Intelligence Community Technical Specification

Data Encoding Specification for IC Full Service Directory Schema

Version 3

09 May 2014

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 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*.[10] 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 and 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

- **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.* [26]

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[3]
- 500 Series:
  - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer[7]
  - Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity[10]
  - Intelligence Community Policy Guidance (ICPG) 500.2, Attribute-based Authorization and Access Management[11]
  - Intelligence Community Standard (ICS) 500-13, Intelligence Community Optimized Network Email Display Name Format[13]
  - Intelligence Community Standard (ICS) 500-15[14]
  - Intelligence Community Standard (ICS) 500-29, IC Digital Identifier[16]
  - Intelligence Community Standard (ICS) 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, And Use For Attribute-Based Access Control Of Resources[17]

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.

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

The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this technical specification are to be interpreted as described in the IETF RFC 2119.[19] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, 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

1.7 - Dependencies

This technical specification depends on the additional technical specifications or additional documentation listed in Table 1 . The documents listed below may or may not be referenced in Chapter 2, and may or may not be considered normative or informative.

Table 1 - Dependencies

Name
IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3+[26]
RFC 2251, Lightweight Directory Access Protocol (v3)[20]
Intelligence Community Certificate Policy V4.4[5]
XML CVE Encoding Specification for US Agency Acronyms, Version 1[27]
ISO 3166-1, Country Codes[25]

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.

For the purposes of this document, normative and informative are defined as:

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 within a major and minor release structure.

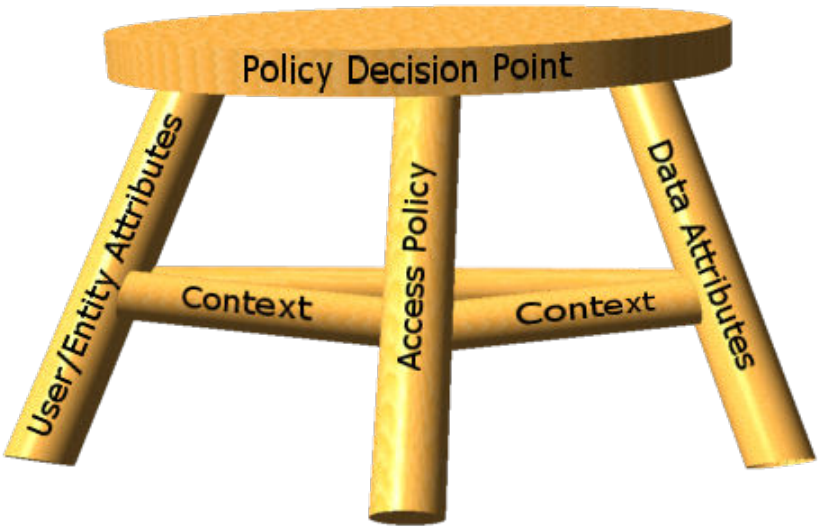
Major releases (whole integers) are for changes to attributes (creation or deprecation), significant changes to definitions or purpose of attributes, and multiplicity of attributes.

Minor releases (“dot releases”) are for changes to controlled vocabularies of existing attributes or clarification of definitions. Changes to controlled vocabularies include the addition or deprecation of values, changes of definitions of values, or changes to location of external controlled vocabularies.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

Technical specifications or information guidance documents are used to make access control decisions. Control decisions comprise 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 being requested (the Who and What respectively), make up the framework that supports an access control decision. A Policy Decision Point (PDP) uses this framework to make a grant or deny access decision. The following is a depiction of the concept of access control decision framework.



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 Enterprise Integration and Architecture (EI&A) 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 attributes specifications include: Fine Access Control (FAC), Full Service Directory *(FSD)* and Unified Identity Attribute Set (UIAS).

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. 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 1 below depicts the IC FSD replication model.

