Intelligence Community Technical Specification

Data Encoding Specification for IC Full Service Directory Schema

Version 2016-SEP

September 9, 2016

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This technical specification codifies the set of Lightweight Directory Access Protocol (LDAP) attributes that Intelligence Community (IC) elements are expected to provide to the Intelligence Community Full Service Directory (IC FSD). It will facilitate the availability, accuracy, and standardization of these attributes across the IC TS/SCI enterprise, building a consistent basis for capabilities including directory services, email functions, and attribute-based access control decisions. The specification defines:

- IC-specific Schema and supporting objectClasses for IC Entities
- Attributes, both standard and IC-defined, that must be managed by IC Elements
- Controlled vocabulary for those attributes whose use requires standard values
- Authentication requirements for accessing the attributes.

1.2 - Scope

This specification is applicable to the IC and access to the information produced by, stored within, or shared throughout the IC's IC TS/ SCI information domain as defined in Intelligence Community Policy Guidance (ICPG) 500.1, *Digital Identity*.[12] Identity attributes defined at the enterprise level within the IC may have relevance outside the scope of the IC; however, prior to applying outside of this defined scope, the models should be closely scrutinized and differences separately documented and assessed for applicability.

This document lists IC-specific Schema and supporting objectClasses for IC Entities; Attributes, both standard and IC-defined, that must be managed by IC Elements; Controlled vocabulary for those attributes whose use requires standard values; and Authentication requirements for the attributes.

Intelligence Community Full Service Directory Attributes are assigned per persona. A persona is an electronic identity that is unambiguously associated with a single person or non-person entity (NPE). A single person or NPE may have multiple personas, with each persona being managed by the same or by different organizations (e.g., a DNI contractor who is also an Army reservist).

1.3 - Background

The IC FSD provides enterprise-level directory services to both IC personnel and applications on the US IC TS/ SCI fabric. This IC-wide directory is made possible by
IC elements sharing attributes amongst themselves via the IC FSD's hub and spoke replication model. Under this model, each participating IC element is responsible for providing attributes about its personnel and non-person entities such as servers and service applications. The IC FSD supports:

- The IC White Pages, a web-based service with which IC TS/ SCI users can locate colleagues' email addresses, phone numbers, and other organizational information [1]

- The sharing of user email attributes between IC Elements' internal address books, to facilitate cross-agency and S/MIME-enabled email capabilities

- The sharing of user email attributes with the IC TS/ SCI Allied Collaborative Shared Services environment, to facilitate US-5 Eyes collaboration

- Attribute-Based Access Control, by resources directly accessing an IC FSD Border Directory or indirectly via the Unified Authorization and Attribute Service (UAAS) Federation, within which the IC FSD serves as a repository for authoritative authorization attributes.

The IC FSD also provides two attributes that indicate where attributes can be passed (e.g., JWICS, NSANET, ACSS):

- **resourceSecurityMark** – an overall data classification and control marking for each entry in the IC FSD (e.g. UNCLASSIFIED//FOUO).

- **icNetworks** - a releasability attribute specifying the IC-approved network on which the object is allowed to be passed (e.g., JWICS, NSANET, ACSS).

Planning and partnerships between IC Elements have made current IC Full Service Directory capabilities possible. However, as the IC FSD has become increasingly important, some limitations have been identified that must be addressed to realize the IC FSD's full potential. The following limitations affect consistent identity management, Attribute-Based Access Control capabilities, and overall user productivity:

- Instances of attributes populated incompletely by IC Elements

- Instances of attributes populated with inconsistent values, making resource providers unable to rely on them for access control

- Lack of clear authentication requirements to secure access to attributes, which has become increasingly important with the dissemination of attributes to other environments, makes some elements hesitant to share and populate certain attributes.

IC elements again demonstrated partnership by addressing these limitations together, resulting in this document, which:

- Formally documents the IC FSD attribute schema

- Increases the number of IC FSD attributes required for each entry

- Defines attribute names

- Identifies the attributes requiring controlled values

- Defines those controlled values

- Establishes authentication requirements for each attribute

[1] URL = http://directory.csp.ic.gov/eGuide/index.html

- Ensures interoperability with the IC enterprise authorization attributes exchanged through the Unified Authorization and Attribute Service federation, as documented in *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set.* [28]

1.4 - Enterprise Need

The IC FSD provides a replication hub for identity attribute related information. The IC FSD replicates identity information to and from IC agency border directories. This centralized repository of select IC user information is automatically populated from each participating agency's border directories and consolidated in the IC FSD. The IC FSD is critical to the operation of many programs within the IC. The IC FSD provides an industry standard (LDAP) interface for attribute retrieval of multiple records at one time.

Defining the set of IC enterprise directory attributes and values for sharing through LDAP supports the opportunity for consistent and assured information sharing across the enterprise. Implementers of IC FSD require coordination of attribute definitions. This requires the usage of standardized attribute names and values when exchanging attributes between agencies.

Enterprise needs and requirements for this specification can be found in the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance:

- IC Information Technology Enterprise (IC ITE):
  - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan[5]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[9]
  - Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity[12]
  - Intelligence Community Policy Guidance (ICPG) 500.2, Attribute-based Authorization and Access Management[13]
  - Intelligence Community Standard (ICS) 500-13, Intelligence Community Optimized Network Email Display Name Format[15]
  - Intelligence Community Standard (ICS) 500-15, Intelligence Community Optimized Network Email Full Service Directory[16]
  - Intelligence Community Standard (ICS) 500-29, IC Digital Identifier[18]
  - Intelligence Community Standard (ICS) 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources[19]

1.5 - Audience and Applicability

The primary audience for this document includes those responsible for implementing and managing the capabilities that create, provide, modify, store, exchange, search, display, or further process IC FSD attributes.

This document applies to all attributes shared via the IC FSD about IC Entities on the IC TS/ SCI fabric, with the majority of attributes pertaining to IC Persons.

Each IC FSD entry about a person provides attributes about a "persona", which means that one person may have several IC FSD records, each with distinct attributes about that persona. A

persona is an electronic identity that can be unambiguously associated with a single person. A single person may have multiple personas, with each persona being managed by the same or by different organizations (such as a DNI contractor who is also an Army reservist).

Since the concept of personas applies to IC FSD records, it is an important concept to remember when reading portions of the IC FSD schema which reference persons.

The governance of this specification and the data it describes, including any requirement to use this specification or prohibition thereof, is explicitly outside the scope of this specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance,* [17] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element. *Department of Defense Instruction (DODI) 8310.01, Information Technology Standards in the DoD*,[1] requires DoD elements to use the DoD IT Standards Registry (DISR).

Use of this specification must be consistent with applicable Federal statutes, Executive Orders, Presidential Directives, Attorney General approved guidelines, IC Policy, IC element policies, established concepts of operation, agreements, contractual obligations, etc. However, the determination of any such requirements or restrictions is the sole responsibility of each implementing entity. Implementers may wish to consult the Office of General Counsel for their cognizant agency to determine existing requirements and restrictions for the use of this DES and to determine if new agreements or policy changes are required related to the use of this DES.

1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

1.6.1 - Language

When appearing in all capital letters in this technical specification, the keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels.” [21] When these words appear in regular case, they are meant in their natural-language sense.

1.6.2 - Typography

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

1.6.3 - Terminology

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

1.7 - 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 direct and transitive 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 specifications listed in Table 1 will be shown in Figure 1; however not all specifications listed in Figure 1 may appear in Table 1. Figure 1 is to aid users in gaining a general understanding of all transitive dependencies.

Table 1 - Dependencies

Name	Dependency Description
RFC 2251, Lightweight Directory Access Protocol (v3)[22]	Internet Engineering Task Force standard for Lightweight Directory Access Protocol
Geopolitical Entities, Names, and Codes[4]	U.S. Government profile of ISO 3166 Codes for the representation of names of countries and their subdivisions
Intelligence Community Certificate Policy V4.4[7]	Policy for Intelligence Community Public Key Infrastructure
CVE Encoding Specification for US Agency Acronyms (USAgency.CES.V2016-SEP+)[29]	This specification does not depend on a specific version of US Agency (USAgency.CES); USAgency.CES versions later than version 2016-SEP MAY be used. The minimum version was based on a technical dependency; The addition of the audit routing organization CVE.
XML Data Encoding Specification for Unified Identity Attribute Set (UIAS.XML.V2016-SEP+)[28]	This specification does not depend on a specific version of Unified Identity Attribute Set (UIAS.XML); UIAS.XML versions later than version 2016-SEP MAY be used. The minimum version was based on a technical dependency; The addition of the new attribute auditRoutingOrganization and use of new CVEs for entityType and lifeCycleStatus.

Name	Dependency Description
CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES.V2015-MAY+)[27]	This specification does not depend on a specific version of ISM Country Codes and Tetragraphs (ISMCAT.CES); ISMCAT.CES versions later than version 2015-MAY MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.
XML Data Encoding Specification for Virtual Coverage (VIRT.XML.V1+)[30]	This specification does not depend on a specific version of Virtual Coverage (VIRT.XML); VIRT.XML versions later than version 1 MAY be used. The minimum version was based on the earliest non-retired version; ESB 16-1 was used for determining the version.

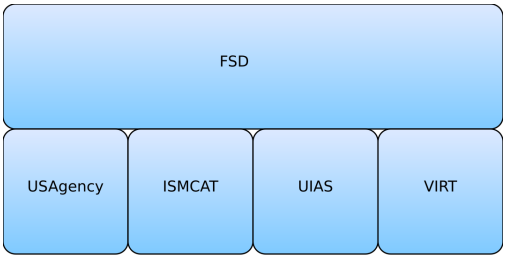

Figure 1 : Related Specifications

1.7.1 - Standalone and Convenience Packages

The standalone package of this specification does not include the specifications that it is dependent on since there may be more recent versions of those specifications available. There is a convenience package of the specification that includes the most recent versions, minus the schemas and Schematron, of all direct dependent specifications at the time the package is generated. Transitive dependencies are intentionally excluded for this specification. It is anticipated that this convenience package will be updated when any of the dependent specifications change; however, it will not be signed as a formal package. In order to obtain all the necessary standalone packages, this specification's dependencies will have to be traversed and obtained.

