutyOrganization** that is not "**SLT**", or
    - b. Have **dutyOrganization** that is "**SLT**", and also have **entityType** that contains one of "**GOV**", "**MIL**", "**SVR**", "**SVC**", "**DEV**", "**NET**" (i.e., contractors are not authorized).
2. For UCNI data that is marked with "**REL**", "**EYES**" or "**DISPLAYONLY**", the NPE:
  - **MUST** be capable of using an entity's **countryOfAffiliation** and **adminOrganization** attributes to enforce the ISM.ACES<sup>[35]</sup> access rules for any and all of "**REL**", "**EYES**" or "**DISPLAYONLY**" markings that appear on the data.
  - **SHOULD** have **handlingControls** that contains "**REL**".

## 2.1.16.24 - USONLY

The "**USONLY**" Handling Control is used for NPEs that are NOT capable of appropriately processing releasability markings on data, but that restrict access to entities that have **countryOfAffiliation** equal to "**USA**" and that work for the U.S. Federal, State, Local or Tribal government.

An NPE is authorized to have the "**USONLY**" Handling Control if it enforces the following rule:

- An entity can access the NPE only if all of the following conditions are satisfied:
  1. The entity's **countryOfAffiliation** **MUST** include the token "**USA**".  
and
  2. The entity's **adminOrganization** **MUST** be from the **USAgency** list.

## 2.1.16.25 - USP

The "**USP**" Handling Control indicates that an NPE has been authorized as having capabilities to handle, share and protect United States Person (USP) data in accordance with E.O. 12333<sup>[8]</sup> and other applicable Federal and agency policies.

The "**USP**" Handling Control is not authorized for use at this time. There are no IC-common metadata tags defined to identify data as containing USP information, and there are no USP-specific access control rules that have been standardized in common across the IC.

The USP Handling Control token **MUST NOT** be used until a future version of this APCS is published.

## 2.1.16.26 - XD

An NPE is authorized to have the XD Handling Control if it meets **ALL** of the following requirements:

1. The NPE **MUST** be capable of dynamically determining if entities are eligible for access to the data based on the entity's **dutyOrganization** value and matching it to one of the following:
  - The authorized distribution list tagged on the data.
  - or
  - NTK tags on the data that conform to the XD-NTK profile in ISM.XML<sup>[36]</sup>.
2. The NPE **MUST** be capable of restricting access to XD data by one or both of the following two rules:
  - a. The NPE **MUST** be capable of restricting access to XD data by processing "XD-NTK.XML" following the rules documented in ISM.ACES<sup>[35]</sup>.
  - or
  - b. The NPE **MUST** be capable of using metadata on the resource that is logically equivalent to "XD-NTK.XML" and applying the access rules documented for XD-NTK in ISM.ACES<sup>[35]</sup>.

## 2.1.16.27 - Constraint Rule Across FDR Handling Controls

An NPE **MUST NOT** be granted more than one of the FDR Handling Controls, listed below:

- "NF"
- "REL"
- "REL\_TYE"
- "REL\_ACGU"
- "REL\_FVEY"
- "USONLY"

This rule is necessary because these FDR Handling Controls are mutually exclusive.

## 2.1.17 - IC Networks

### 2.1.17.1 - Person Entity (PE) Compliance Statements

The token(s) in the **@icNetworks** attribute MUST be defined for PEs by the respective IC element.

The **@icNetworks** attribute MUST identify the network(s) to which an entity's attributes are allowed to be transferred.

The token(s) in the **@icNetworks** attribute MUST come from the CVE "CVEnumVIRTNetworkName.xml" in the *XML Data Encoding Specification for Virtual Coverage* (VIRT.XML<sup>[44]</sup>) (see also UIAS.XML<sup>[42]</sup>, Section 2.3.16).

### 2.1.17.2 - Non-Person Entity (NPE) Compliance Statements

The token(s) in the **@icNetworks** attribute MUST be defined for NPEs by the respective IC element.

The attribute must contain the network(s) to which an entity's attributes can be transferred. Network values are described in UIAS.XML<sup>[42]</sup>.

