Intelligence Community Technical Specification

Access Control Encoding Specification for Information Security Markings

Version 1

6 September 2013

Table of Contents

List of Tables

Chapter 1 - Introduction

1.1 - Purpose

This *Access Control Encoding Specification for Information Security Markings* (ISM.ACES) defines detailed implementation guidance for providing access to documents based on ISM data. This Access Control Encoding Specification (ACES) defines the combinational logic between data and user/entity attributes. This logic is intended to be used in the decision process of access control decisions based on Extensible Markup Language (XML) elements and attributes that represent ISM data concepts and the associated user attributes.

1.2 - Scope

This specification profile is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This ACES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the ACES should be closely scrutinized and differences separately documented and assessed for applicability.

1.3 - Background

The IC Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an “interoperable federated architecture.” Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [7] grants the IC CIO the authority and responsibility to:

- Develop an IC Enterprise Architecture.
- Lead the IC's identification, selection, development, and management of IC enterprise architecture.
- Incorporate technically sound, deconflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

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

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse. As detailed in Intelligence Community Standard (ICS) 500-21, *Tagging of Intelligence and Intelligence-Related Information* [14] the extensive and consistent use of XML within data encoding specifications allows for improved data exchanges and processing of information, thereby achieving the IC's data discovery, data sharing, and interoperability goals.

Access control encoding specifications further those goals by codifying mappings and combinational logic between data attributes and user/entity attributes to facilitate consistent enterprise-wide boolean access decisions. Historically, access control decisions have been made in local environments based on local interpretations of agreements and policies which has resulted in decisions that are not uniform across the entire enterprise. ACES hope to reduce the need for such local interpretations and further the goal of improving data exchanges and processing of information by documenting and encoding the enterprise interpretation.

ACES provide both abstract and concrete guidance for making access control decisions. The generic abstract guidance is intended to be used in various contexts for making informed access decision logic, but it is the goal of ACES to also provide concrete guidance in appendixes or separate annexes for certain contexts.

1.4 - Enterprise Need

Information security markings vary depending on if the data is from the IC, DoD, DOE, or NATO. There is a clear need to be able to understand these markings and make automated access control decisions. The ISM.ACES builds upon existing policies and guidance to accomplish this need.

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[4]
- 500 Series:
  - Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the IC[8]
  - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information[14]
- 200 Series:
  - Intelligence Community Directive (ICD) 208, Write for Maximum Utility[5]
  - Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination[6]
  - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, Preparing Intelligence to Meet the Intelligence Community’s Responsibility to Provide[12]
- 700 Series:
  - Intelligence Community Directive (ICD) 710, Classification and Control Markings System[10]
  - Intelligence Community Policy Guidance (ICPG) 710.1, Application of Dissemination Controls: Originator Control[11]

1.5 - Audience and Applicability

ACESs are primarily intended to be used by those developing tools and services that perform access control decisions.

The conditions of use and applicability of this technical specification are defined outside of this technical specification. IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance* [13] defines the IC Enterprise Standards Baseline (IC ESB) and the applicability of such to an IC element.

The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

Additional applicability and guidance may be defined in separate IC policy guidance.

1.6 - Conventions

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

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[15]. 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.

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 the following table. The documents listed below are referenced in this encoding specification, and are normative or informative as indicated in the dependencies table.

Table 1 - Dependencies

Name	Dependency Description
XML Data Encoding Specification for Need-To-Know (NTK.XML.V8+)[16]	Depends on Need-To-Know (NTK). The version of NTK imported is not normative, so any NTK version 8 or above may be used.

1.8 - Conformance

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 or enlighten or inform.

Concrete mappings of one set of attributes to another as defined within an ACES are normative.

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.