Convenience packages convey all dependencies pre-packaged together. When trying to mix and match versions that have not been pre-packaged together, there may be risk that a particular combination may not be compatible, especially when mixing with versions of specifications that were not available at the time of a specification's release.

1.8 - Conformance

This specification defines a business object to which an implementation and a subsequent deployment MUST conform.

For an implementation to conform to this specification, it MUST adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

Within this document, class diagrams are normative for the class name, attribute names, attribute multiplicity, attribute visibility, and class inheritance. All tables describing the class attributes are normative for descriptions of the attributes and informative for all other aspects of the class.

Additional guidance that is either classified or has handling controls can be found in separate annexes, which are distributed to the appropriate networks and environments, as necessary. Systems and services operating in those environments must consult the appropriate annexes.

1.9 - Version Policies

The version numbering for this specification is defined by a year-month structure (e.g., YYYY-MMM). This provides a temporal representation of when the specification was released.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions are based upon three components (data attributes, user attributes, and access control policies) and are held together by the context in which the access control decision is made. The context itself includes various elements, such as the environment, temporal state, and method of access, that together provide the Where, When, and How details of the access request. The context, together with the user making the request and the data/repository/ application being requested (the Who and What respectively), make up the framework that supports an access control decision. Access Policy SHOULD be constrained to use data attributes, user attributes, and context information. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. An entity MUST meet all criteria in the framework to be granted access. The concept of the access control decision framework is depicted in Figure 2.

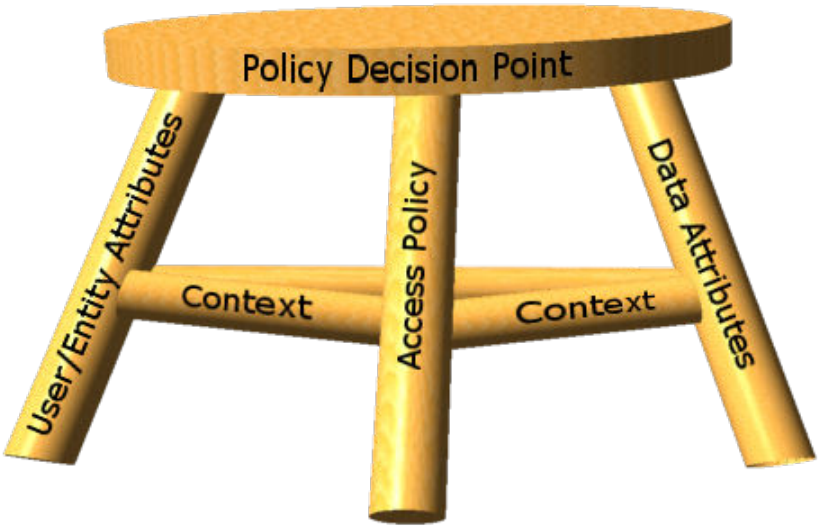

Figure 2 : Three-legged Stool of Access Decisions

All of these parts come together to create a tri-legged stool of access control. When a stool is missing one of the components of its frame, it is unable to function properly. The same is true of access control. Without each component of the framework, access control falls apart. Each component is crucial to make accurate, reliable, and automated access control decisions. Each IC CIO document will address a piece of the framework of access control decisions.

This specification falls into the user attributes leg of the access control framework. User attribute specifications include:

- Full Service Directory (FSD)[3]
- Unified Identity Attribute Set (UIAS.XML)[28]

2.2 - IC FSD System Description

The IC FSD is based on the X.500 standard for electronic directory services. It is a fully replicated directory framework in which each participating IC element holds a full and accurate copy of the IC FSD content. The architecture is based on a hub and spoke model, with the central IC FSD serving as the master replication hub. IC elements are the authoritative provider of their personnel's directory data. Other sources may provide data only in coordination with the IC element. When a participating IC element adds, deletes, or modifies data in its border directory, the IC FSD detects and replicates the updated content to itself and all other border directories. This full replication scenario strengthens the IC FSD's disaster recovery posture. Figure 3 below depicts the IC FSD replication model.

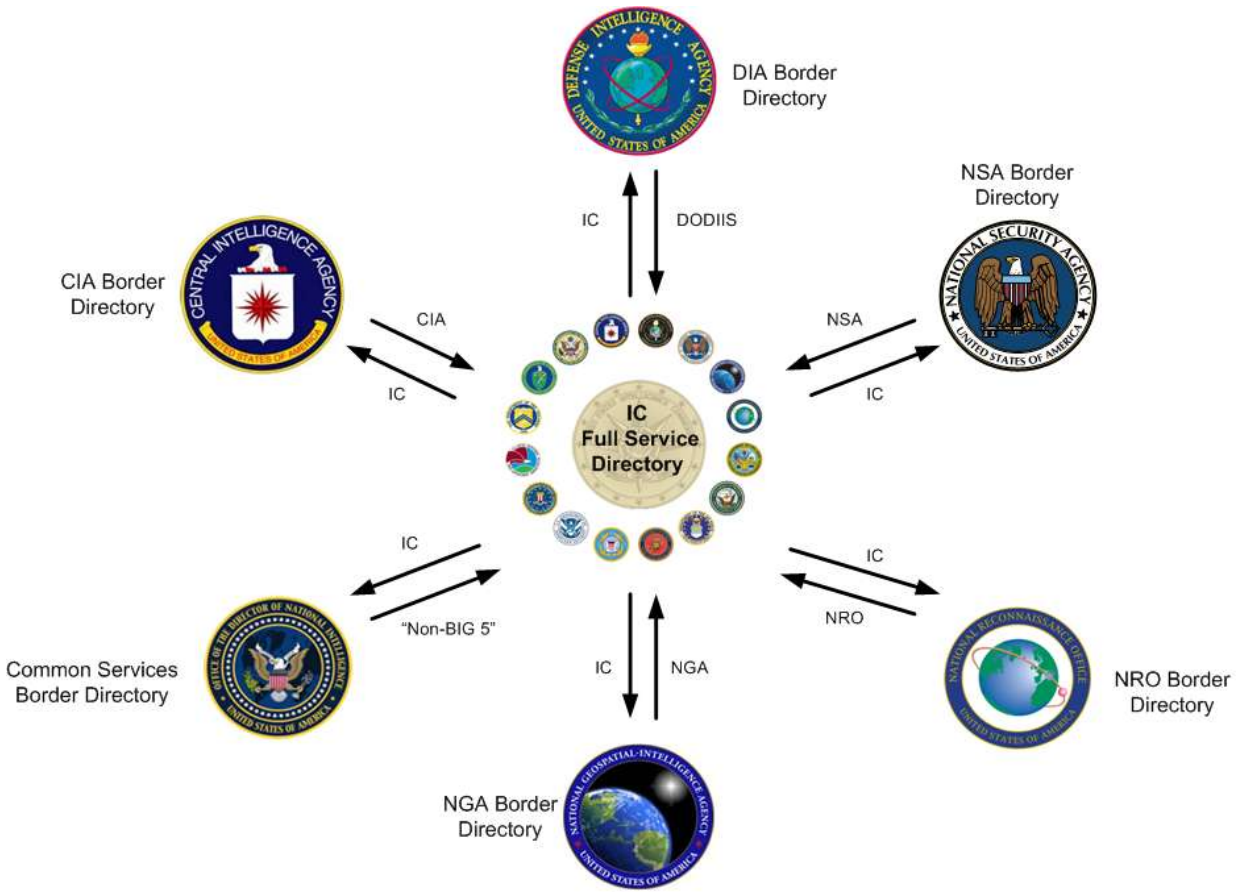

Figure 3 : IC FSD Replication

The IC FSD, acting in its role as the master replication manager, is designed to only communicate with authorized border directories. The IC FSD always initiates communications with the authorized border directories; no IC Element border directory can initiate communication with the IC FSD.

The IC FSD maintains redundancy through two geographically diverse locations, each with three servers. The first server communicates with authorized border directories (currently CIA, DIA,

NGA, NRO, and NSA), retrieving updates hourly and immediately replicating any changes to the other border directories. The second server replicates information to and from the Common Services border directory. The third server provides local redundancy and, in the event of a complete failure of one of the first two servers, can serve as the replication engine for either.

2.3 - IC FSD Policy Statements

2.3.1 - Duplicate Entries

IC elements that replicate information via their IC FSD border directories to the IC FSD shall provide only records that contain IC Email addresses in address spaces that they own, or to which they have been delegated administrative responsibility for populating the IC FSD. IC elements shall not contribute a record to their IC FSD border directory with an IC Email address in an address space that they do not control or manage.

2.3.2 - Account Disablement

The identity and attributes associated with an inactive user shall not be replicated to an agency's border directory for update to the IC FSD White Pages. A user shall be considered inactive when the user has not accessed the account for ninety (90) calendar days unless the agency indicates an exception to the 90 day rule for that user, allowing them to remain active.

Chapter 3 - Definitions, Interfaces, and Constraints

The normative LDAP schemas are found in Chapter 5 - IC FSD Schema and Chapter 8 - IC FSD Schema for PKI Root and Intermediate Certificate Authorities. Constraints on attributes are listed in Chapter 6 - Attribute Status

Chapter 4 - Conformance Validation

An implementation of FSD MUST be conforming to the schema's provided and abide by the cardinality constraints.

Chapter 5 - IC FSD Schema

The IC FSD Schema is defined by several standard LDAP objectClasses and two derived auxiliary objectClasses that designate additional attributes about IC Entities. IC Entities fall into the categories of an “IC Person” or “IC Non-Person Entity,” with the latter being used to define objects such as servers, devices, appliances, applications, and services that exist within the IC enterprise.