## 2.1.18 - Is IC Member

### 2.1.18.1 - Person Entity (PE) Compliance Statements

The value for the **@isICMember** attribute MUST be **"true"** or **"1"** if the PE is a person employed by, assigned or detailed to, or acting for an element within the IC, as documented by the respective organization and approved by the organization's senior leadership and as defined by Executive Order (E.O.) 12333, *United States Intelligence Activities* <sup>[8]</sup>.

The value for the **@isICMember** attribute MUST be **"false"** or **"0"** if the PE is not a member of the IC.

### 2.1.18.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@isICMember** attribute MUST be **"true"** or **"1"** if the NPE is owned by, assigned to, or acting for an element within the IC as defined by E.O.12333<sup>[8]</sup>.

The value for the **@isICMember** attribute MUST be **"false"** or **"0"** if the NPE is not operating under an IC element.

## 2.1.19 - Lifecycle Status

### 2.1.19.1 - Person Entity (PE) Compliance Statements

Not applicable.

## 2.1.19.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **lifeCycleStatus** attribute MUST be "**DEV**" if the NPE is in a development life cycle phase.

The value for the **lifeCycleStatus** attribute MUST be "**TEST**" if the NPE is in a test life cycle phase.

The value for the **lifeCycleStatus** attribute MUST be "**PROD**" if the NPE is in a production life cycle phase.

The value for the **lifeCycleStatus** attribute MUST be "**SUNSET**" if the NPE is in a sunset/to-be-retired life cycle phase.

## 2.1.20 - Originating Network

### 2.1.20.1 - Person Entity (PE) Compliance Statements

The value for the **@originatingNetwork** attribute MUST reflect the network or domain from which the entity's identity originates.

### 2.1.20.2 - Non-Person Entity (NPE) Compliance Statements

The value for the **@originatingNetwork** attribute MUST reflect the network or domain from which the entity's identity originates.

## 2.1.21 - Region

### 2.1.21.1 - Person Entity (PE) Compliance Statements

The token(s) in the **@region** attribute MUST specify the authorized regions assigned to an entity (based on the entity's position, job, or area of responsibility) needed to determine the protected resources the entity may access.

The token(s) in the **@region** attribute MUST be provided by one of the community core ICAM services operated and maintained by the ICAM-SP.

The ANAN token in the **@region** attribute MUST have one or more other **@regions** provisioned. Both of the following criteria MUST be true:

- If a PE has one or more **@regions** provisioned it MUST have "**ANAN**".

AND

- "**ANAN**" MUST NOT be the only **@region** provisioned for a PE.

## 2.1.21.2 - Non-Person Entity (NPE) Compliance Statements

The token(s) in the **@region** attribute MUST specify the authorized regions assigned to the entity (based on the entity's scope or function) needed to determine the protected resources the entity may access.

The token(s) in the **@region** attribute MUST be provided by one of the community core ICAM services operated and maintained by the ICAM-SP.

The ANAN token in the **@region** attribute MUST have one or more other **@regions** provisioned. Both of the following criteria MUST be true:

- If an NPE has one or more **@regions** provisioned it MUST have **"ANAN"**.

AND

- **"ANAN"** MUST NOT be the only **@region** provisioned for an NPE.

## 2.1.22 - Role

### 2.1.22.1 - Person Entity (PE) Compliance Statements

The token(s) in the **@role** attribute MUST specify the authorized roles assigned to an entity (based on the entity's position, job, or area of responsibility) needed to determine access to protected resources.

The token(s) in the **@role** attribute MUST be tokens found in the Extensible Markup Language (XML) CVE Encoding Specification for Role.

The token(s) in the **@role** attribute MUST be provided by either AccessIT! for C2S Workflow Administrator role or another community core ICAM services operated and maintained by the ICAM-SP.

### 2.1.22.2 - Non-Person Entity (NPE) Compliance Statements

The token(s) in the **@role** attribute MUST specify the authorized roles assigned to an entity (based on the entity's scope or function) needed to determine access to protected resources.

The token(s) in the **@role** attribute MUST be tokens found in the XML CVE Encoding Specification for Role.

The token(s) in the **@role** attribute MUST be provided for NPEs by one of the community core ICAM services operated and maintained by the ICAM-SP.