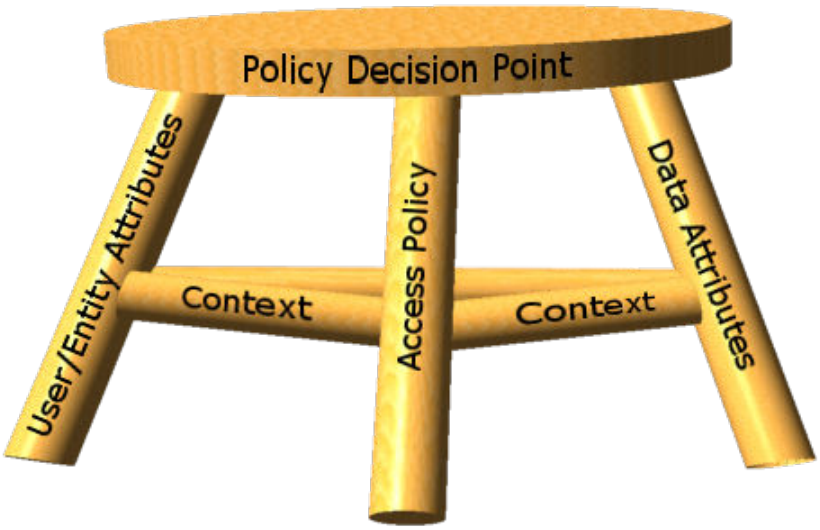
1.9 - Version Policies

The version numbering of this encoding is an integer that increments by 1 for each release. ACES are specifically designed such that changes to the specification are retroactive and apply to all data previously marked with the ACES. Changes to the specification in which that is not the desired behaviour would require a new ACES to be created. Due to this feature, data marked with an ACES do NOT capture the version number in the instance document like other types of encoding specifications. ACES therefore have no equivalent to the DESVersion or CESVersion attributes, and, if an ACES is directly referenced in data, it is done so only by its URI with no version number.

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 access policy leg of the access control framework helping to define mapping conditions between the other two legs. Access policy specifications include: Intelligence Community Only Access Control Encoding Specification (ICO-ACES), ISM-ACES, and OC-NTK-ACES.

2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, documented here are situations for which there is not clearly a single method of encoding the data. The content of this section will evolve over time as additional situations are identified. Implementers of this DES are encouraged to contact the maintainers of this DES for further guidance when necessary.

2.2.1 - The URI

This specification is represented by the URI: guide://2020/ism.aces.

This URI is used to reference and denote the application of this ACES.

2.2.2 - Basic Usage

The presence of ISM data attributes within a data asset specifies that the data asset is controlled by the rules in this ACES and any contextually relevant annexes of this document. This ACES has no need to express information beyond what is already expressed in the ISM attributes. As such, no specific NTK Profile is necessary, however, certain ISM attribute values may have their own requirements for NTK Profiles.

Chapter 3 - Definitions, Interfaces, and Constraints

The ISM specification expresses many constraints that impact access to data. The ISM.ACES is implied by use of ISM. Since part of access control decisions are the context in which they are made, the guidance in this chapter is abstract and any associated concrete mappings can be found in the appendices. The listing of relevant appendices can be found at the end of this chapter in Section 3.4 - Specification Specific Mappings .

The associated concrete mappings are normative and MUST be used when applicable. In the absence of an appropriate concrete mapping, the following abstract mapping may be used to make the access determination. For ISM marks not listed below, guidance from the owner of the marking is required to make an access determination.

3.1 - Classification

This section describes the mapping of data attributes to a user's/person's clearance or a non-person entity's (NPE) accreditation that is determined to be sufficient for access in accordance with Executive Order (E.O.) 13526, *Classified National Security Information* [3].

3.1.1 - US Classification

The guidance in this section applies to when the ownerProducer contains USA either alone or commingled with other values in the case of a JOINT classified resource.

Table 2 - US Classification

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="USA", ism:classification="TS"	The user has a clearance level of TOP SECRET OR The NPE has been accredited to handle TOP SECRET data.
ism:ownerProducer="USA", ism:classification="S"	The user holds a minimum clearance level of SECRET; may have SECRET or TOP SECRET OR The NPE has been accredited at a minimum to handle SECRET data. Accreditation for SECRET or TOP SECRET is acceptable.