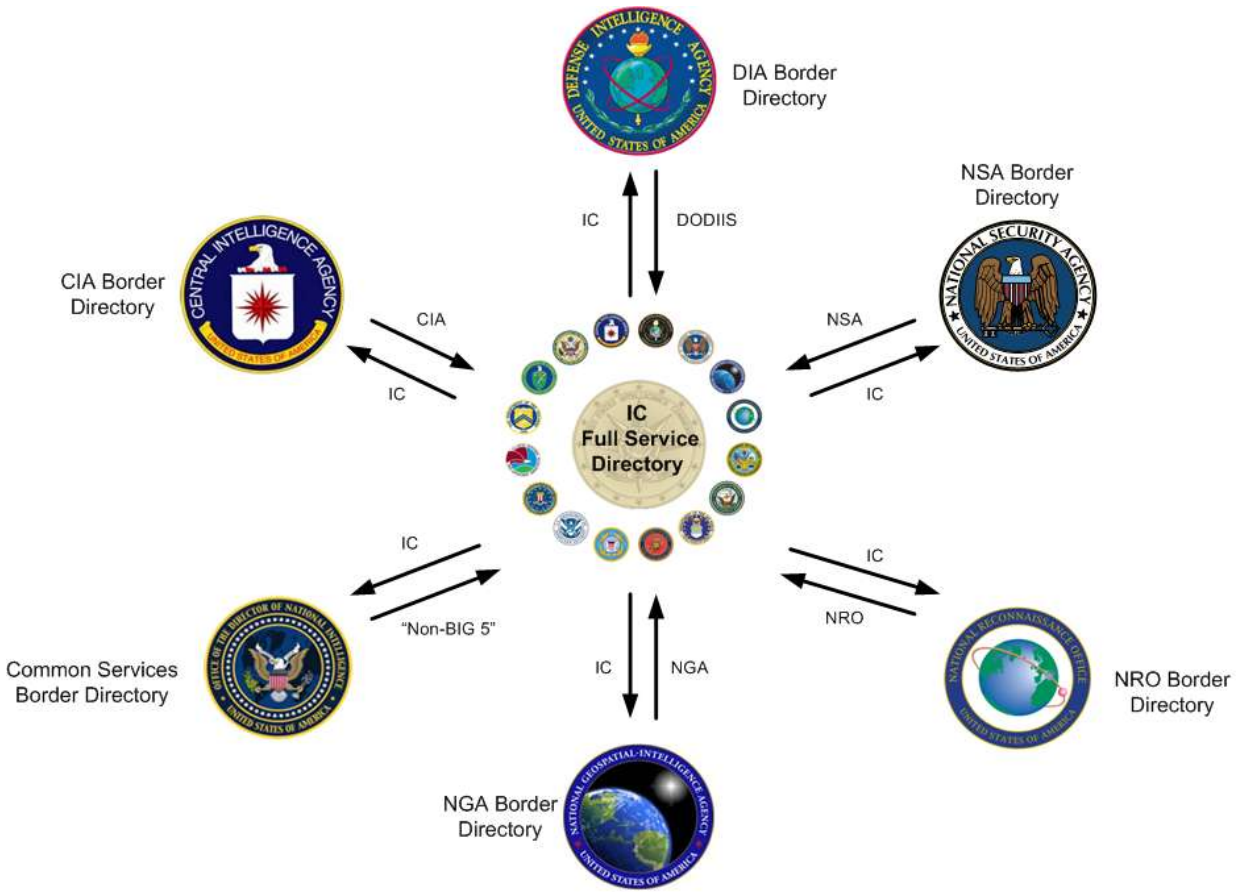


Figure 1 : IC FSD Replication

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.

Chapter 3 - 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.

3.1 - 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 $

           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
      MAY ( audio $ businessCategory $ carLicense $
            departmentNumber $ displayName $ employeeNumber $
            employeeType $ 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 ( countryOfAffiliation $ dutyOrganization $
            adminOrganization $ isICMember $
            icNetworks $ resourceSecurityMark )
      MAY ( icEmail $ secureTelephoneNumber $ companyName $
            internetEmail $ niprnetEmail $ siprnetEmail $
            rank $ buildingName $ countryName $
            militaryTelephoneNumber $
            secureFacsimileNumber $ uid $ expertCountry $
            expertFunctionalArea $ productionManager $
```

```
            languageProficiency )

      )
```

3.2 - 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 ( cn $ icServerAddress $ dutyOrganization $

             adminOrganization $ isICMember $

             ATOStatus $ lifeCycleStatus $

             countryOfAffiliation

             uid $ userCertificate $ resourceSecurityMark $

             icNetworks $ serverPOC )

      MAY ( description $ serverURL )

      )
```

3.3 - 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*.[21] 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