5.1 - IC FSD Schema for IC Person

Attributes that characterize an “IC Person” are defined through a combination of standard LDAP objectClasses and a derived IC-defined objectClass called “**icOrgPerson**”. The specific implementation of an “**icOrgPerson**” objectClass may vary depending on the directory server in use, so the definition of the actual objectClass is left to the discretion of the implementing IC Element. The suggested objectClass hierarchy used to hold the various attributes about an IC Person is as follows:

```
objectclass (2.5.6.6 NAME ‘person’ SUP top

      DESC ‘RFC2256: Person’

      STRUCTURAL

      MUST ( sn $ cn )

      MAY ( userPassword $ telephoneNumber $ seeAlso $

            description)

      )
```

```
objectclass (2.5.6.7 NAME ‘organizationalPerson’ SUP person

      DESC ‘RFC2256: organizationalPerson’

      STRUCTURAL

      MAY ( title $ x121Address $ registeredAddress $

            generationQualifier $ personalTitle $

            destinationIndicator $ preferredDeliveryMethod $

            telexNumber $ teletexTerminalIdentifier $

            telephoneNumber $ internationaliSDNNumber $

            facsimileTelephoneNumber $ street $ postOfficeBox $

            postalCode $ postalAddress $

            physicalDeliveryOfficeName $ ou $ st $ l )

      )
```

```
objectclass (2.16.840.1.113730.3.2.2 NAME ‘inetOrgPerson’
      DESC ‘RFC2798: Internet Organizational Person’
      SUP organizationalPerson
      STRUCTURAL
      MUST ( employeeType )
      MAY ( audio $ businessCategory $ carLicense $
            departmentNumber $ displayName $
            employeeNumber $ givenName $ homePhone $
            homePostalAddress $ initials $ jpegPhoto $
            labeledURI $ mail $ manager $ mobile $ o $ pager $
            photo $ roomNumber $ secretary $ uid $
            userCertificate $ x500uniqueIdentifier $
            preferredLanguage $ userSMIMECertificate $
            userPKCS12 )
      )
```

```
objectclass (2.16.840.1.101.2.2.3.73 NAME ‘icOrgPerson’
      DESC ‘Intelligence Community Person’
      SUP inetOrgPerson
      STRUCTURAL
      MUST ( auditRoutingOrganization $ countryOfAffiliation $
dutyOrganization $
          dn $ adminOrganization $ isICMember $
            icNetworks $ resourceSecurityMark )
      MAY ( icEmail $ secureTelephoneNumber $ companyName $
            internetEmail $ niprnetEmail $ siprnetEmail $
            rank $ buildingName $ countryName $
            militaryTelephoneNumber $ preferredName $
            secureFacsimileNumber $ expertCountry $
```

```
            expertFunctionalArea $ productionManager $

            personaUID $ dutySubOrganization)

      )
```

5.2 - IC FSD Schema for IC Non-Person Entity

Attributes that characterize an IC Non-Person Entity are defined through a combination of standard LDAP objectClasses and a derived IC-defined objectClass called "**icOrgServer**". The "**icOrgServer**" objectClass used to hold the various attributes about an IC Non-Person Entity is defined below. As is the case with "**icOrgPerson**", the actual objectClass hierarchy used to implement "**icOrgServer**" is left to the discretion of the implementing IC element.

```
objectclass (2.16.840.1.101.2.2.3.74 NAME 'icOrgServer'

      DESC 'Intelligence Community Non-Person Entity'

      SUP <implementation specific>

      STRUCTURAL

      MUST ( auditRoutingOrganization $ cn $ dutyOrganization $

        adminOrganization $ isICMember $ dn $

        ATOStatus $ lifeCycleStatus $ givenName $

        countryOfAffiliation $ employeeType $

             uid $ userCertificate $ resourceSecurityMark $

             icNetworks $ serverPOC $ userCertificate )

      MAY ( description $ serverURL $ icServerAddress )

      )
```

5.3 - IC FSD Attribute Definitions

The following section defines a collection of attributes from the objectClasses described in sections 3.1 and 3.2 that participating IC Elements should attempt to support so that the IC FSD can realize its full potential as an IC Enterprise-level directory service. Each attribute is described using the formal attribute definition format as defined in *RFC 2252 Section 4.2*.[23] A tabular format will also be used to provide additional information and a controlled vocabulary (when appropriate) for each attribute.

In terms of IC Element provisioning requirements, this specification organizes attributes about an IC entity into mandatory, policy-based, optional or deprecated categories and is further described in Chapter 4.

This specification establishes three authentication tiers, providing graded authentication for attributes of varying sensitivity and is further described in Chapter 5.

All attributes are assumed to be MULTI-VALUE unless specifically identified as SINGLE-VALUE.

Several of the designated attributes are “children” of the SUPERIOR (SUP) attribute, **name**. As a result, each child attribute inherits the properties of **name**, described as follows:

```
attributetype ( 2.5.4.41 NAME ‘name’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

5.3.1 - adminOrganization

This attribute specifies the home or administrative organization affiliation with which the entity (person or non-person) is associated.

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

```
attributetype (`OID TBD` NAME `adminOrganization`

        EQUALITY  caseignoreMatch

        SUBSTR  caseignoreSubstringMatch

        SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

         )
```

Table 2 - adminOrganization

Attribute Name	adminOrganization
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Admin Organization
Description	Reflects the home organization of the entity

Attribute Name	adminOrganization
Allowable Values	Summation of two sets: • Values listed in *XML CVE Encoding Specification for US Agency Acronyms* [29] • Values listed in table Table 3
Example	DIA
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

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

Table 3 - Foreign Government adminOrganization Countries

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

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

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

5.3.2 - auditRoutingOrganization

This attribute indicates the organizations to which audit records are to be forwarded. There MUST be at least one value present and there MAY be up to two values present. Allowable values can be found in CVEnumAuditRoutingOrg. This attribute is applicable to both Persons and Non-Persons.

```
attributetype (`OID TBD` NAME `auditRoutingOrganization`

        EQUALITY  caseignoreMatch

        SUBSTR  caseignoreSubstringMatch

        SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        MULTI-VALUE

        )
```

Table 4 - auditRoutingOrganization

Attribute Name	auditRoutingOrganization
Reference	IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Audit Routing Organization
Description	This attribute indicates the one or two organization to which audit records are to be forwarded.
Allowable Values	Values listed in *XML CVE Encoding Specification for US Agency Acronyms* [29] from the CVE CVEnumAuditRoutingOrg
Example	CIA
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

5.3.3 - ATOStatus

This attribute indicates the Authority to Operate (ATO) status for the non-person entity. As defined by ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* [11] ATO is approved for operation at a particular level of security in a particular environment, with the established level of risk associated with operating the system. This includes ATOs with waivers, which can be derived based upon the approved necessary conditions of the approving authority.

The **ATOStatus** attribute is only applicable for non-person entities.

```
attributetype (`OID TBD` NAME `ATOStatus`

        EQUALITY  booleanmatch
```

```
        SYNTAX    1.3.6.1.4.1.1466.115.121.1.7

        SINGLE-VALUE

        )
```

Table 5 - ATOStatus

Attribute Name	ATOStatus
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgServer
Friendly Name	Authority to Operate Status
Description	This attribute indicates the Authority to Operate (ATO) status for the Non-Person entity.
Allowable Values	Boolean True/False (false by default)
Example	True
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.4 - buildingName

```
attributetype ( 0.9.2342.19200300.100.1.48 NAME ‘buildingName’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 6 - buildingName

Attribute Name	buildingName
Reference	RFC 1274[20]
Object Class	icOrgPerson
Friendly Name	Physical Building Name
Description	Defines the building name associated with an IC Person
Allowable Values	IC Person’s community recognized building name

Attribute Name	buildingName
Examples	LX2 NBP-304
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.5 - c, countryName

```
attributetype ( 2.5.4.6 NAME ( 'c' 'countryName' ) SUP name SINGLE-VALUE )
```

Table 7 - c, countryName

Attribute Name	c, countryName
Reference	RFC 2256[24]
Object Class	icOrgPerson
Friendly Name	Physical Country
Description	Country where IC Person's physical work facility is located
Allowable Values	Two-letter country codes as identified by Geopolitical Entities, Names, and Codes Standard (GENC) [4]
Examples	US AU
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

5.3.6 - cn, commonName

```
attributetype ( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

Table 8 - cn, commonName

Attribute Name	cn, commonName
Reference	RFC 2256[24]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Common Name
Description	This is the X.500 **commonName** attribute, which contains a name of an object. When the object corresponds to an IC Entity, it typically matches the CN component of the entity's Distinguished Name in its/his/her PKI certificate.

Attribute Name	cn, commonName
Allowable Values	For the IC, the *Intelligence Community Public Key Infrastructure Interface Specification* [8] provides the basis for specifying Common Names for both IC Person and Non-Person Entities. Consult Chapter 6 - CERTIFICATE DISTINGUISHED NAME (DN) SCHEMA of the IC PKI Interface Specification for allowable values.
Examples	Smith John A dijasmi John A Smith webserver.dni.ic.gov
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.7 - companyName

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.148 NAME 'companyName'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 9 - companyName

Attribute Name	companyName
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Company Name
Description	Company name of an IC Person with CTR **employeeType**
Allowable Values	Legal name of company provided by authoritative source
Example	Company Inc.
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

5.3.8 - countryOfAffiliation

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

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

```
attributetype (`OID TBD` NAME `countryOfAffiliation`

          EQUALITY  caseignoreMatch

          SUBSTR  caseignoreSubstringMatch

          SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 10 - countryOfAffiliation

Attribute Name	countryOfAffiliation
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Country of Affiliation
Description	Reflects the citizenship or affiliation of the entity
Allowable Values	Values listed in *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs[27] (ISMCAT)* from the CVE CVEnumISMCATResponsibleEntity excluding "NATO"
Example	USA
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.9 - displayName

```
attributetype ( 2.16.840.1.113730.3.1.241 NAME 'displayName'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE
```

```
        )
```

Table 11 - displayName

Attribute Name	displayName
Reference	RFC 2798,[25], Intelligence Community Standard 500-13, *Intelligence Community Optimized Network E-Mail Display Name Format* [15]
Object Class	inetOrgPerson
Friendly Name	Display Name
Description	Preferred name of an IC Person to be used when displaying entries. Especially useful in displaying a preferred name within a one-line summary list, such as the case with an IC email client.
Allowable Values	Format as defined in ICS 500-13[15]: Last Name<space>First Name<space>Middle Name/ Initial<space>Generation ID<space> Personal Title<space>Duty Organization<space> Duty Sub-Organization<space> Citizenship<space>Employee Type In terms of corresponding directory attribute names: <sn givenName initials generationQualifier personalTitle dutyOrganization dutySubOrganization countryOfAffiliation employeeType> In cases where multiple values are available for **countryOfAffiliation**, the value "USA" should be listed last, and the values separated by spaces.
Example	Smith John M Jr Maj DIA PACOM USA MIL
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.10 - dn, distinguishedName

```
attributetype ( 2.5.4.3 NAME ( 'dn' 'distinguishedName' ) SUP name )
```