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="USA", ism:classification="C"	The user holds a minimum clearance level of CONFIDENTIAL; may have CONFIDENTIAL, SECRET, or TOP SECRET OR The NPE has been accredited at a minimum to handle CONFIDENTIAL data. Accreditation for CONFIDENTIAL, SECRET, or TOP SECRET is acceptable.
ism:ownerProducer="USA", ism:classification="U"	No user clearance or system accreditations are required based on classification. However, there may be other restrictions for Controlled Unclassified Information (CUI).

3.1.2 - Five Eyes Classification

NOTE: [FVEY] in the following table is used to represent the case when ownerProducer contains [AUS], [CAN], [GBR], or [NZL].

Table 3 - Five Eyes Classification

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="FVEY", ism:classification="TS"	The user has a clearance level of TOP SECRET OR The NPE has been accredited to handle TOP SECRET data.
ism:ownerProducer="FVEY", ism:classification="S"	The user holds a minimum clearance level of SECRET; may have SECRET or TOP SECRET OR The NPE has been accredited at a minimum to handle SECRET data. Accreditation for SECRET or TOP SECRET is acceptable.

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="FVEY", ism:classification="C"	The user holds a minimum clearance level of CONFIDENTIAL; may have CONFIDENTIAL, SECRET, or TOP SECRET OR The NPE has been accredited at a minimum to handle CONFIDENTIAL data. Accreditation for CONFIDENTIAL, SECRET, or TOP SECRET is acceptable.
ism:ownerProducer="FVEY", ism:classification="R"	The user holds a minimum clearance level of SECRET; may have SECRET or TOP SECRET OR The NPE has been accredited at a minimum to handle CONFIDENTIAL data. Accreditation for CONFIDENTIAL, SECRET, or TOP SECRET is acceptable.
ism:ownerProducer="FVEY", ism:classification="U"	No user clearance or system accreditations are required based on classification. However, there may be other restrictions for CUI.

3.1.3 - NATO Classification

In this section there is a distinction between general classification levels (R, C, S, and TS) and the NATO version of these classifications represented as [NATO-R], [NATO-C], [NATO-S], and [NATO-TS]. Note that for UNCLASSIFIED, NATO UNCLASSIFIED is not separated from a generic UNCLASSIFIED since it falls outside the classified realm.

Table 4 - NATO Classification

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="NATO", ism:classification="TS"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS] clearance.
ism:ownerProducer="NATO", ism:classification="S"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S] clearance.
ism:ownerProducer="NATO", ism:classification="C"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S], or [NATO-C] clearance.

ISM Attributes	Person or NPE Attributes
ism:ownerProducer="NATO", ism:classification="R"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S], or [NATO-C], or [NATO-R] clearance.
ism:ownerProducer="NATO", ism:classification="U"	clearance = [U], [C], [S], [TS], [NATO-R], [NATO-C], [NATO-S], [NATO-TS]

3.2 - Dissemination Controls

This section describes the mapping of dissemination related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access.

3.2.1 - For Official Use Only

Table 5 - FOUO

ISM Attributes	Person or NPE Attributes
ism:disseminationControls="FOUO"	The user must be one of: • Civilian or Military Member of the US Government. • Contractor under contract to the US Government. • Affiliated with a foreign country that the US is partnered with for purposes related to the information. OR The NPE must meet minimum security standards required for the handling of FOUO data as defined by local agency policy.

3.2.2 - Releasable To

For the purposes of this section, the expression "[LIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For decomplication of tetragraph values in [LIST], please refer to CAPCO Register Annexes for Tetragraphs; CAPCO Register Annex A[1] or CAPCO Register Annex B[2].

Table 6 - REL

ISM Attributes	Person or NPE Attributes
ism:disseminationControls="REL", ism:ReleasableTo="[LIST]"	The person's or NPE's CountryOfAffiliation exists in [LIST].

3.2.3 - Displayable Only To

For the purposes of this section the expression "[LIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For decomplication of tetragraph values in [LIST], please refer to CAPCO Register Annexes for Tetragraphs; CAPCO Register Annex A[1] or CAPCO Register Annex B[2].