### 2.1.22.3 - Authorized Law Enforcement Personnel (ALEP)

The **@Role** value of **"ALEP"** MUST be provisioned for a PE when the assigned GSA Job Series is one of the following:

- 1811 (Criminal Investigation Series)
- 1801 (General Inspection, Investigation, Enforcement, and Compliance Series)
- 1881 (Customs and Border Protection Interdiction Series)
- 1896 (Border Patrol Enforcement Series)
- 132 (Intelligence Series) when the Admin Organization or Duty Organization is any of the following:
  - Federal Bureau of Investigation (FBI)
  - Department of Homeland Security (DHS)
  - United States Drug Enforcement Administration (DEA)
  - Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
  - Department of Justice (DOJ)

The **@Role** value of "**ALEP**" for a NPE is provisioned when the agency assigns it per their requirements.



## Note

For example, the FBI may use the *CVE Encoding Specification for Role* (ROLE.CES<sup>[41]</sup>) Enterprise namespace taxonomy as follows:

- Role Scope ::= ENT (Enterprise Role)
- Role Organization ::= 1\*255 (ALPHA/DIGIT/"-" , in this case it will be FBI)
- Role Name ::= 1\*255 (ALPHA/DIGIT/"-" , in this case it will be ALEP)
- Implementation: ENT-FBI-ALEP

## 2.1.23 - Topic

### 2.1.23.1 - Person Entity (PE) Compliance Statements

The token(s) in the **@topic** attribute **MUST** specify the authorized topics assigned to an entity (based on the entity's authorized position, job, or area of responsibility) needed to determine the protected resources the entity may access.

The token(s) in the **@topic** attribute **MUST** be provided by one of the community core ICAM services operated and maintained by the ICAM-SP.

The ANY token in the **@topic** attribute **MUST** have one or more other **@topics** provisioned. Both of the following criteria **MUST** be true:

- If a PE has one or more @**topics** provisioned it MUST have "**ANY**".

AND

- "**ANY**" MUST NOT be the only @**topic** provisioned for a PE.

## 2.1.23.2 - Non-Person Entity (NPE) Compliance Statements

The token(s) in the @**topic** attribute MUST specify the authorized topics assigned to the entity (based on the entity's scope or function) needed to determine the protected resources the entity may access.

The token(s) in the @**topic** attribute MUST be provided by one of the community core ICAM services operated and maintained by one of the ICAM-SP.

The ANY token in the @**topic** attribute MUST have one or more other @**topics** provisioned. Both of the following criteria MUST be true:

- If an NPE has one or more @**topics** provisioned it MUST have "**ANY**".

AND

- "**ANY**" MUST NOT be the only @**topic** provisioned for an NPE.

## 2.2 - AAS and AS Operation Compliance Statements

### 2.2.1 - Attribute Latency

IC ASs or their operators MUST fill attribute requests with attributes retrieved no more than 24 hours earlier from supporting AASs, irrespective of latency from the actual source system from which the information originates.

IC ASs or their operators MUST publish to the IC Enterprise details on how the AAS provides accurate and current attributes to the AS, including AAS policy on attribute cache periods (up to 24 hours).

AAS policy on attribute cache periods (up to 24 hours) MUST be met unless technical difficulties prevent attribute updates.

For any updated attributes received, the AS MUST use those updates, and not cached attributes, to fill attribute requests.

### 2.2.2 - Publish & Subscribe

ASs that cache attributes from AASs that provide publish and subscribe services MUST subscribe to and use those services to receive updates to attributes the AS may have cached.

For any updated values received, the AS MUST immediately begin using the updated values to fulfill attribute requests.

An AS MUST only subscribe to the published AAS attributes for which they have a need.

An AAS MUST only send the published attributes for which the receiving AS has subscribed.

### **2.2.3 - Attribute Protection**

IC ASs or their operators MUST collect only the information necessary to perform the attribute service.

IC ASs or their operators MUST comply with the requirements of the Privacy Act and other statutory and policy limitations on the collection, maintenance and sharing of Personally Identifiable Information (PII) and other personal data (e.g., health data), in accordance with ICD 107, *Civil Liberties, Privacy and Transparencies* [\[21\]](#), and the policies and procedures of the IC element that owns or operates the AS.

Appendix A Feature Summary

The following tables summarize major features by version for UIAS-APCS. 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<sup>[15]</sup> manual has an implementation date of one year after issuance).