Table 12 - dn, distinguishedName

Attribute Name	dn, distinguishedName
Reference	RFC 2256[24], Intelligence Community Standard 500-29, *Intelligence Community Digital Identifier* [18]
Object Class	icOrgPerson / icOrgServer

Attribute Name	dn, distinguishedName
Friendly Name	Distinguished Name
Description	This is the X.500 **distinguishedName** attribute, which contains the entity's Distinguished Name from the PKI certificate
Allowable Values	For the IC, the *Intelligence Community Public Key Infrastructure Interface Specification* [8] provides the basis for specifying Common Names for both IC Person and Non-Person Entities. Consult Chapter 6 - CERTIFICATE DISTINGUISHED NAME (DN) SCHEMA of the IC PKI Interface Specification for allowable values
Examples	cn=Doe John A jdoe, ou=DNI, o=U.S Government, c=US cn=webserver.dni.ic.gov, ou=DNI, o=U.S. Government, c=US
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.11 - dutyOrganization

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

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

In support of Second Party Integrees, the **dutyOrganization** should represent the US government sponsoring agency.

```
attributetype (`OID TBD` NAME `dutyOrganization`

        EQUALITY  caseignoreMatch

          SUBSTR  caseignoreSubstringMatch

          SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 13 - dutyOrganization

Attribute Name	dutyOrganization
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Duty Organization

Attribute Name	dutyOrganization
Description	Reflects the assigned organization of the entity
Allowable Values	Values listed in *XML CVE Encoding Specification for US Agency Acronyms* [29]
Example	DNI
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.12 - dutySubOrganization

This attribute specifies the sub-organization which the IC Person is representing.

```
attributetype (`OID TBD` NAME `dutySubOrganization`

        EQUALITY  caseignoreMatch

          SUBSTR  caseignoreSubstringMatch

          SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 14 - dutySubOrganization

Attribute Name	dutySubOrganization
Reference	DES for the IC Full Service Directory Schema,[3] Intelligence Community Standard 500-13, *Intelligence Community Optimized Network E-Mail Display Name Format* [15]
Object Class	icOrgPerson
Friendly Name	Duty Sub-Organization
Description	Reflects the assigned sub organization of the entity
Allowable Values	Agency defined authoritative sub-organization of the IC Person's duty organization
Example	PACOM, NCTC
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.13 - employeeType

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

This attribute is consistent with the **entityType** attribute in *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* [28]

```
attributetype ( 2.16.840.1.113730.3.1.4 NAME 'employeeType'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 15 - employeeType

Attribute Name	employeeType
Reference	RFC 2798,[25] DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	inetOrgPerson / icOrgServer
Friendly Name	Employee Type
Description	Reflects the type of the entity
Allowable Values	Values found in XML CVE for Entity Type, CVEnumUIASEntity-Type.XML.
Example	GOV
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

Per RFC 2798 this LDAP attribute is Multi-Valued, however, the IC FSD implementation is Single-Valued.

Further clarification of NPE attribute definitions are below:

SVR - A hardware or software server system upon which other software systems reside and execute. Such systems typically provide support for and management of those other software systems. Such server systems include, but are not limited to, physical servers, virtual servers or server environments, application servers, and web servers. Note that while similar, end-point devices (DEV) and network devices (NET) are special purpose systems which have been called out separately.

SVC - A software system that performs specific functionality which can be generally viewed as self-encapsulated or decomposed and managed as discrete functional components. The intent is to deliver functional capabilities to systems, users or other software systems. Such software systems can include, but are not limited to, services, widgets, applications, and appliances whose primary functionality is delivery of functional capabilities as opposed to networking capabilities.

DEV - A hardware or software end-point device from which users or other external entities access systems or networks. End-point devices, while typically used to access networks or other key systems directly, can operate as standalone entities if required by mission use and enabled by functional capabilities. End-point devices can include, but are not limited to, workstations, laptops, smart phones, tablets, and sensors.

NET - A hardware or software device directly supportive of networking operations. This does not include those end-point devices and servers which leverage and are dependent upon the networking operations. Networking operation devices include, but are not limited to, firewalls, bridges, routers, switches, concentrators, DNS servers, and appliances whose primary function is the support and management of such operations.

5.3.14 - expertCountry

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.149 NAME ‘expertCountry’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 16 - expertCountry

Attribute Name	expertCountry
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Expert Country
Description	3-letter country code describing an IC Person’s expertise area
Allowable Values	Values listed in *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs[27] (ISMCAT)* from the CVE CVEnumISMCATResponsibleEntity excluding “NATO”
Example	USA
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.15 - expertFunctionalArea

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.150 NAME 'expertFunctionalArea'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 17 - expertFunctionalArea

Attribute Name	expertFunctionalArea
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Expert Functional Area
Description	IC Person's functional area expertise
Allowable Values	DIA Intelligence Functional Code
Example	IFC1000
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.16 - facsimileTelephoneNumber

```
attributetype ( 2.5.4.23 NAME ( 'facsimileTelephoneNumber' 'fax' )

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

        )
```

Table 18 - facsimileTelephoneNumber

Attribute Name	facsimileTelephoneNumber
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Unclassified Telephone FAX Number
Description	IC Person's unclassified/commercial FAX number
Allowable Values	<Country Code (if applicable)> (Area Code) <Prefix> <Suffix>
Example	(703) 561-0000
Provisioning	Optional
Authentication	Network

Attribute Name	facsimileTelephoneNumber
Single/Multi	MULTI-VALUE

5.3.17 - generationQualifier

```
attributetype ( 2.5.4.44 NAME 'generationQualifier' SUP name )
```

Table 19 - generationQualifier

Attribute Name	generationQualifier
Reference	RFC 2256[24]
Object Class	*Implementation Dependent*
Friendly Name	Generational Qualifier
Description	The generationQualifier attribute contains the part of the IC Person's name which typically is the suffix
Allowable Values	JR, SR, III, IV, etc.
Examples	JR SR
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.18 - givenName

```
attributetype ( 2.5.4.42 NAME 'givenName' SUP name )
```

Table 20 - givenName

Attribute Name	givenName
Reference	RFC 2256[24]
Object Class	inetOrgPerson / icOrgServer
Friendly Name	First Name
Description	The **givenName** attribute is used to hold the part of a person's name which is not his or her surname nor middle name. For Non-Person Entities, the **givenName** attribute is used for the name of the service.
Allowable Values	For IC Persons, this should reflect a person's legal first name
Examples	Joseph Katherine
Provisioning	Mandatory
Authentication	Network

Attribute Name	givenName
Single/Multi	MULTI-VALUE

5.3.19 - icEmail

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.154 NAME ‘icEmail’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 21 - icEmail

Attribute Name	icEmail
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	IC Email Address
Description	IC Email address of an IC Person
Allowable Values	Official email address of the IC Person as given by the email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.20 - icNetworks

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.160 NAME ‘icNetworks’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 22 - icNetworks

Attribute Name	icNetworks
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson / icOrgServer
Friendly Name	IC Networks
Description	**icNetworks** is used to specify what networks an object may exist on. This attribute provides the capability for other security domains to be listed. Directory objects include both IC Person and Non-Person Entities.
Allowable Values	Values listed in *VIRTCVEnums.pdf* in XML *Data Encoding Specification for Virtual Coverage* [30]
Examples	ACSS NSANET
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

5.3.21 - icServerAddress

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.2.200 NAME 'icServerAddress'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 23 - icServerAddress

Attribute Name	icServerAddress
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgServer
Friendly Name	IP Address
Description	IP Address of IC Non-Person Entity
Allowable Values	Valid IPv4 or IPv6 address

Attribute Name	icServerAddress
Examples	10.1.2.3 3ffe:1900:4545:3:200:f8ff:fe21:67cf
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.22 - initials

```
attributetype ( 2.5.4.43 NAME 'initials' SUP name )
```

Table 24 - initials

Attribute Name	initials
Reference	RFC 2256[24]
Object Class	inetOrgPerson
Friendly Name	Middle Initial
Description	IC Person's middle initial(s)
Allowable Values	Single, first letter of the middle name(s) with no periods, if one is available
Examples	K L N, etc.
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.23 - internetEmail

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.155 NAME 'internetEmail'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 25 - internetEmail

Attribute Name	internetEmail
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Internet Email Address
Description	Internet email address of an IC Person
Allowable Values	Official Internet email address of the IC Person as given by the email provider
Example	jsmith@ugov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.24 - isICMember

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( ‘OID TBD’ NAME ‘isICMember’

        EQUALITY booleanMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.7

        SINGLE-VALUE

        )
```

Table 26 - isICMember

Attribute Name	isICMember
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgPerson / icOrgServer
Friendly Name	IC Membership
Description	Value that denotes an individual’s IC membership status for ICD 501[10] purposes
Allowable Values	Boolean true/false (false by default)
Example	False
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

The **isICMember** attribute is a flag that reflects whether the persona is a member of the Intelligence Community.

This is a Boolean attribute that will be set to false by default. Null values for this attribute should be treated as false by applications using this attribute for access control purposes.

Each IC organization will make the determination as to which of its users will have a true value for this attribute. This process will be documented by the organization and approved by the organization's senior leadership and general counsel. The ODNI will then review and approve the process. The following, from Executive Order 12333,[2] is used as general guidance in making this determination: an IC member is "a person employed by, assigned or detailed to, or acting for an element within the IC".

5.3.25 - l, localityName

```
attributetype( 2.5.4.7 NAME ( 'l' 'localityName' ) SUP name )
```

Table 27 - l, localityName

Attribute Name	l, localityName
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Physical City
Description	IC Person's physical city or location name
Allowable Values	City or location name
Example	Fairfax
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.26 - languageProficiency

IC-defined attribute. Suggested definition for implementation by IC Element.