Table 7 - DISPLAYONLY

ISM Attributes	Person or NPE Attributes
ism:disseminationControls="DISPLAYONLY", ism:displayableOnlyTo="[LIST]"	DO NOT RELEASE. Only display if the person's or NPE's CountryOfAffiliation exists in [LIST].

3.2.4 - Not Releasable To Foreign Nationals

Table 8 - NF

ISM Attributes	Person or NPE Attributes
ism:disseminationControls="NF"	The person's or NPE's CountryOfAffiliation must be USA.

3.2.5 - Originator Control

Originator Control requires the use of OC-NTK which details the agencies permitted access by the data's originating agency. There is no direct ISM to UIAS mapping. Please see the OC-NTK.ACES specification for guidance on access control decisions related to OC without OC-USGOV.

3.2.6 - Originator Control USGOV

For the purposes of this section, the expression "[USGovList]" refers to the list of organizations in the USGOV Agency Acronym List with namespace urn:us:gov:ic:cvenum:usgovagency:agencyacronym.

Note

If an OC-NTK profile is present, it may increase the dissemination beyond the default for USGOV. As such, it may be necessary to refer to the OC-NTK.ACES for guidance on making an access control decision beyond what is expressed here.

Table 9 - OC-USGOV

ISM Attributes	Person or NPE Attributes
ism:disseminationControls="OC OC-USGOV"	The entity's DutyOrganization exists in [USGovList] or in an optional OC-NTK assertion.

3.3 - SCI Controls

This section describes the mapping of SCI control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with ICD 503 *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation* [9].

3.3.1 - Special Intelligence (SI)

Table 10 - SI

ISM Attributes	Person or NPE Attributes
ism:SCIcontrols="SI"	The user has been read into the SCI Control SI OR The NPE has been accredited to handle SI data.

3.3.2 - Talent-Keyhole (TK)

Table 11 - TK

ISM Attributes	Person or NPE Attributes
ism:SCIcontrols="TK"	The user has been read into the SCI Control TK OR The NPE has been accredited to handle TK data.

3.4 - Specification Specific Mappings

For mappings to specific specifications for the concepts covered in this chapter, please refer to the following appendices:

- Mapping ISM and UIAS Appendix B - Mapping ISM and UIAS

Chapter 4 - Conformance Validation

An access decision is considered conformant with this specification if it grants or denies access based on the normative mappings. The following steps do not dictate how this validation strategy is implemented.

4.1 - Business Rule Validation

The only necessary compliance validation step is to ensure that an access control decision complies with the business rules expressed in this specification. It should be noted that while the business rules for this specification are expressed in English, the English is informative but the constraints they express are normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the English included in this specification and its dependencies.

Appendix A Change History

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

Table 12 - DES Version Identifier History

Version	Date	Purpose
1	06 September 2013	Initial Release

Appendix B Mapping ISM and UIAS

B.1 - Introduction

This appendix discusses the relationship of Information Security Markings (ISM) on data objects to the entity attributes expressed in UIAS. Specifically, it gives an exact value-to-value mapping between the two specifications.

B.2 - Classification

This section describes the mapping of UIAS Clearance to the associated ISM attributes and values sufficient for access.

B.2.1 - US Classification

This section describes the exact value mapping when the classification of the data asset is a US classification.

Table 13 - US Classification

ISM Attributes	Permissible UIAS Clearance
ism:ownerProducer="USA", ism:classification="TS"	TS
ism:ownerProducer="USA", ism:classification="S"	S, TS
ism:ownerProducer="USA", ism:classification="C"	C, S, TS
ism:ownerProducer="USA", ism:classification="U"	U, C, S, TS

B.2.2 - Five Eyes Classification

This section describes the exact value mapping when the classification of the data asset is a Five Eyes partner classification.

NOTE: [FVEY] in the following table is used to represent the case when ownerProducer contains [AUS], [CAN], [GBR], or [NZL].