Table 2 - 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-APCS Feature Summary

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

Table 3 - UIAS-APCS Feature Comparison V2018-DEC to V2021-NOV

| Required date | Feature                                                                        | V2018-DEC | V2019-MAR | V2019-SEP | V2021-NOV |
|---------------|--------------------------------------------------------------------------------|-----------|-----------|-----------|-----------|
|               | Support hierarchical Sensitive Compartmented Information (SCI)s                | N         | N         | F         | F         |
|               | Incorporate DOD Special Access Program Control Office (SAPCO) guidance on SAPs | N         | N         | N         | F         |

A.1.2. Features from V2016-FEB to V2018-DEC

Table 4 - UIAS-APCS Feature Comparison V2016-FEB to V2018-DEC

| Required date | Feature | V2016-FEB | V2018-DEC |
|---------------|---------|-----------|-----------|
|---------------|---------|-----------|-----------|

## Appendix B Change History

The following table summarizes the version identifier history for this Data Encoding Specification (DES).

**Table 5 - DES Version Identifier History**

| Version  | Date              | Purpose                                                                                                                           |
|----------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 2016-FEB | February 18, 2016 | Initial Release.                                                                                                                  |
| 2018-DEC | Dec 10, 2018      | Routine revision to technical specification. For details of changes, see <a href="#">Section B.4 - V2018-DEC Change Summary</a> . |
| 2019-MAR | March 8, 2019     | Routine revision to technical specification. For details of changes, see <a href="#">Section B.3 - V2019-MAR Change Summary</a> . |
| 2019-SEP | September 6, 2019 | Routine revision to technical specification. For details of changes, see <a href="#">Section B.2 - V2019-SEP Change Summary</a> . |
| 2021-NOV | December 3, 2021  | Routine revision to technical specification. For details of changes, see <a href="#">Section B.1 - V2021-NOV Change Summary</a> . |

### B.1 - V2021-NOV Change Summary

Significant drivers for Version 2021-NOV include:

- IC Marking System Register and Manual 30 August 2019<sup>[14]</sup>
- Community change requests.

[Table 6](#) summarizes the changes made to this technical specification from Version 2019-SEP to Version 2021-NOV.

**Table 6 - V2021-NOV Change History**

| # | Change                                                                         | Artifacts Changed | Compatibility Notes   |
|---|--------------------------------------------------------------------------------|-------------------|-----------------------|
| 1 | Corrected sub-compartment to subcompartment. (CR-2019-164).                    | Documentation     | No impact to systems. |
| 2 | Federating ANAN and ANY values for Topic and Region attributes. (CR-2019-141). | Documentation     | No impact to systems. |
| 3 | Addition of ALEP Role to ROLE Attribute. (CR-2019-013)                         | Documentation     | No impact to systems. |

| # | Change                                                                    | Artifacts Changed | Compatibility Notes                        |
|---|---------------------------------------------------------------------------|-------------------|--------------------------------------------|
| 4 | Add UCNI and DCNI to UIAS CVE for handlingControls. (CR-2021-006)         | Documentation     | No impact to systems.                      |
| 5 | Updated fineAccessControls for NATO. (CR-2020-005)                        | Documentation     | No impact to systems.                      |
| 6 | Modify handling of SAP accesses to support DOD SAPCO rules. (CR-2021-024) | Documentation     | Impact to data being entered into systems. |

## B.2 - V2019-SEP Change Summary

Significant drivers for Version 2019-SEP include:

- Technical Integration Committee Next Generation (TIC NG)

[Table 7](#) summarizes the changes made to this technical specification from Version 2019-MAR to Version 2019-SEP.

**Table 7 - V2019-SEP Change History**

| # | Change                                                                                                      | Artifacts Changed | Compatibility Notes                                                                                                                                                                          |
|---|-------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Modified rules for tokens in the @fineAccessControls attribute to support hierarchical SCIs. (CR-2019-016). | Documentation     | 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 | Update chapters for consistency with other specifications. (CR-2019-096).                                   | Documentation     | No impact to systems.                                                                                                                                                                        |

## B.3 - V2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Consolidation of security control related specifications.

[Table 8](#) summarizes the changes made to this technical specification from Version 2018-DEC to Version 2019-MAR.