This attribute is deprecated and should no longer be used.

```
attributetype ( 2.16.840.1.101.2.2.1.151 NAME 'languageProficiency'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 28 - languageProficiency

Attribute Name	languageProficiency
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Language Proficiency
Description	Individual's evaluated ability to read, write and speak a second language other than English. Based on Defense Language Proficiency Test.
Allowable Values	Contains a reading level and listening level based on the Defense Language Proficiency Test results
Examples	Reading Level 1 Listening Level 0+
Provisioning	Deprecated
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.27 - lifeCycleStatus

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

```
attributetype (`OID TBD` NAME `lifeCycleStatus`

          EQUALITY  caseignoreMatch

          SUBSTR  caseignoreSubstringMatch

          SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

          SINGLE-VALUE

        )
```

Table 29 - lifeCycleStatus

Attribute Name	lifeCycleStatus
Reference	DES for the IC Full Service Directory Schema,[3] ICD 501,[10] Executive Order 12333,[2] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set[28]
Object Class	icOrgServer
Friendly Name	Life Cycle Status
Description	Indicates the life cycle phase in which the entity is operating
Allowable Values	Values found in XML CVE for Life Cycle Status, CVEnum-UIASLifeCycleStatus.XML.

Attribute Name	lifeCycleStatus
Example	DEV
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.28 - mail

```
attributetype ( 0.9.2342.19200300.100.1.3 NAME (‘mail’ ‘rfc822Mailbox’ )

        EQUALITY caseIgnoreIA5Match

        SUBSTR caseIgnoreIA5SubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

        )
```

Table 30 - mail

Attribute Name	mail
Reference	RFC 2798[25]
Object Class	inetOrgPerson
Friendly Name	Email Address
Description	Email address of an object on a particular network
Allowable Values	Official email address of the IC Person as given by the email provider
Example	jsmith@intelink.ic.gov
Provisioning	Policy-based
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.29 - militaryTelephoneNumber

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.120 NAME ‘militaryTelephoneNumber’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE
```

```
        )
```

Table 31 - militaryTelephoneNumber

Attribute Name	militaryTelephoneNumber
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	DSN Voice Telephone Number
Description	IC Person's Defense Switched Network (DSN) phone number
Allowable Values	Authoritative DSN telephone number provided by the user's home agency
Example	867-5309
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.30 - nationality-Extended

IC-defined attribute. Suggested definition for implementation by IC Element.

This attribute is deprecated and should no longer be used.

```
attributetype ( 2.16.840.1.101.2.2.1.61 NAME 'nationality-Extended'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 32 - nationality-Extended

Attribute Name	nationality-Extended
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Citizenship
Description	3-letter country code describing an IC Person's citizenship
Allowable Values	Values listed in *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs[27] (ISMCAT)* from the CVE CVEnumISMCATResponsibleEntity excluding "NATO"

Attribute Name	nationality-Extended
Examples	USA GBR AUS
Provisioning	Deprecated
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.31 - niprnetEmail

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.156 NAME ‘niprnetEmail’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 33 - niprnetEmail

Attribute Name	niprnetEmail
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	NIPRNet Email Address
Description	NIPRNet email address of an IC Person
Allowable Values	Official NIPRNet email address of the IC Person as given by the DoD email provider
Example	jsmith@af.mil
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.32 - personalTitle

```
attributetype ( 0.9.2342.19200300.100.1.40 NAME ‘personalTitle’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 34 - personalTitle

Attribute Name	personalTitle
Reference	RFC 1274[20]
Object Class	*Implementation Dependent*
Friendly Name	Personal Title
Description	The **personalTitle** attribute contains the personal title of an IC Person
Allowable Values	Dr, Mr, Ms, Prof, Gen, Adm etc.
Examples	Mr Dr Ms Adm
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.33 - personaUID

```
attributetype (  2.16.840.1.101.2.2.1.161 NAME ‘personaUID’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 35 - personaUID

Attribute Name	personaUID
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Persona Unique Identifier
Description	Unique IC identifier that is persistent for the life of the persona
Allowable Values	[A-Za-z]{2}[0-9]{5}
Examples	AB12345 XY56789

Attribute Name	personaUID
Provisioning	Policy-Based
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

The **personaUID** attribute is an alternate unique identifier associated with the Distinguished Name (DN) of the PKI Certificate that is used to both support use of identities in systems that cannot technically utilize the DN, and enable management of the relationship between those identifiers.

5.3.34 - postalAddress

```
attributetype ( 2.5.4.16 NAME ‘postalAddress’

        EQUALITY caseIgnoreListMatch

        SUBSTR caseIgnoreListSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.41

        )
```

Table 36 - postalAddress

Attribute Name	postalAddress
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Mailing Address
Description	IC Person’s address for receiving mail
Allowable Values	Full address used to receive mail
Example	1 Main St., Fairfax, VA 22030-4345
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.35 - postalCode

```
attributetype ( 2.5.4.17 NAME ‘postalCode’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 37 - postalCode

Attribute Name	postalCode
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Physical Postal Code
Description	IC Person's physical postal code
Allowable Values	XXXXX-XXXX (if last four digits are known)
Example	22030-4345
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.36 - preferredName

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.2.201 NAME 'preferredName'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 38 - preferredName

Attribute Name	preferredName
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Name the user prefers to be used in email communications
Description	Preferred name of an IC Person in email communications
Allowable Values	Preferred name of an IC Person in email communications
Example	Valid name
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

The **preferredName** attribute is an alternate displayable name (e.g., if the user goes by his/her middle name) for the user rather than **displayName** or **givenName**.

5.3.37 - productionManager

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.152 NAME ‘productionManager’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 39 - productionManager

Attribute Name	productionManager
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Production Manager
Description	IC Person’s Production Manager
Allowable Values	Distinguished Name of production manager
Example	cn=Smith Joe K Jr smithj,ou=test,o=u.s.government,c=us
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.38 - rank

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.133 NAME ‘rank’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 40 - rank

Attribute Name	rank
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Grade/Rank
Description	Individual's Office of Personnel Management (OPM) defined grade level
Allowable Values	OPM defined grades with two digit level required >Schedule<->Level<
Examples	GS-01 O-01 E-09 GG-09
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.39 - resourceSecurityMark

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.161 NAME  'resourceSecurityMark'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 41 - resourceSecurityMark

Attribute Name	resourceSecurityMark
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Resource Classification
Description	The classification and handling markings for the associated directory object for both IC Person and Non-Person Entities.
Allowable Values	Classification and handling marking banner as described in the latest published version of the IC Markings System Register and Manual[6]

Attribute Name	resourceSecurityMark
Examples	UNCLASSIFIED SECRET//NOFORN
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

5.3.40 - secureFacsimileNumber

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.127 NAME ‘secureFacsimileNumber’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

        SINGLE-VALUE

        )
```

Table 42 - secureFacsimileNumber

Attribute Name	secureFacsimileNumber
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Secure FAX Number
Description	IC Person’s secure/classified FAX number
Allowable Values	<Country Code> (Area Code) <Prefix> <Suffix>
Example	(703) 561-0000
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.41 - secureTelephoneNumber

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.128 NAME ‘secureTelephoneNumber’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 43 - secureTelephoneNumber

Attribute Name	secureTelephoneNumber
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	Secure Telephone Number
Description	IC Person's secure/classified phone number
Allowable Values	Authoritative secure telephone number provided by the user's home agency (seven digits in length)
Example	867-5309
Provisioning	Policy-based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.42 - serverPOC

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.2.201 NAME 'serverPOC'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 44 - serverPOC

Attribute Name	serverPOC
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgServer
Friendly Name	Server Point of Contact
Description	Name of an IC Person or IC Element organizational point of contact responsible for an IC Non-Person Entity

Attribute Name	serverPOC
Allowable Values	Name of an IC Person or IC Element organizational POC
Example	Valid name
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

5.3.43 - serverURL

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.2.202 NAME ‘serverURL’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 45 - serverURL

Attribute Name	serverURL
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgServer
Friendly Name	Server URL
Description	Uniform/Universal Resource Locator (URL) for IC Non-Person Entity when applicable
Allowable Values	Valid URL for IC Non-Person Entity
Example	https://myserver.dni.ic.gov
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

5.3.44 - serviceOrAgency

IC-defined attribute. Suggested definition for implementation by IC Element.

This attribute is deprecated and should no longer be used.

```
attributetype ( 2.16.840.1.101.2.2.1.82 NAME ‘serviceOrAgency’
```

```
        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 46 - serviceOrAgency

Attribute Name	serviceOrAgency
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Home Organization
Description	IC Person's owning organization (e.g., CIA, DIA, NGA, etc.) If military, this attribute contains the agency to which they are assigned. If a contractor, this attribute contains the agency that holds his or her contract. IC Non-Person Entity's owning organization.
Allowable Values	Commonly recognized agency acronym or identifier (CIA, DIA, DNI, NSA, NGA, NRO, DOJ, DOS, DOE, DHS, DOT, DOI, HHS, DOC, TREA, USDA, EOP, NRC, FRB, USCP, U.S. Congress, USAID, USPS, USPIS, NASA, EPA, DVA). DoD values not covered above will be determined and included in a later issuance of the Data Encoding Specification for the IC Full Service Directory Schema.
Examples	CIA, NSA, NGA, etc.
Provisioning	Deprecated
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.45 - siprnetEmail

IC-defined attribute. Suggested definition for implementation by IC Element:

```
attributetype ( 2.16.840.1.101.2.2.1.157 NAME 'siprnetEmail'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 47 - siprnetEmail

Attribute Name	siprnetEmail
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson
Friendly Name	SIPRNet Email Address
Description	SIPRNet email address of an IC Person
Allowable Values	Official SIPRNet email address of the IC Person as given by the email provider
Example	jsmith@intelink.sgov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

5.3.46 - sn

```
attributetype ( 2.5.4.4 NAME 'sn' SUP name )
```

Table 48 - sn

Attribute Name	sn
Reference	RFC 2256[24]
Object Class	Person
Friendly Name	Surname, Last Name
Description	This is the X.500 surname attribute, which contains the family name of a person.
Allowable Values	For IC Persons, this should reflect a person's legal last name
Examples	Smith Jones
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.47 - st, stateOrProvinceName