Table 14 - Five Eyes Classification

ISM Attributes	Permissible UIAS Clearance
ism:ownerProducer="[FVEY]", ism:classification="TS"	TS
ism:ownerProducer="[FVEY]", ism:classification="S"	S, TS

ISM Attributes	Permissible UIAS Clearance
ism:ownerProducer="[FVEY]", ism:classification="C"	C, S, TS
ism:ownerProducer="[FVEY]", ism:classification="R"	U, C, S, TS
ism:ownerProducer="[FVEY]", ism:classification="U"	U, C, S, TS

B.2.3 - NATO Classification

This section describes the exact value mapping when the classification of the data asset is a NATO classification.

Table 15 - NATO Classification

ISM Attributes	Permissible UIAS Clearance
ism:ownerProducer="NATO", ism:classification="TS"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS] clearance.
ism:ownerProducer="NATO", ism:classification="S"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S] clearance.
ism:ownerProducer="NATO", ism:classification="C"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S], or [NATO-C] clearance.
ism:ownerProducer="NATO", ism:classification="R"	The user or NPE has a read on or accreditation for access to NATO information and a [NATO-TS], or [NATO-S], or [NATO-C], or [NATO-R] clearance.
ism:ownerProducer="NATO", ism:classification="U"	clearance = [U], [C], [S], [TS], [NATO-R], [NATO-C], [NATO-S], [NATO-TS]

B.3 - Dissemination Controls

This section describes the exact value mapping between the ism:disseminationControls attribute and the appropriate UIAS attributes.

B.3.1 - For Official Use Only

Table 16 - FOUO

ISM Attributes	UIAS Attributes
ism:disseminationControls="FOUO"	DigitalIdentifier is present.

B.3.2 - Releasable To

For the purposes of this section, the expression "[LIST]" refers to a subset list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto.

Table 17 - REL

ISM Attributes	UIAS Attributes
ism:disseminationControls="REL", ism:ReleasableTo="[LIST]"	CountryOfAffiliation exists in [LIST].

B.3.3 - Displayable Only To

For the purposes of this section, the expression "[LIST]" refers to a subset list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto.

Table 18 - DISPLAYONLY

ISM Attributes	UIAS Attributes
ism:disseminationControls="DISPLAYONLY", ism:displayableOnlyTo="[LIST]"	DO NOT RELEASE. Only display if CountryOfAffiliation exists in [LIST].

B.3.4 - Not Releasable To Foreign Nationals

Table 19 - NF

ISM Attributes	UIAS Attributes
ism:disseminationControls="NF"	CountryOfAffiliation="USA"

B.3.5 - Originator Control

Originator Control requires the use of OC-NTK-ACES for access control determinations. OC-NTK-ACES details the agencies permitted access by the data's originating agency. There is no direct ISM to UIAS mapping. Please see the OC-NTK specification for guidance on access control decisions related to OC and for the UIAS mapping.

B.3.6 - Originator Control USGOV

For the purposes of this sectio,n the expression "[USGovList]" refers to the list of organizations in the USGOV Agency Acronym List with namespace urn:us:gov:ic:cvenum:usgovagency:agencyacronym.

Table 20 - OC-USGOV

ISM Attributes	UIAS Attributes
ism:disseminationControls="OC OC-USGOV"	DutyOrganization exists in [USGovList] or in the 'ORCON NTK' block specified on the document.

B.4 - SCI Controls

B.4.1 - Special Intelligence (SI)

Table 21 - SI

ISM Attributes	UIAS Attributes
ism:SCIcontrols="SI"	FineAccessControls="SI"

B.4.2 - Talent-Keyhole (TK)

Table 22 - TK

ISM Attributes	UIAS Attributes
ism:SCIcontrols="TK"	FineAccessControls="TK"

Appendix C Acronyms

This appendix lists all the acronyms referenced in this encoding specification and lists other acronyms that may have been used in other encoding specifications. This appendix is a shared resource across multiple documents so in any given encoding specification there are likely acronyms that are not referenced in that particular encoding specification.