**Table 8 - V2019-MAR Change History**

| # | Change                                                                                                                                                                            | Artifacts Changed | Compatibility Notes                                                                                                                                                  |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Updated <b>@countryOfAffiliation</b> to align with E.O 12968, and update handling controls section to specify practice statements for individual handling controls. (CR-2018-106) | Documentation     | Changes criterion for <b>@countryOfAffiliation</b> and established criterion for handling controls systems will have to ensure they comply with the new definitions. |
| 2 | Updated documentation to use the specification framework. (CR-2018-126)                                                                                                           | Documentation     | No impact to systems.                                                                                                                                                |

## B.4 - V2018-DEC Change Summary

Significant drivers for Version 2018-DEC include:

- Consolidation of security control related specifications.

[Table 9](#) summarizes the changes made to this technical specification from Version 2016-FEB to Version 2018-DEC.

**Table 9 - V2018-DEC Change History**

| # | Change                                                                                                                      | Artifacts Changed | Compatibility Notes                                                                                                |
|---|-----------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------|
| 1 | Update definitions of <b>@fineAccessControls</b> to clarify what Flat means for SCI and clarify other values. (CR-2018-150) | Documentation     | Changes criterion for <b>@fineAccessControls</b> systems will have to ensure they comply with the new definitions. |

## 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 <b>@mn:region</b> attribute as listed in “CVerenumMNRegion”. The token was added in an effort to move complexity from the ABAC system to the subject provisioning system by denormalizing the Region list. <b>"ANAN"</b> 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 <b>"ANAN"</b> to the subject, we now have a simple string match.</p> <p>On a resource when <b>"ANAN"</b> is selected, it is the most permissive while still requiring some provisioning of "any" region.</p> <p>The subject provisioning system <b>MUST</b> provision <b>"ANAN"</b> when the user has at least one region. When any region is provisioned <b>"ANAN"</b> must be selected also and cannot be the only region selected.</p> |
| ANY             | <p>A token in the <b>@mn:issue</b> attribute as listed in “CVerenumMNIssue”. The token was added in an effort to move complexity from the ABAC system to the subject provisioning system by denormalizing the Issue list. <b>"ANY"</b> 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 <b>"ANY"</b> to the subject, we now have a simple string match.</p> <p>On a resource when <b>"ANY"</b> is selected, it is the most permissive while still requiring some provisioning of "any" issue.</p> <p>The subject provisioning system <b>MUST</b> provision <b>"ANY"</b> when the user has at least one issue. When any issue is provisioned <b>"ANY"</b> 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> <a href="#">[33]</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| attribute value | <p>The complete string of data entered into an attribute. For example, if <b>@attribute="ABC DEF GHI"</b> then the value of <b>@attribute</b> is full string "ABC DEF GHI"</p> <p>Source:</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> <p>Source: NIST SP 800-205, <i>Attribute Considerations for Access Control Systems</i> <a href="#">[39]</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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> <a href="#">[33]</a>.</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> <a href="#">[33]</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| audit                                | <ol style="list-style-type: none"> <li>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.</li> </ol> <p>Source: Committee on National Security Systems Instruction (CNSSI) 4009, <i>National Information Assurance (IA) Glossary</i> <a href="#">[5]</a>.</p> <ol style="list-style-type: none"> <li>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.</li> </ol> <p>Source: Intelligence Community Standard (ICS) 500-27, <i>Intelligence Community Standard for Collection and Sharing of Audit Data</i> <a href="#">[31]</a></p> |
| authorized                           | <p>Access privileges granted to a user, program or process or the act of granting these privileges.</p> <p>Source: CNSSI 4009 <a href="#">[5]</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| compartmentalization                 | <p>A non-hierarchical grouping of information used to control access to data more finely than with hierarchical security classification alone. Hierarchical security classifications are the UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET indicators of the sensitivity of information. Compartmentalization or fine access</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | control attributes include SCIs, SAPs, NATO markings, and AEA markings that require special access approvals.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                         | Source: CNSSI 4009 <sup>[5]</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 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> <sup>[5]</sup>.</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> <sup>[38]</sup>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| need-to-know            | <ul style="list-style-type: none"> <li>A determination within the executive branch in accordance with directives issued pursuant to E.O. 13526<sup>[10]</sup> that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.</li> </ul> <p>Source: Executive Order (E.O.) 13526, <i>Classified National Security Information</i> <sup>[10]</sup>.</p> <ul style="list-style-type: none"> <li>A determination that personnel require access to classified information to perform or assist in authorized governmental functions. The need-to-know determination is made based on the functions of an agency or the roles and responsibilities of personnel in the course of their official duties.</li> </ul> <p>Source: ISOO 32 CFR Parts 2001 and 2003, <i>Classified National Security Information; Final Rule</i> <sup>[37]</sup>.</p> |
| Non-Person Entity (NPE) | <p>Entity related to Information Technology (IT), e.g., hardware objects (physical entities/devices) and software objects (virtual/logical entities).</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> <sup>[33]</sup>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Person Entity (PE)      | <p>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).</p> <p>Source: NIST SP 800-56Br1, <i>Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1</i> <sup>[38]</sup>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Source: CNSSI 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25* <sup>[4]</sup>