        )
```

3.3.1 - 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,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Admin Organization

Attribute Name	adminOrganization
Description	Reflects the home organization of the entity
Allowable Values	XML CVE Encoding Specification for US Agency Acronyms, Version 1[27]
Example	DIA
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.2 - 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,* [9] 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 3 - ATOStatus

Attribute Name	ATOStatus
Reference	DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
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 only for NPE

Attribute Name	ATOStatus
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.3 - 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 4 - buildingName

Attribute Name	buildingName
Reference	RFC 1274[18]
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
Examples	LX2 NBP-304
Provisioning	Optional
Authentication	Strong User
Single/Multi	MULTI-VALUE

3.3.4 - c, countryName

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

Table 5 - c, countryName

Attribute Name	c, countryName
Reference	RFC 2256[22]
Object Class	icOrgPerson
Friendly Name	Physical Country
Description	Country where IC Person’s physical work facility is located

Attribute Name	c, countryName
Allowable Values	ISO 3166 two-letter country code[25]
Examples	US AU
Provisioning	Optional
Authentication	Strong User
Single/Multi	SINGLE-VALUE

3.3.5 - cn, commonName

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

Table 6 - cn, commonName

Attribute Name	cn, commonName
Reference	RFC 2256[IETF-RF 2256]
Object Class	Person
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 IC PKI certificate.
Allowable Values	For the IC , the *Intelligence Community Public Key Infrastructure Interface Specification* [6] 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

3.3.6 - 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 7 - companyName

Attribute Name	companyName
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.7 - 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 8 - countryOfAffiliation

Attribute Name	countryOfAffiliation
Reference	DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Country of Affiliation
Description	Reflects the citizenship or affiliation of the entity
Allowable Values	3-letter country code as defined in ISO 3166-1[25]
Example	USA
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

3.3.8 - 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 9 - displayName

Attribute Name	displayName
Reference	RFC 2798,[23] Intelligence Community Standard 500-13, *Intelligence Community Optimized Network E-Mail Display Name Format* [13]
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.

Attribute Name	displayName
Allowable Values	Format as defined in ICS 500-13[13]: 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

3.3.9 - 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.

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

        EQUALITY  caseignoreMatch

          SUBSTR  caseignoreSubstringMatch

          SYNTAX  1.3.6.1.4.1.1466.115.121.1.15

        )
```

Table 10 - dutyOrganization

Attribute Name	dutyOrganization
Reference	DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	icOrgPerson / icOrgServer
Friendly Name	Duty Organization
Description	Reflects the assigned organization of the entity
Allowable Values	XML CVE Encoding Specification for US Agency Acronyms, Version 1[27]
Example	DNI
Provisioning	Mandatory
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.10 - 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 11 - dutySubOrganization

Attribute Name	dutySubOrganization
Reference	DES for the IC Full Service Directory Schema,[2] Intelligence Community Standard 500-13, *Intelligence Community Optimized Network E-Mail Display Name Format* [13]
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

Attribute Name	dutySubOrganization
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.11 - 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, Version 3.1* [26]

```
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 12 - employeeType

Attribute Name	employeeType
Reference	RFC 2798,[23] DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	inetOrgPerson / icOrgServer
Friendly Name	Employee Type
Description	Reflects the type of the entity
Allowable Values	GOV, CTR, MIL, SVR, SVC, DEV, NET
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.

Table 13 - employeeType Value Description

Value	Definition	Applicable Entity
MIL	Military service member	Person
CTR	Contractor	Person
GOV	U.S. federal government civilian employee	Person
SVR	Server	Non-Person
SVC	Service, Widget, Application, Software, etc	Non-Person
DEV	End-point device	Non-Person
NET	Network device	Non-Person

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.

3.3.12 - 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 14 - expertCountry

Attribute Name	expertCountry
Reference	DES for the IC Full Service Directory Schema[2]
Object Class	icOrgPerson
Friendly Name	Expert Country
Description	3-letter country code describing an IC Person's expertise area
Allowable Values	3-letter country code as defined in ISO 3166-1[25]
Example	USA
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.13 - 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 15 - expertFunctionalArea

Attribute Name	expertFunctionalArea
Reference	DES for the IC Full Service Directory Schema[2]
Object Class	icOrgPerson
Friendly Name	Expert Functional Area

Attribute Name	expertFunctionalArea
Description	IC Person's functional area expertise
Allowable Values	DIA Intelligence Functional Code
Example	IFC1000
Provisioning	Optional
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.14 - facsimileTelephoneNumber

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

        SYNTAX 1.3.6.1.4.1.1466.115.121.1.22

        )
```