```
attributetype ( 2.5.4.8 NAME ('st' 'stateOrProvinceName' ) SUP name )
```

Table 49 - st, stateOrProvinceName

Attribute Name	st, stateOrProvinceName
Reference	RFC 2256[24]

Attribute Name	st, stateOrProvinceName
Object Class	organizationalPerson
Friendly Name	Physical State or Province
Description	IC Person's physical state or province name
Allowable Values	Standard Post Office abbreviation for state or province name
Example	VA
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.48 - street, streetAddress

```
attributetype ( 2.5.4.9 NAME ( 'street' 'streetAddress' )

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 50 - street, streetAddress

Attribute Name	street, streetAddress
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Physical Address
Description	IC Person's physical street address location
Allowable Values	Street address of a physical location
Example	1 Main St.
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

5.3.49 - telephoneNumber

```
attributetype ( 2.5.4.20 NAME 'telephoneNumber'

        EQUALITY telephoneNumberMatch

        SUBSTR telephoneNumberSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50
```

```
        )
```

Table 51 - telephoneNumber

Attribute Name	telephoneNumber
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Unclassified Telephone Number
Description	IC Person's unclassified/commercial phone number
Allowable Values	<Country Code (when applicable)> (Area Code) <Prefix> <Suffix>
Example	(703) 561-0000
Provisioning	Policy-based
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.50 - title

```
attributetype ( 2.5.4.12 NAME 'title' SUP name )
```

Table 52 - title

Attribute Name	title
Reference	RFC 2256[24]
Object Class	organizationalPerson
Friendly Name	Title
Description	The **title** attribute contains the title of an IC Person in the organizational context
Allowable Values	Major, Captain, Vice President, etc.
Examples	Major Captain Vice President
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.51 - uid

```
attributetype ( 0.9.2342.19200300.100.1.1 NAME ('uid' )

        EQUALITY caseIgnoreMatch
```

```
        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 53 - uid

Attribute Name	uid
Reference	RFC 2798[25]
Object Class	inetOrgPerson / icOrgServer
Friendly Name	Agency Unique ID
Description	IC Element assigned unique identifier for IC Person IC Element assigned unique identifier for IC Non-Person Entity
Allowable Values	IC Element unique identifiers
Examples	jsmith jsmith1234 12345, etc.
Provisioning	Optional, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

5.3.52 - userCertificate

userCertificate attributes must be transferred using the binary encoding, by requesting or returning the attributes via '**usercertificate; binary**'

```
attributetype ( 2.5.4.36 NAME 'userCertificate'

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.9 )

        )
```

Table 54 - userCertificate

Attribute Name	userCertificate
Reference	RFC 2256,[24] IC PKI Interface Specification[8]/>
Object Class	inetOrgPerson / icOrgServer
Friendly Name	PKI Certificate
Description	X.509-compliant PKI certificate issued to either an IC Person or IC Non-Person Entity
Allowable Values	Certificate issued by a trusted Certificate Authority operating within a trusted PKI

Attribute Name	userCertificate
Example	IC PKI certificate
Provisioning	Policy-based, Mandatory for NPE
Authentication	Network
Single/Multi	MULTI-VALUE

Chapter 6 - Attribute Status

This Data Encoding Specification for the IC Full Service Directory Schema organizes attributes about an “IC Person” or “IC Non-Person Entity” into mandatory, policy-based, optional or deprecated categories. These categories are defined as follows:

- Mandatory: Attributes that IC Elements MUST include in FSD records, without which the record will not be added to the IC FSD.
- Policy-based: Attributes which IC Elements MAY provide, if present in that IC Element’s internal directories.
- Optional: Attributes which IC Elements MAY provide to the IC FSD, depending on that IC Element’s security requirements and capabilities. Most optional attributes are not populated.
- Deprecated: Attributes that are present in the FSD schema, however, they are no longer needed. By policy the attribute is no longer passed between agency borders and the IC FSD.

Table 55 - IC Person Attributes Mandatory, Policy-Based, Optional or Deprecated

Attribute Name	Mandatory	Policy-Based	Optional	Deprecated
adminOrganization	X			
auditRoutingOrganization	X			
buildingName			X	
c, **countryName**			X	
cn, **commonName**	X			
companyName			X	
countryOfAffiliation	X			
displayName		X		
dn, **distinguishedName**	X			
dutyOrganization	X			
dutySubOrganization			X	
employeeType	X			
expertCountry			X	
expertFunctionalArea			X	
facsimileTelephoneNumber			X	
generationQualifier			X	
givenName	X			
icEmail		X		
icNetworks	X			
initials			X	

Attribute Name	Mandatory	Policy-Based	Optional	Deprecated
internetEmail		X		
isICMember	X			
l, localityName			X	
languageProficiency				X
mail		X		
militaryTelephoneNumber			X	
nationality-Extended				X
niprnetEmail		X		
personalTitle			X	
personaUID		X		
postalAddress			X	
postalCode			X	
preferredName			X	
productionManager			X	
rank			X	
resourceSecurityMark	X			
secureFacsimileNumber			X	
secureTelephoneNumber		X		
serviceOrAgency				X
siprnetEmail		X		
sn	X			
st, stateOrProvinceName			X	
street, streetAddress			X	
telephoneNumber		X		
title			X	
uid			X	
userCertificate		X		

Table 56 - IC Non-Person Entity Attributes Mandatory, Policy-Based, Optional or Deprecated

Attribute Name	Mandatory	Policy-Based	Optional	Deprecated
adminOrganization	X			
ATOStatus	X			
auditRoutingOrganization	X			
cn, commonName	X			

Attribute Name	Mandatory	Policy-Based	Optional	Deprecated
countryOfAffiliation	X			
dn, **distinguishedName**	X			
dutyOrganization	X			
employeeType	X			
givenName	X			
icNetworks	X			
icServerAddress			X	
isICMember	X			
lifeCycleStatus	X			
resourceSecurityMark	X			
serviceOrAgency				X
serverPOC	X			
serverURL			X	
uid	X			
userCertificate	X			

Note: givenName is not a mandatory attribute in terms of the **inetOrgPerson** objectClass. Compliance with the mandatory requirement for **givenName** is enforced through the replication agreements in place between the master IC FSD and participating IC Element Border directories.

Chapter 7 - Securing Access to IC FSD Attributes

This technical specification requires three authentication tiers, providing graded authentication for attributes of varying sensitivity. The three tiers are defined as follows:

- Network authentication
  - Permits end user access to content
  - Primarily used to support IC White Pages functionality, for attributes viewable by users through the IC White Pages
  - Relies on PKI authentication for web service access to content
  - Applies to attributes such as **name**, **countryOfAffiliation**, and **employeeType**.
- Strong user authentication
  - Permits end user access to content
  - Used for attributes more sensitive than those above
  - Requires users to present an IC PKI certificate
  - Applies to attributes such as **isICMember**, **streetAddress**, and **companyName**.
- Strong server/application authentication
  - Attributes which end users have no need to view in the IC FSD
  - Attributes used by servers and applications
  - Requires those servers and applications to present an IC PKI certificate
  - Applies to attributes such as **languageProficiency** and **certificateRevocationList**.

The IC FSD operator and IC elements are expected to maintain the authentication levels defined for each attribute, in whatever locations IC FSD data resides: border directories, element address books, etc. A reduction from three to two IC FSD authentication tiers is desired (eliminating network authentication and requiring strong user authentication to all user accessible content) if and when requirements are defined *and* supporting technology capabilities exist.

Table 57 - Securing Access to IC FSD IC Person Attributes

Attribute Name	Network	Strong User	Strong Server
adminOrganization			X
auditRoutingOrganization			X
buildingName		X	
c, **countryName**		X	

Attribute Name	Network	Strong User	Strong Server
cn, commonName	X		
companyName		X	
countryOfAffiliation	X		
displayName	X		
dn, distinguishedName	X		
dutyOrganization	X		
dutySubOrganization	X		
employeeType	X		
expertCountry			X
expertFunctionalArea			X
facsimileTelephoneNumber	X		
generationQualifier	X		
givenName	X		
icEmail	X		
icNetworks			X
initials	X		
internetEmail	X		
isICMember		X	
languageProficiency			X
l, localityName		X	
mail	X		
militaryTelephoneNumber	X		
nationality-Extended	X		
niprnetEmail	X		
personaUID			X
personalTitle	X		
postalAddress		X	
postalCode		X	
preferredName	X		
productionManager	X		
rank	X		
resourceSecurityMark			X
secureFacsimileNumber	X		
secureTelephoneNumber	X		
serviceOrAgency	X		

Attribute Name	Network	Strong User	Strong Server
siprnetEmail	X		
sn	X		
st, stateOrProvinceName		X	
street, streetAddress		X	
telephoneNumber	X		
title	X		
uid	X		
userCertificate	X		

Table 58 - Securing Access to IC FSD IC Non-Person Entity Attributes

Attribute Name	Network	Strong User	Strong Server
adminOrganization			X
ATOStatus			X
auditRoutingOrganization			X
cn, commonName	X		
countryOfAffiliation	X		
dn, distinguishedName	X		
employeeType	X		
givenName	X		
icNetworks			X
icServerAddress			X
isICMember		X	
lifeCycleStatus			X
serverPOC		X	
serverURL		X	
uid	X		
userCertificate	X		

The IC FSD operator and IC elements are expected to perform audit at a minimum as indicated through applicable security controls mandated by ICD 503[11] and subordinate policy documents, and as directed by IC-wide audit policies.

Chapter 8 - IC FSD Schema for PKI Root and Intermediate Certificate Authorities

For those IC Elements providing Certification Authority (CA) capabilities under the Intelligence Community Public Key Infrastructure (IC PKI), Cryptologic Agencies Domain (CAD) PKI, or other authorized PKIs, the following objectClass and associated attributes should be used as a basis to propagate critical CA information into the IC FSD architecture. This CA information is vital to the proper PK-enablement of services and applications within the IC TS/ SCI enterprise.