## 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* <sup>[7]</sup>.

## token

A token datatype is an XML schema language built-in datatype. A token datatype is a string datatype that contains one or more strings separated by a single space, e.g., `ism:releasableTo='USA AFG FVEY'` is an example of an ISM attribute that has token datatype. A token datatype contains no leading or trailing spaces, no carriage returns, no line feeds and no tab characters. The individual strings in an element or attribute that is a token datatype are referred to as tokens. In the `ism:releasableTo='USA AFG FVEY'` example, the tokens are 'USA', 'AFG' and 'FVEY'. In contrast, the value of `ism:releasableTo` is the entire string 'USA AFG FVEY'.

Source: <https://www.w3.org/TR/2004/REC-xmlschema-2-20041028/#token>

## Appendix D List of Abbreviations

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

|       |                                                     |
|-------|-----------------------------------------------------|
| 2PI   | Second Party Integree                               |
| AAS   | Authoritative Attribute Source                      |
| ABAC  | Attribute Based Access Control                      |
| ACCM  | Alternative Compensatory Control Measures           |
| AICP  | Authorized IC Person                                |
| AO    | Authorizing Official                                |
| APCS  | Attribute Practice Compliance Statement             |
| APS   | Attribute Practice Statement                        |
| AS    | Attribute Service                                   |
| ATF   | Bureau of Alcohol, Tobacco, Firearms and Explosives |
| ATO   | Authority To Operate                                |
| CNSSI | Committee on National Security Systems Instruction  |
| CRL   | Certificate Revocation List                         |
| CVE   | Controlled Vocabulary Enumeration                   |
| DEA   | United States Drug Enforcement Administration       |
| DES   | Data Encoding Specification                         |
| DHS   | Department of Homeland Security                     |
| DN    | Distinguished Name                                  |
| DNI   | Director of National Intelligence                   |
| DOD   | Department of Defense                               |
| DOJ   | Department of Justice                               |
| E.O.  | Executive Order                                     |
| FBI   | Federal Bureau of Investigation                     |
| FD&R  | Foreign Disclosure & Release                        |
| IC    | Intelligence Community                              |

|            |                                                               |
|------------|---------------------------------------------------------------|
| ICAM       | Identity, Credential, and Access Management                   |
| ICAM-SP    | Identity, Credential, and Access Management Service Providers |
| IC CIO     | Intelligence Community Chief Information Officer              |
| ICD        | Intelligence Community Directive                              |
| IC EA      | Intelligence Community Enterprise Architecture                |
| IC ESB     | Intelligence Community Enterprise Standards Baseline          |
| IC ICAM SC | IC Identity, Credential, and Access Management Subcommittee   |
| IC IE      | IC Information Environment                                    |
| IC ITE     | Intelligence Community Information Technology Enterprise      |
| ICPG       | Intelligence Community Program Guidance                       |
| ICS        | Intelligence Community Standard                               |
| ISM        | Information Security Markings                                 |
| ISOO       | Information Security Oversight Office                         |
| IT         | Information Technology                                        |
| NATO       | North Atlantic Treaty Organization                            |
| NPE        | Non-Person Entity                                             |
| NTK        | Need-To-Know Metadata                                         |
| PE         | Person Entity                                                 |
| PII        | Personally Identifiable Information                           |
| PKI        | Public Key Infrastructure                                     |
| SAP        | Special Access Program                                        |
| SAPCO      | Special Access Program Control Office                         |
| SAT        | Sensitive Analytical Techniques                               |
| SCI        | Sensitive Compartmented Information                           |
| SSP        | System Security Plan                                          |
| TIC NG     | Technical Integration Committee Next Generation               |
| USP        | United States Person                                          |