Table 16 - facsimileTelephoneNumber

Attribute Name	facsimileTelephoneNumber
Reference	RFC 2256[22]
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
Single/Multi	MULTI-VALUE

3.3.15 - generationQualifier

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

Table 17 - generationQualifier

Attribute Name	generationQualifier
Reference	RFC 2256[22]
Object Class	*Implementation Dependent*
Friendly Name	Generational Qualifer
Description	The generationQualifier attribute contains the part of the IC Person's name which typically is the suffix

Attribute Name	generationQualifier
Allowable Values	JR, SR, III, IV, etc.
Examples	JR SR
Provisioning	Optional
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.16 - givenName

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

Table 18 - givenName

Attribute Name	givenName
Reference	RFC 2256[22]
Object Class	inetOrgPerson
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
Single/Multi	MULTI-VALUE

3.3.17 - 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 19 - icEmail

Attribute Name	icEmail
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.18 - 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 20 - icNetworks

Attribute Name	icNetworks
Reference	DES for the IC Full Service Directory Schema[2]
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	5EE , ACSS , NSANET , JWICS , IMIS , QNET
Examples	ACSS NSANET
Provisioning	Mandatory

Attribute Name	icNetworks
Authentication	Strong Server
Single/Multi	MULTI-VALUE

3.3.19 - 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 21 - icServerAddress

Attribute Name	icServerAddress
Reference	DES for the IC Full Service Directory Schema[2]
Object Class	icOrgServer
Friendly Name	IP Address
Description	IP Address of IC Non-Person Entity
Allowable Values	Valid IPv4 or IPv6 address
Examples	10.1.2.3 3ffe:1900:4545:3:200:f8ff:fe21:67cf
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.20 - initials

```
attributetype ( 2.5.4.43 NAME ‘initials’ SUP name )
```

Table 22 - initials

Attribute Name	initials
Reference	RFC 2256[22]
Object Class	inetOrgPerson

Attribute Name	initials
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

3.3.21 - 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 23 - internetEmail

Attribute Name	internetEmail
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.22 - 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 24 - isICMember

Attribute Name	isICMember
Reference	DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	icOrgPerson / icOrgServer
Friendly Name	IC Membership
Description	Value that denotes an individual's IC membership status for ICD 501[8] 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,[1] 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 ".

3.3.23 - l, localityName

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

Table 25 - l, localityName

Attribute Name	l, localityName
Reference	RFC 2256[22]
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