```
objectclass ( OID-TBD NAME ‘icCertificationAuthority’

      DESC ‘Intelligence Community Certification Authority’

      SUP <implementation specific>

      STRUCTURAL

      MUST ( certificateRevocationList $ cACertificate $

             icNetworks $ resourceSecurityMark
    )

      MAY ( crossCertificatePair $ authorityRevocationList )

      )
```

Note: the objectClass hierarchy in support of **icCertificationAuthority** may vary depending on the commercial Certificate Authority product implementation. In addition, the **crossCertificatePair** attribute is not applicable to the IC PKI.

8.1 - authorityRevocationList

The use and support of authority revocation lists by the IC PKI is not specifically identified in the IC PKI Certificate Policy or Interface Specifications.[7] [8] It currently is an optional attribute within the **icCertificationAuthority** objectClass.

This attribute SHOULD be stored and MUST be requested in binary form as ‘**authorityRevocationList;binary**’.

```
attributetype ( 2.5.4.38 NAME ‘authorityRevocationList’

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.9

        )
```

Table 59 - authorityRevocationList

Attribute Name	authorityRevocationList
Reference	RFC 2256[24]
Object Class	icCertificationAuthority
Friendly Name	Authority Revocation List
Description	An authority revocation list is a form of CRL containing certificates issued to certificate authorities, contrary to CRLs which contain revoked end-entity certificates
Allowable Values	Valid authority revocation list
Example	Any ARL issued by an authorized PKI Certificate Authority
Provisioning	Optional
Authentication	Network
Single/Multi	MULTI-VALUE

8.2 - certificateRevocationList

This attribute SHOULD be stored and MUST be requested in binary form as '**certificateRevocationList;binary**'.

```
attributetype ( 2.5.4.39 NAME 'certificateRevocationList'

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.9

        )
```

Table 60 - certificateRevocationList

Attribute Name	certificateRevocationList
Reference	RFC 2256,[24] RFC 5280[26]
Object Class	icCertificationAuthority
Friendly Name	Certificate Revocation List, CRL
Description	A CRL lists all unexpired certificates, within the scope of a specific Certificate Authority, that have been revoked for one of the reasons as defined in the *Intelligence Community Public Key Infrastructure Certificate Policy* [7]
Allowable Values	A valid X.509 V2 CRL as defined in RFC 5280[26] and the *Intelligence Community Public Key Infrastructure Interface Specification* [8]
Example	Any CRL issued by an authorized PKI Certificate Authority
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

8.3 - cACertificate

This attribute SHOULD be stored and MUST be requested in binary form as '**cACertificate;binary**'.

```
attributetype ( 2.5.4.37 NAME 'cACertificate'

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.8

        )
```

Table 61 - cACertificate

Attribute Name	cACertificate
Reference	RFC 2256,[24] RFC 5280[26]
Object Class	icCertificationAuthority
Friendly Name	CA Certificate
Description	A Certificate Authority's X.509 v3 compliant certificate
Allowable Values	A valid X.509 V3 certificate as defined in RFC 5280[26] and the *Intelligence Community Public Key Infrastructure Interface Specification* [8]
Example	Any authorized PKI Certificate Authority certificate
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

8.4 - icNetworks

```
attributetype ( 2.16.840.1.101.2.2.1.160 NAME 'icNetworks'

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 62 - icNetworks

Attribute Name	icNetworks
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson / icOrgServer, icCertificationAuthority
Friendly Name	IC Networks

Attribute Name	icNetworks
Description	**icNetworks** is used to specify what networks an object may exist on. This attribute provides the capability for other security domains to be listed. Directory objects include both IC Person and Non-Person Entities and Certification Authorities (CA).
Allowable Values	Values listed in *VIRTCVEnums.pdf* in XML *Data Encoding Specification for Virtual Coverage* [30]
Examples	ACSS NSANET
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	MULTI-VALUE

8.5 - resourceSecurityMark

```
attributetype ( 2.16.840.1.101.2.2.1.161 NAME  ‘resourceSecurityMark’

        EQUALITY caseIgnoreMatch

        SUBSTR caseIgnoreSubstringsMatch

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

        SINGLE-VALUE

        )
```

Table 63 - resourceSecurityMark

Attribute Name	resourceSecurityMark
Reference	DES for the IC Full Service Directory Schema[3]
Object Class	icOrgPerson / icOrgServer, icCertificationAuthority
Friendly Name	Resource Classification
Description	The classification and handling markings for the associated directory object for both IC Person and Non-Person Entities and Certification Authorities (CA).
Allowable Values	Classification and handling marking banner as described in the latest published version of the IC Markings System Register and Manual[6]
Examples	UNCLASSIFIED SECRET//NOFORN
Provisioning	Mandatory
Authentication	Strong Server

Attribute Name	resourceSecurityMark
Single/Multi	SINGLE-VALUE

Appendix A Feature Summary

The following table shows the version dependencies for FSD on other specifications. This table only includes direct dependencies. Transitive dependencies are ignored for FSD due the exclusions of schemas and Schematron from dependencies.

Table 64 - FSD Dependency over Time

Dependent Specification	V2016-SEP
USAgency	V2016-SEP+
ISMCAT	V2015-MAY+
VIRT	V1+
UIAS	V2016-SEP+

The following table summarizes major features by version for FSD and all dependent specs. The “Required date” is the date when systems should support a feature based on the specified driver. Executive Orders, ISOO notices, ICDs and other policy documents have a variety of effective dates.

Table 65 - 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. FSD Feature Comparison

Table 66 - FSD Feature Comparison

FSD Feature Comparison							
Required date	**Feature**	**V1**	**V2**	**V3**	**V2014-DEC**	**V2015-AUG**	**V2016-SEP**
	Map to UIAS	N	F	F	F	F	F
	Comply with ICS 500-13 Technical Amendment	N	N	F	F	F	F
	Added personaUID and distinguishedName (dn)	N	N	N	F	F	F
90 Days from Signature	Comply with IC FSD Policy Statements	N	N	N	F	F	F
	Update Chapter 6 for ARL, icNetworks, and resourceSecurityMarks	N	N	N	N	F	F
	Add attribute preferredName	N	N	N	N	F	F
	Replace Object Class certificationAuthority with icCertificationAuthority	N	N	N	N	F	F
	Support for other PKI CAs (e.g., CAD)	N	N	N	N	F	F

FSD Feature Comparison							
Required date	**Feature**	**V1**	**V2**	**V3**	**V2014-DEC**	**V2015-AUG**	**V2016-SEP**
	Add attribute auditRoutingOrganization	N	N	N	N	N	F

Appendix B Change History

Table 67 summarizes the version identifier history for this Data Encoding Specification.

Table 67 - Identifier History

Version	Date	Purpose
1	14 Dec 2011	Initial Release
2	16 August 2013	Updated to comply with appropriate attributes from *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1*
3	14 March 2014	Updated to comply with Technical Amendment to ICS 500-13
2014-DEC	4 December 2014	Added personaUID and distinguishedName (dn)
2015-AUG	13 August 2015	Routine revision to technical specification. For details of changes, see Section B.2 - V2015-AUG Change Summary
2016-SEP	9 September 2016	Routine revision to technical specification. For details of changes, see Table 68

B.1 - V2016-SEP Change Summary

Significant drivers for Version 2016-SEP include:

- Community Change Requests

Table 68 summarizes the changes made to this technical specification from Version 2015-AUG to Version 2016-SEP.

Table 68 - V2016-SEP Change History

Change	Artifacts Changed	Compatibility Notes
Added **auditRoutingOrganization** (CR-2016-022)	DES Schema	Added new required attribute
Added reference to UIAS CVEs for entityType and lifeCycleStatus. (CR-2015-034, CR-2016-016)	DES Schema	Align with UIAS CVEs
Added reference to ISMCAT's Responsible Entity CVE for expertCountry, nationality-extended, and countryOfAffiliation (CR-2015-102)	DES Schema	Align with other specifications designating country names.
Added reference to GENC for countryName (CR-2016-044)	DES Schema	Align with other specifications designating country names.

Change	Artifacts Changed	Compatibility Notes
Update applicability section to reflect a requirement to comply with Law/ Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.2 - V2015-AUG Change Summary

Significant drivers for Version 2015-AUG include:

- Community Change Requests

Table 69 summarizes the changes made to this technical specification from Version 2014-DEC to Version 2015-AUG.

Table 69 - V2015-AUG Change History

Change	Artifacts Changed	Compatibility Notes
Attribute updated.	**icNetworks**	Changed from Optional to Mandatory for CA Objects; updated allowed values to reference VIRT.XML.[30]
Attribute updated.	**resourceSecurityMark**	Changed from Optional to Mandatory for CA Objects.
Attribute updated.	**authorityRevocationList**	Changed from Mandatory to Optional for CA Objects.
Deprecated attribute.	**languageProficiency**	Deprecated attribute.
Attribute added.	**preferredName**	Attribute added.
Modified text.	FSD DES Chapter 4	Added table to separate persons from NPE.
Modified text.	FSD DES Chapter 5	Added table to separate persons from NPE.
Modified text.	FSD DES Chapter 6	changed certificationAuthority to icCertificationAuthority.
Modified text.	FSD DES Chapter 6	changed language to support other PKI Certification Authorities.

B.3 - V2014-DEC Change Summary

Significant drivers for Version 2014-DEC include:

- Added new attribute for personaUID
- Added policy statements

Table 70 summarizes the changes made to this technical specification from Version 3 to Version 2014-DEC.

Table 70 - V2014-DEC Change History

Change	Artifacts Changed	Compatibility Notes
Implemented new versioning scheme.	DES	Changed versioning scheme from version number (e.g., V3) to version YYYY-MMM (e.g, 2014-DEC).
Attribute updated.	**ipServerAddress**	Changed from Mandatory to Optional.
Attribute updated.	**adminOrganization**	Added support for 2PI.
Added new attribute.	**personaUID**	Added new attribute.
Added new attribute.	**distinguishedName (dn)**	Added attribute to support Common Operating Environment identifier.
Added policy statements.	n/a	Added new policy statements.

B.4 - V3 Change Summary

Significant drivers for Version 3 include:

- Add attribute for **dutySubOrganization**

Table 71 summarizes the changes made to this technical specification from Version 2 to Version 3.