XML

Extensible Markup Language

## Appendix E Bibliography

[1] AUDIT.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Enterprise Audit Exchange (AUDIT.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/Og5CcLk> (case sensitive – Oscar golf 5 Charlie charlie Lima kilo )

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

[2] BOE.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Body Of Evidence (BOE.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/NRyKd26> (case sensitive – November Romeo yankee Kilo delta 2 6 )

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

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

[3] CNSSI 1254

Committee on National Security Systems. *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*. 1254. 31 August 2016.

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

[4] 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>

[5] 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>

[6] 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>

[7] ES 2016-00816

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

[8] 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>
- [9] E.O. 12968  
The White House. *Executive Order 12968 - Access to Classified Information*. Federal Register, Vol. 60, No. 151. 7 August 1995.  
Available online at: <https://www.federalregister.gov/documents/1995/08/07/95-19654/access-to-classified-information>
- [10] E.O. 13526  
The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.  
Available online at: <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>
- [11] 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/uZz5I7T> (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>
- [12] 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>
- [13] 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.
- [14] 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>
- [15] 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>
- [16] IC PKI CRL  
Office of the Director of National Intelligence. *Intelligence Community (IC) Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profiles*. Version 2.9.13 FINAL. 13 April 2021.

Available online Intelink-TS at: <https://go.ic.gov/bEA2UCP> (case sensitive – bravo Echo Alpha 2 Uniform Charlie Papa )

[17] IC Memo 2010-0460

Office of the Director of National Intelligence. *Instructions for Designation of Authorized IC Personnel Approvers*. September 2010.

Available online Intelink-TS at: <https://go.ic.gov/zd6Qg0o> (case sensitive – zulu delta 6 Quebec golf 0 oscar )

[18] 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>

[19] 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>

[20] IC ICAM SC TOR

Office of the Director of National Intelligence. *IC Identity, Credential, & Access Management Subcommittee - Terms of Reference*.

[21] ICD 107

Office of the Director of National Intelligence. *Civil Liberties, Privacy and Transparency*. Intelligence Community Directive 107. 28 February 2018.

Available online at: <https://www.dni.gov/files/documents/ICD/ICD-107.pdf>

[22] 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>

[23] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima )

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_500.pdf](http://www.dni.gov/files/documents/ICD/ICD_500.pdf)

[24] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <https://go.ic.gov/fTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra )

Available online at: [http://www.dni.gov/files/documents/ICD/ICD\\_501.pdf](http://www.dni.gov/files/documents/ICD/ICD_501.pdf)

[25] 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>

[26] ICD 906

Office of the Director of National Intelligence. *Controlled Access Programs*. Intelligence Community Directive 906. 17 October 2015.

Available online at: <https://www.dni.gov/files/documents/ICD/ICD906.pdf>

[27] 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 )

[28] ICPG 500.2

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

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

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

[29] 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](https://www.dni.gov/files/documents/ICPG/02-25-20_ODNI_ICPG_IC_Personnel_Security_Database_Scattered_Castles_20-00078_U.pdf)

[30] 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>

[31] 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 )

[32] 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 )

[33] 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 )

[34] IETF-RFC 4514

OpenLDAP Foundation. *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*. June 2006.

Available online at: <https://www.ietf.org/rfc/rfc4514.txt>

[35] ISM.ACES

Office of the Director of National Intelligence. *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*.

Available online Intelink-TS at: <https://go.ic.gov/rOG2Bjt> (case sensitive – romeo Oscar Golf 2 Bravo juliet tango )

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

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

[36] 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>

[37] ISOO 32 CFR Parts 2001 and 2003

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information; Final Rule*. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. 28 June 2010.

Available online at: <http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf>

[38] 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>

[39] 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>

[40] 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>

[41] 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>

[42] UIAS.XML

Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1 )

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

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

[43] 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>

[44] 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>

## 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](mailto:ic-standards-support@odni.gov).

## Appendix G IC CIO Approval Memo

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

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

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the Intelligence Community Enterprise Standards Baseline (IC ESB) as defined in ICS 500-20<sup>[30]</sup>.