3.3.24 - languageProficiency

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

```
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 26 - languageProficiency

Attribute Name	languageProficiency
Reference	DES for the IC Full Service Directory Schema[2]
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	Optional

Attribute Name	languageProficiency
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.25 - 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 27 - lifeCycleStatus

Attribute Name	lifeCycleStatus
Reference	DES for the IC Full Service Directory Schema,[2] ICD 501,[8] Executive Order 12333,[1] IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3.1[26]
Object Class	icOrgServer
Friendly Name	Life Cycle Status
Description	Indicates the life cycle phase in which the entity is operating
Allowable Values	DEV, TEST, PROD, SUNSET
Example	DEV
Provisioning	Mandatory only for NPE
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

Table 28 - lifeCycleStatus Definitons

Value	Definition
DEV	Development
TEST	Test
PROD	Production

Value	Definition
SUNSET	Sunset/Retired

3.3.26 - 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 29 - mail

Attribute Name	mail
Reference	RFC 2798[23]
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

3.3.27 - 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 30 - militaryTelephoneNumber

Attribute Name	militaryTelephoneNumber
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.28 - 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 31 - nationality-Extended

Attribute Name	nationality-Extended
Reference	DES for the IC Full Service Directory Schema[2]
Object Class	icOrgPerson
Friendly Name	Citizenship
Description	3-letter country code describing an IC Person's citizenship
Allowable Values	3-letter country code as defined in ISO 3166-1[25]
Examples	USA GBR AUS

Attribute Name	nationality-Extended
Provisioning	Deprecated
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.29 - 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 32 - niprnetEmail

Attribute Name	niprnetEmail
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.30 - 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 33 - personalTitle

Attribute Name	personalTitle
Reference	RFC 1274[18]
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

3.3.31 - 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 34 - postalAddress

Attribute Name	postalAddress
Reference	RFC 2256[22]
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

3.3.32 - 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 35 - postalCode

Attribute Name	postalCode
Reference	RFC 2256[22]
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

3.3.33 - 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 36 - productionManager

Attribute Name	productionManager
Reference	DES for the IC Full Service Directory Schema[2]

Attribute Name	productionManager
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

3.3.34 - 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 37 - rank

Attribute Name	rank
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.35 - 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 38 - resourceSecurityMark

Attribute Name	resourceSecurityMark
Reference	DES for the IC Full Service Directory Schema[2]
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[4]
Examples	UNCLASSIFIED SECRET//NOFORN
Provisioning	Mandatory
Authentication	Strong Server
Single/Multi	SINGLE-VALUE

3.3.36 - 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 39 - secureFacsimileNumber

Attribute Name	secureFacsimileNumber
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.37 - 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 40 - secureTelephoneNumber

Attribute Name	secureTelephoneNumber
Reference	DES for the IC Full Service Directory Schema[2]
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

Attribute Name	secureTelephoneNumber
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.38 - 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 41 - serverPOC

Attribute Name	serverPOC
Reference	DES for the IC Full Service Directory Schema[2]
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
Allowable Values	Name of an IC Person or IC Element organizational POC
Example	Valid name
Provisioning	Mandatory
Authentication	Strong User
Single/Multi	SINGLE-VALUE

3.3.39 - 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 42 - serverURL

Attribute Name	serverURL
Reference	DES for the IC Full Service Directory Schema[2]
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

3.3.40 - 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 43 - serviceOrAgency

Attribute Name	serviceOrAgency
Reference	DES for the IC Full Service Directory Schema[2]
Object Class	icOrgPerson, icOrgServer
Friendly Name	Home Organization

Attribute Name	serviceOrAgency
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

3.3.41 - 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 44 - siprnetEmail

Attribute Name	siprnetEmail
Reference	DES for the IC Full Service Directory Schema[2]
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

Attribute Name	siprnetEmail
Example	jsmith@intelink.sgov.gov
Provisioning	Policy-Based
Authentication	Network
Single/Multi	SINGLE-VALUE

3.3.42 - sn

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

Table 45 - sn

Attribute Name	sn
Reference	RFC 2256[22]
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

3.3.43 - st, stateOrProvinceName

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

Table 46 - st, stateOrProvinceName

Attribute Name	st, stateOrProvinceName
Reference	RFC 2256[22]
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

Attribute Name	st, stateOrProvinceName
Authentication	Strong User
Single/Multi	MULTI-VALUE

3.3.44 - 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 47 - street, streetAddress

Attribute Name	street, streetAddress
Reference	RFC 2256[22]
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

3.3.45 - 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 48 - telephoneNumber

Attribute Name	telephoneNumber
Reference	RFC 2256[22]
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

3.3.46 - title

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

Table 49 - title

Attribute Name	title
Reference	RFC 2256[22]
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

3.3.47 - 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 50 - uid

Attribute Name	uid
Reference	RFC 2798[23]
Object Class	inetOrgPerson
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

3.3.48 - 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 51 - userCertificate

Attribute Name	userCertificate
Reference	RFC 2256,[22] IC PKI Interface Specification[6]/>
Object Class	inetOrgPerson
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
Example	IC PKI certificate

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

Chapter 4 - 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 52 - Mandatory, Policy-Based, Optional and Deprecated Attributes

Attribute Name	Mandatory	Policy-Based	Optional	Deprecated
adminOrganization	X			
ATOStatus	**X only for NPE**			
buildingName			X	
c, **countryName**			X	
cn, **commonName**	X			
companyName			X	
countryOfAffiliation	X			
displayName		X		
dutyOrganization	X			
dutySubOrganization			X	
employeeType	X			
expertCountry			X	
expertFunctionalArea			X	
facsimileTelephoneNumber			X	
generationQualifier			X	
givenName	X			
icEmail		X		
icNetworks	X			
icServerAddress	X			
initials			X	

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

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

Chapter 5 - Securing Access To IC FSD Attributes

There are no stated requirements for controlling access to the attributes. This technical specification requires three authentication tiers, providing graded authentication for attributes of varying sensitivity. These 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 53 - Securing Access to IC FSD Attributes

Attribute Name	Network	Strong User	Strong Server
adminOrganization			X
ATOStatus			**X only for NPE**
buildingName		X	

Attribute Name	Network	Strong User	Strong Server
c, countryName		X	
cn, commonName	X		
companyName		X	
countryOfAffiliation	X		
displayName	X		
dutyOrganization	X		
dutySubOrganization	X		
employeeType	X		
expertCountry			X
expertFunctionalArea			X
facsimileTelephoneNumber	X		
generationQualifier	X		
givenName	X		
icEmail	X		
icNetworks			X
icServerAddress			X
initials	X		
internetEmail	X		
isICMember		X	
languageProficiency			X
lifeCycleStatus			**X only for NPE**
l, localityName		X	
mail	X		
militaryTelephoneNumber	X		
nationality-Extended	X		
niprnetEmail	X		
personalTitle	X		
postalAddress		X	
postalCode		X	
productionManager	X		
rank	X		
resourceSecurityMark			X
secureFacsimileNumber	X		
secureTelephoneNumber	X		
serverPOC		X	

Attribute Name	Network	Strong User	Strong Server
serverURL		X	
serviceOrAgency	X		
siprnetEmail	X		
sn	X		
st, **stateOrProvinceName**		X	
street, **streetAddress**		X	
telephoneNumber	X		
title	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[9] and subordinate policy documents, and as directed by IC- wide audit policies.

Chapter 6 - IC FSD Schema For IC PKI Root And Intermediate Certificate Authorities

For those IC Elements providing Certification Authority (CA) capabilities under the Intelligence Community Public Key Infrastructure (IC PKI), 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 ( 2.5.6.16 NAME ‘certificationAuthority’ SUP top
AUXILIARY

      DESC ‘RFC2256: certificationAuthority’

      MUST ( authorityRevocationList $

             certificateRevocationList $ cACertificate )

      MAY ( crossCertificatePair $ icNetworks $

            resourceSecurityMark )

      )
```