Table 71 - V3 Change History

Change	Artifacts Changed	Compatibility Notes
Attribute displayName updated.	**displayName**	Updated with new attribute dutySubOrganization.
Added Attribute.	**dutySubOrganization**	Added new attribute to be managed and populated by participating IC Elements.
Updated CVE.	**icNetworks**	Updated CVE.

B.5 - V2 Change Summary

Significant drivers for Version 2 include:

- Provide alignment to UIAS

Table 72 summarizes the changes made to this technical specification from Version 1 to Version 2.

Table 72 - V2 Change History

Change	Artifacts Changed	Compatibility Notes
New Attribute	**adminOrganization**	New attribute to be managed and populated by participating IC Elements.
New Attribute	**ATOStatus**	New attribute to be managed and populated by participating IC Elements.
New Attribute	**countryOfAffiliation**	New attribute to be managed and populated by participating IC Elements.
New Attribute	**dutyOrganization**	New attribute to be managed and populated by participating IC Elements.
New Attribute	**lifeCycleStatus**	New attribute to be managed and populated by participating IC Elements.
Deprecated attribute.	**serviceOrAgency**	Deprecated attribute.
Deprecated attribute.	**nationality-Extended**	Deprecated attribute.
Promoted	**isICMember**	Promotion to Mandatory attribute.
Updated	**employeeType**	Added NPE values.
Updated	**CA objects**	Added Resource Security Mark and icNetworks attributes to schema.

B.6 - V1 Change Summary

Significant drivers for Version 1 include:

- Many of these attributes were already in use in the community. This specification serves to codify an agreed-upon interpretation of these attributes and their meaning.

Table 73 summarizes the changes made to this technical specification from prior documentation to Version 1.

Table 73 - V1 Change History

Change	Artifacts Changed	Compatibility Notes
New attribute to be managed and populated by participating IC Elements.	**isICMember**	New attribute to be managed and populated by participating IC Elements.

Change	Artifacts Changed	Compatibility Notes
New attribute to be managed and populated by participating IC Elements.	**generationQualifier**	New attribute to be managed and populated by participating IC Elements.
Deprecated attribute.	**COI**	Deprecated attribute due to lack of use.
Promotion to Mandatory attribute.	**cn**	Promotion to Mandatory attribute.
Promotion to Mandatory attribute.	**employeeType**	Promotion to Mandatory attribute.
Promotion to Mandatory attribute.	**icNetworks**	Promotion to Mandatory attribute.
Promotion to Mandatory attribute.	**resourceSecurityMark**	Promotion to Mandatory attribute.
Controlled Vocabulary defined.	**employeeType**	Controlled Vocabulary defined.
Controlled Vocabulary defined.	**serviceOrAgency**	Controlled Vocabulary defined.
Authentication Mechanisms	Various	In addition to schema changes, this technical specification establishes three authentication tiers for controlling access to IC FSD attributes of varying sensitivity. For a description of these new authentication requirements, please consult section *5 – Securing Access to IC FSD Attributes* of this technical specification.

Appendix C List of Abbreviations

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

2PI	Second Party Integree
ACSS	Allied Collaborative Shared Services
ARL	Authority Revocation List
ATO	Authority To Operate
CA	Certification Authority
CAD	Cryptologic Agencies Domain
CIA	Central Intelligence Agency
CN	Common Name
COI	Community of Interest
CRL	Certificate Revocation List
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DN	Distinguished Name
DNI	Director of National Intelligence
DNS	Domain Name System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Digital Object Identifier
DOJ	Department of Justice
DOS	U.S. Department of State
DOT	Department of Transportation
DSN	Defense Switched Network

DVA	Department of Veterans Affairs
EOP	Executive Office of the President
EPA	Environmental Protection Agency
ESB	Enterprise Standards Baseline
FRB	Federal Reserve Board
FSD	Full Service Directory
GENC	Geopolitical Entities, Names, and Codes
HHS	Health and Human Services
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISM	Information Security Markings
ISMCAT	Information Security Marking Country Codes and Tetragraphs
ISOO	Information Security Oversight Office
JWICS	Joint Worldwide Intelligence Communications System
LDAP	Lightweight Directory Access Protocol
NASA	National Aeronautics and Space Administration
NGA	National Geospatial Intelligence Agency
NIPRNet	Non-Classified Internet Protocol Router Network
NPE	Non-Person Entity
NRC	Nuclear Regulatory Commission

NRO	National Reconnaissance Office
NSA	National Security Agency
NSANET	The National Security Agency intranet
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
PDP	Policy Decision Point
PK	Private Key
PKI	Public Key Infrastructure
POC	Point of Contact
RFC	Request for Comments
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
S/MIME	Secure/Multipurpose Internet Mail Extensions
TREA	Department of the Treasury
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
USAGENCY	Controlled Vocabulary Enumeration Encoding Specification for US Agencies
URL	Uniform Resource Locator
US	United States
USA	United States of America
USAID	U.S. Agency for International Development
USCP	United States Capitol Police
USDA	U.S. Department of Agriculture
USPIS	United States Postal Inspection Service

USPS	United States Postal Service
VIRT	Virtual Coverage
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Appendix D Bibliography

Bibliography

[1] DoD Instruction 8310.01
DoD CIO. *Information Technology Standards in the DoD*. 8310.01. 2 February 2015.
Available online at: http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf

[2] 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

[3] FSD
Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD)*.
Available online Intelink-TS at: http://go.ic.gov/iZiePDW
Available online Intelink-U at: https://w3id.org/ic/standards/FSD
Available online at: https://w3id.org/ic/standards/public

[4] GENC
Country Codes Working Group. *Geopolitical Entities, Names, and Codes*. 3.0.
Available online Intelink-TS at: http://go.ic.gov/QWkfrXy
Available online at: https://geo.aitcnet.org/NSGREG/genc/discovery

[5] IC ITE INC1 IMPL
Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.
Available online Intelink-TS at: http://go.ic.gov/4X6TOc1

[6] IC Markings
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.
Available online Intelink-TS at: http://go.ic.gov/5DjqqWz
Available online Intelink-U at: https://w3id.org/ic/standards/policy/icmarkings [https://w3id.org/ic/standards/policy/icmarkings]

[7] IC PKI CP
Office of the Director of National Intelligence. *Intelligence Community Public Key Infrastructure Certificate Policy*. Version 4.4. 30 April 2012.
Available online Intelink-TS at: http://go.ic.gov/nXRgFih

[8] IC PKI IS
Office of the Director of National Intelligence. *Intelligence Community Public Key Infrastructure Interface Specification*. Version 2.9.4. September 2008.
Available online Intelink-TS at: http://go.ic.gov/D0G8e89

[9] 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: http://go.ic.gov/5Ot5sbK
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[10] 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: http://go.ic.gov/GG61roi
Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[11] ICD 503
Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*. Intelligence Community Directive 503. 15 September 2008.
Available online Intelink-TS at: http://go.ic.gov/W0oErK2
Available online at: http://www.dni.gov/files/documents/ICD/ICD_503.pdf

[12] 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: http://go.ic.gov/qY6rM4s

[13] 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: http://go.ic.gov/ha2FxyZ
Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[14] ICPG 710.1
Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at: http://go.ic.gov/0d147Ee
Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf

[15] ICS 500-13
Director of National Intelligence Chief Information Officer. *Intelligence Community Email Standard Display Name Format* . Intelligence Community Standard 500-13. 2014.
Available online Intelink-TS at: http://go.ic.gov/VxcsfAs

[16] ICS 500-15
Director of National Intelligence Chief Information Officer. *Intelligence Community Optimized Network Email Full Service Directory*. Intelligence Community Standard 500-15. 16 October 2008.
Available online Intelink-TS at: http://go.ic.gov/VhjYQOT

[17] 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: http://go.ic.gov/sLKNq3N
Available online Intelink-U at: https://w3id.org/ic/standards/policy/ICS500-20

[18] 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: http://go.ic.gov/zdD89EN

[19] 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: http://go.ic.gov/EwKUJ2f

[20] IETF-RFC 1274
Internet Engineering Task Force. *The COSINE and Internet X.500 Schema*. November 1991.
Available online at: http://www.ietf.org/rfc/rfc1274.txt

[21] IETF-RFC 2119
Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.
Available online at: http://tools.ietf.org/html/rfc2119

[22] IETF-RFC 2251
Internet Engineering Task Force. *Lightweight Directory Access Protocol (v3)*. December 1997.
Available online at: http://www.ietf.org/rfc/rfc2251.txt

[23] IETF-RFC 2252
Internet Engineering Task Force. *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*. December 1997.
Available online at: http://www.ietf.org/rfc/rfc2252.txt

[24] IETF-RFC 2256
Internet Engineering Task Force. *A Summary of the X.500(96) User Schema for use with LDAPv3*. December 1997.
Available online at: http://www.ietf.org/rfc/rfc2256.txt

[25] IETF-RFC 2798
Internet Engineering Task Force. *Definition of the inetOrgPerson LDAP Object Class*. April 2000.
Available online at: http://www.ietf.org/rfc/rfc2798.txt

[26] IETF-RFC 5280
Internet Engineering Task Force. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008.

Available online at: http://www.ietf.org/rfc/rfc5280.txt

[27] ISMCAT.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.
Available online Intelink-TS at: http://go.ic.gov/xhPfIl3
Available online Intelink-U at: https://w3id.org/ic/standards/ISMCAT
Available online at: https://w3id.org/ic/standards/public

[28] 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: http://go.ic.gov/H8RwEw8
Available online Intelink-U at: https://w3id.org/ic/standards/UIAS
Available online at: https://w3id.org/ic/standards/public

[29] USAgency.CES
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.
Available online Intelink-TS at: http://go.ic.gov/MmBEpFU
Available online Intelink-U at: https://w3id.org/ic/standards/USAgency
Available online at: https://w3id.org/ic/standards/public

[30] VIRT.XML
Office of the Director of National Intelligence. *XML Data Encoding Specification for Virtual Coverage (VIRT.XML)*.
Available online Intelink-TS at: http://go.ic.gov/HGb1I2P
Available online Intelink-U at: https://w3id.org/ic/standards/VIRT
Available online at: https://w3id.org/ic/standards/public

Appendix E Points of Contact

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

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

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

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

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

Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO 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 OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.[17]