Table 23 - Acronyms

Name	Definition
A&A	Assessment and Authorization
AAS	Authoritative Attribute Sources
ABAC	Attribute Based Access Control
ABNF	Augmented Backus-Naur Form
ACSS	Allied Collaborative Shared Services
ADD	Abstract Data Definition
AICP	Authorized IC Person
AOI	Area of Interest
AOR	Area of Responsibility
API	Applications Programming Interface
APS	Attribute Practice Statement
ARH	Access Rights and Handling
AS	Attribute Service
ATO	Authority To Operate
BBOX	Bounding Box
BNF	Backus-Naur Form
CA	Certification Authority
CAPCO	Controlled Access Program Coordination Office
CAT	Catalog Services Interface Standard
CDR	Content Discovery and Retrieval
CF-NetCDF	Climate and Forecast - Network Common Data Format
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CMS	Cryptographic Message Syntax
CNWDI	Critical Nuclear Weapons Design Information
COMET	Completely Open Mapping Environment
CONOPS	Concept of Operations
CORBA	Common Object Request Broker Architecture

Name	Definition
CQL	Common Catalog Query Language (CQL)
CRL	Certificate Revocation List
CSW	Catalog Service for Web
CTM	Conformance Test Matrix
CUI	Controlled Unclassified Information
CVE	Controlled Vocabulary Enumeration
D & R	Discovery and Retrieval
DAA	Designated Approval Agent
DC MES	Dublin Core Metadata Element Set
DCMI	Dublin Core Metadata Initiative
DDMS	Department of Defense Discovery Metadata Specification
DES	Data Encoding Specification
DI	Digital Identifier
DIA	Defense Intelligence Agency
DISR	DoD Information Technology Standards Registry
DN	Distinguished Name
DNI	Director of National Intelligence
DNS	Domain Name System
DOD	Department of Defense
DOE	Department of Energy
DOI	Digital Object Identifier
DOMEX	Document and Media Exploitation
EA	Enterprise Architecture
EI&A	Enterprise Integration and Archetecture
E.O.	Executive Order
EBNF	Extended Backus-Naur Form
EDH	Enterprise Data Header
EPR	Endpoint Reference
ES&IS	Enterprise Search & Integration Services
ESB	Enterprise Standards Baseline
FD&R	Foreign Disclosure & Release
FOUO	For Official Use Only
FSD	Full Service Directory
FTP	File Transfer Protocol
FY	Fiscal Year

Name	Definition
GENC	Geopolitical Entities, Names, and Codes
GeoRSS	Geographic Really Simple Syndication
GeoTIFF	Geographic Tagged Image File Format
GIF	Graphics Interchange Format
GIS	Geospatial Information System
GML	Geography Markup Language
GNS	Geographic Names Server
GUIDE	Globally Unique Identifiers for Everything
GVS	GEOINT Visualization Services
HDF-EOS	Hierarchical Data Format - Earth Observing System
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I2	Information Integration
IC	Intelligence Community
IC.ADD	Intelligence Community Abstract Data Definition
IC CIO	Intelligence Community Chief Information Officer
IC EA	IC Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	IC Information Technology Enterprise
ICD	Intelligence Community Directive
ICEA	Intelligence Community Enterprise Architecture
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
ICSR	Intelligence Community Standards Registry
ICTS	Intelligence Community Technical Specification
IdAM	Identity and Access Management
IDM	Interface Data Model
IDMView	Interface Data Model View
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability
IP	Internet Protocol
IPT	Integrated Project Team
IRM	Information Resource Metadata
ISBN	International Standard Book Number
ISM	Information Security Marking

Name	Definition
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
ITE	Information Technology Enterprise
JPEG	Joint Photographic Experts Group
JPIP	JPEG 2000 Interactive Protocol
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWICS	Joint Worldwide Intelligence Communications System
JWT	JSON Web Token
KA	Knowledge Assertion
KML	Keyhole Markup Language
KOS	Knowledge Organization System
KVP	Key Value Pair
LDAP	Lightweight Directory Access Protocol
LIMDIS	Limited Distribution
LNI	Library of National Intelligence
MAC	Multi Audience Collection
MC&GIL	Mapping, Charting, and Geodesy Information Library
MC&GView	Mapping, Charting, and Geodesy View
MIME	Multipurpose Internet Mail Extensions
MTOM	Message Transmission Optimization Mechanism
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NGA	National Geospatial Intelligence Agency
NGDS	Net-Centric GEOINT Discovery Services
NGIC	National Ground Intelligence Center
NGT	Next Generation Trident
NIPRNet	Non-Classified Internet Protocol Router Network
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NPE	Non-Person Entity
NMEC	National Media Exploitation Center
NRO	National Reconnaissance Office