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

6.1 - 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.[5] [6] However, it is a mandatory attribute within the **certificationAuthority** objectClass and is currently supported by all IC PKI Certificate Authorities.

This attribute is to be stored and 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 54 - authorityRevocationList

Attribute Name	authorityRevocationList
Reference	RFC 2256[22]
Object Class	certificationAuthority

Attribute Name	authorityRevocationList
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 IC PKI Certificate Authority
Provisioning	Mandatory (LDAP object class requirement)
Authentication	Network
Single/Multi	MULTI-VALUE

6.2 - certificateRevocationList

This attribute is to be stored and 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 55 - certificateRevocationList

Attribute Name	certificateRevocationList
Reference	RFC 2256,[22] RFC 5280[24]
Object Class	certificationAuthority
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* [5]
Allowable Values	A valid X.509 V2 CRL as defined in RFC 5280[24] and the *Intelligence Community Public Key Infrastructure Interface Specification* [6]
Example	Any CRL issued by an IC PKI Certificate Authority
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

6.3 - cACertificate

This attribute is to be stored and 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 56 - cACertificate

Attribute Name	cACertificate
Reference	RFC 2256,[22] RFC 5280[24]
Object Class	certificationAuthority
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[24] and the *Intelligence Community Public Key Infrastructure Interface Specification* [6]
Example	Any IC PKI Certificate Authority certificate
Provisioning	Mandatory
Authentication	Network
Single/Multi	MULTI-VALUE

Appendix A Feature Summary

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 57 - 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 58 - FSD Feature comparison

FSD Feature Comparison				
Required date	**Feature**	**V1**	**V2**	**V3**
	Map to UIAS	N	F	F
	Comply with ICS 500-13 Technical Amendment	N	N	F

Appendix B Change History

Table 59 summarizes the version identifier history for this Data Encoding Specification.

Table 59 - 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

B.1 - V3 Change Summary

Significant drivers for Version 3 include:

- Add attribute for **dutySubOrganization**

Table 60 summarizes the changes made to this technical specification from Version 2 to Version 3.

Table 60 - V3 Change History

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

B.2 - V2 Change Summary

Significant drivers for Version 2 include:

- Provide alignment to UIAS

Table 61 summarizes the changes made to this technical specification from Version 1 to Version 2.

Table 61 - 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.3 - 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 62 summarizes the changes made to this technical specification from prior documentation to Version 1.

Table 62 - 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	**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 Glossary

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

5EE	Five-Eyes Enterprise
ACSS	Allied Collaborative Shared Services
ARL	Authorization Revocation List
ATO	Authority To Operate
CA	Certification Authority
CIA	Central Intelligence Agency
CIO	Chief Information Officer
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
DOD	Department of Defense
DOE	Department of Energy
DOI	Digital Object Identifier
DOJ	Department of Justice
DOC	Department of Corrections
DOS	U.S. Department of State
DOT	Department of Transportation
DSN	Defense Switched Network

DVA	Department of Veterans Affairs
EI&A	Enterprise Integration and Architecture
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FAC	Fine Access Control
FRB	Federal Reserve Board
FSD	Full Service Directory
HHS	Health and Human Services
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IMIS	Integrated Management Information System
IP	Internet Protocol
ISO	International Organization for Standardization
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
QNET	Quintipartite Network
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
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
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Appendix D Bibliography

Bibliography

[1] 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

[2] FSD
Office of the Director of National Intelligence. *Data Encoding Specification for IC Full Service Directory Schema (FSD*. 14 December 2011.
Available online Intelink-U at: http://purl.org/IC/Standards/FSD
Available online at: http://purl.org/IC/Standards/public

[3] 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/HvBHBmY

[4] IC Markings
Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2013.
FOUO version available Intelink-TS at: http://go.ic.gov/SLaEjkw

[5] 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://intelshare.intelink.ic.gov/sites/pki/ic%20pki%20policy%20documents/icpki%20cp%20v4.4%20april%202012%20final.pdf
[http://intelshare.intelink.ic.gov/sites/pki/ic%20pki%20policy%20documents/icpki%20cp%20v4.4%20april%202012%20final.pdf]

[6] 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://intelshare.intelink.ic.gov/sites/pki/ic%20pki%20policy%20documents/ICPKI_Interface_Spec_V2.9.4-Sep08_approved.pdf
[http://intelshare.intelink.ic.gov/sites/pki/ic%20pki%20policy%20documents/ICPKI_Interface_Spec_V2.9.4-Sep08_approved.pdf]

[7] 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/enm8L9x
Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[8] 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

[9] 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/b1ZONju
Available online at: http://www.dni.gov/files/documents/ICD/ICD_503.pdf

[10] ICPG 500.1
Assistant Director of National Intelligence for. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 7 May 2010.
Available online Intelink-TS at: http://go.ic.gov/3rfgL6D

[11] 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

[12] ICPG 710.1
Assistant Director of National Intelligence for . *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.
Available online Intelink-TS at: http://go.ic.gov/yAqVQ0H

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

[14] 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

[15] ICS 500-20
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.
Available online Intelink-TS at: http://go.ic.gov/QUDIJkZ
Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/500_20_signed_16DEC2010.pdf

[16] 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/aCTDYKI

[17] ICS 500-30
Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Authoritative Sources, And Use For Attribute-Based Access Control Of Resources*. Intelligence Community Standard 500-30. TBD.
Available online Intelink-TS at: http://go.ic.gov/m2bUQYN

[18] 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

[19] 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

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

[21] 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

[22] 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

[23] 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

[24] 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

[25] ISO 3166-1
International Organization for Standardization (ISO). *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*. ISO 3166-1:2006.

Available online at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719

[26] UIAS
Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS)*.
Available online Intelink-U at: http://purl.org/IC/Standards/UIAS
Available online at: http://purl.org/IC/Standards/public

[27] USAgency.XML
Office of the Director of National Intelligence. *XML CVE Encoding Specification for US Agency Acronyms (USAgency.XML)*.
Available online Intelink-U at: http://purl.org/IC/Standards/USAgency
Available online at: http://purl.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 DNI -sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Public Website: http://purl.org/ic/standards/public

E-mail: ic-standards-support@intelink.gov [mailto:ic-standards-support@intelink.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.[15]