Name	Definition
NSA	National Security Agency
NSG	National System for Geospatial Intelligence
NSI	National Security Information
NTK	Need-To-Know Metadata
OCIO	Office of the Intelligence Community Chief Information Officer
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
OGC	Open Geospatial Consortium
OGCA	Open Geospatial Consortium Australia
OGCE	Open Geospatial Consortium Europe
ONEMail	Optimized Network Email
OPM	Office of Personnel Management
OWS	OGC Web Services
PAP	Policy Administration Point
PAYL	Payload
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PK	Private Key
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
PUBS	Intelligence Publications
PURL	Persistent Uniform Resource Locator
RA	Reference Architecture
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RFC	Request for Comments
RR-ID	REST Security Encoding Specification for End-to-End Identity Propagation
SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSD	Special Security Directorate

Name	Definition
SSL	Secure Sockets Layer
STIL	St Louis Information Library
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Trusted Data Collection
TDF	Trusted Data Format
TDO	Trusted Data Object
TGN	Thesaurus of Geographic Names
TIFF	Tagged Image File Format
TIN	Triangulated Irregular Network
TLS	Transport Layer Security
TS	Top Secret
UAAS	Unified Authorization and Attribute Services
UIAS	Unified Identity Attribute Set
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
US	United States
UUID	Universal Unique Identifier
VIRT	Virtual Coverage
W3CDTF	World Wide Web Consortium Date Time Format
WARP	Web Based Access and Retrieval Portal
WCS	Web Coverage Service
WFS	Web Feature Service
WMS	Web Map Service
WSDL	Web Service Definition Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XPath	XML Path Language
XPointer	XML Pointer Language
Xquery	XML Query
XSLT	XML Stylesheet Language for Transformations

Appendix D Bibliography

Bibliography

[1] CAPCO Register Annex A
Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *CAPCO Register Annex A Tetragraphs* . SECRET//REL FVEY version. Volume 6. (Version 6.0). Effective: 19 July 2013.
Available online Intelink-TS at: http://intelshare.intelink.ic.gov/sites/ncix/ssd/csg/capco/ccm/U%20CAPCO%20Guidance/CAPCO%20Register%20Annex%20A%20Tetragraph%20Table_19July13_(S_REL).pdf

[2] CAPCO Register Annex B
Director of National Intelligence (DNI), Special Security Directorate (SSD), Controlled Access Program Coordination Office (CAPCO). *CAPCO Register Annex B Tetragraphs* . SECRET//NOFORN version. Volume 5. (Version 5.1). Effective: 31 May 2012.
Available online Intelink-TS at: http://intelshare.intelink.ic.gov/sites/ncix/ssd/csg/capco/ccm/U%20CAPCO%20Guidance/U%20CAPCO%20Guidance%20CAPCO%20Register%20Annex%20B%20Tetragraph%20Table_31May2012_NOFORN.pdf

[3] E.O. 13526
The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.
Available online at: http://www.archives.gov/isoo/pdf/cnsi-eo.pdf

[4] 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

[5] ICD 208
Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.
Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[6] ICD 209
Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.
Available online at: http://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.pdf [http://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.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] ICD 710
Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.
Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[11] 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

[12] ICPM 2007-200-2
Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2, . 11 December 2007.
Available online at: http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf

[13] 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

[14] ICS 500-21
Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.
Available online Intelink-U at: https://intelshare.intelink.gov/sites/odni/cio/ea/library/Data%20Specifications/500-21/ICS_500-21_SIGNED_20110128.pdf

[15] 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

[16] NTK.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML)*.
Available online Intelink-U at: http://purl.org/IC/Standards/NTK
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> .

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.[13]